Congress of the United States
Washington, DC 20515

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

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

April 18, 2024

Dear Chairwoman Murray and Vice Chair Collins:

In March 2020, the Cyberspace Solarium Commission published recommendations for defending the United States in cyberspace.[1] As a result of Congress's determined attention to cybersecurity issues in the intervening four years, more than 80 percent of the Commission's original recommendations have seen significant progress, and almost 70 percent of them are implemented or nearly so. However, the implementation of a recommendation – codification in law, establishment through executive order, or otherwise – does not guarantee success. In order to have a meaningful impact on cybersecurity, these efforts must also 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 (FY19 NDAA) 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 to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power. 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. We ask that you support these requests to ensure that Congress's recent work on cybersecurity leads to lasting improvements in defending U.S. interests in cyberspace.

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

Agriculture, Rural Development, and Food and Drug Administration

- As the co-Sector Risk Management Agency for the agricultural sector, the USDA's Office of Homeland Security (OHS) plays a pivotal role in coordinating efforts to mitigate cybersecurity risks for over two million farms nationwide. However, past funding requests from the administration for OHS have lacked transparency regarding the allocations of resources to tackle cybersecurity challenges. Adequate funding is imperative for OHS to fulfill its sector risk management duties, helping foster public-private collaboration and ensuring effective coordination within the food and agriculture sector. Therefore, **we recommend an increase of $1,500,000 over the administration's request for Food and Agriculture Sector Support within the USDA Office of Homeland Security to specifically address cybersecurity threats to the sector.**

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. Within the federal 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 (NSF) 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 $85 million in FY25, $11 million above the request.**

  We note our strong opinion that this funding should not be divided or diminished to fund the replication of the Scholarship for Service model in any other field 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 $85,000,000 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."

- **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 (AI), quantum information science, and next-

generation communications technologies. Last year, the administration issued Executive Order 14110 on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which highlights the significance of NIST's work as it is tasked to establish AI standards for critical infrastructure. While many emerging 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. Leveraging its research insights and data and forging 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, including AI.

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. Last year, Congress recognized the importance of providing adequate funding for NIST's Cybersecurity and Privacy portfolio, approving the $20 million increase in funding as requested in FY24. Despite the increased responsibilities, the FY25 budget request, however, is $0.9 million below the FY24 request. **We recommend the following report language**:

*"National Vulnerabilities Database.—*The Committee acknowledges the critical importance of NIST's role in maintaining the National Vulnerabilities Database, which is a vital resource in identifying, assessing, and mitigating vulnerabilities in software systems, thus enhancing the overall security posture of our nation's digital infrastructure. With limited interagency support to carry out this work, NIST will need consistent funding and personnel to maintain a common vulnerabilities and exposures (CVE) database, especially with a surge of vulnerability reporting in recent years. To address this, the Committee recommends that no less than $1,500,000 be made available for CVE analysis and $1,500,000 be made available for personnel to support its operations.

3) Section 9401 of the FY21 NDAA authorized **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 $50 million over the request for Cybersecurity and Privacy portfolio, and we recommend an increase of $20 million for advancing research in Critical and Emerging Technologies for Scientific and Technical Research and Services at the National Institute of Standards and Technology. We further recommend the following report language:**

"*Critical and Emerging Technologies.*—The Committee recognizes the National Institute of Standards and Technology's (NIST) 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."

"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 the National Institute of Standards and Technology's Cybersecurity and Privacy activity for purposes including increasing personnel and contracting resources: $2,000,000 for vulnerability management, $1,500,000 for cryptography programs, $7,000,000 for privacy programs, $1,500,000 for identity and access management, $3,500,000 for software security, $2,500,000 for infrastructure with a particular focus on Domain Name System and Border Gateway Protocol security, $5,000,000 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 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)."

"Update NIST 800-193.—The Committee recognizes that enhancing the private sector's cybersecurity resilience is a critical component to protecting national security. However, limited standards and guidance for implementing best security practices leave these firms as a target for cyberattacks. Therefore, the Committee recommends that the National Institute of Standards and Technology (NIST) undertake a comprehensive update of Platform Firmware Resiliency Guidelines (NIST 800-193), containing guidelines for private companies to implement specific

firmware security. This would include ways to maintain software inventories, like the Software Bill of Materials (SBOMs), to document all components of the software in use to enable quick identification of potential vulnerabilities in their 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. However, this year's salary adjustments for the FBI's cybersecurity workforce pose a serious concern for national security. The FBI's goal is to expand its cyber ALAT program from 11 to 16 by the end of 2024, and any cuts to the FBI's salaries and expenses would jeopardize the expansion of the program and the FBI's cyber workforce writ large. Thus, sustained funding will be crucial 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 FY25 funding request of $11,327,900 for the Federal Bureau of Investigation's Salaries and Expenses account. We 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."

- 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 one of only 13 principal statistical agencies 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**

of $20 million above the FY25 request for the NCSES and further recommend the following report language:

"National Center for Science and Engineering Statistics.—The Committee provides $20,000,000 over the request for the National Center for Science and Engineering Statistics (NCSES) 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."

- The international telecommunications market is currently watching the race to develop and deploy **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 $3 million over the administration's request for Advanced Communications Research at the National Telecommunications and Information Administration and the following report language:**

  "Advanced Communications Research.—The Committee provides an increase of $3,000,000 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."

Defense

- The U.S. Cyber Command's (CYBERCOM) **Hunt Forward missions** are crucial to proactively identify and counter cyber threats globally. In 2023, CYBERCOM deployed 22 hunt forward missions to 17 countries. CYBERCOM then publicly shared 90 malware samples to the cybersecurity community for analysis, which could provide key intelligence data to protect billions of Internet users online. Investing in these missions is instrumental in bolstering the cybersecurity posture of our international partners and allies, thereby enhancing the collective security within cyberspace. Deployment of the Cyber National Mission Force to allied nations for hunt forward missions not only aids in strengthening their cyber defenses but provides CYBERCOM with invaluable insights and strategic advantages against adversaries. In light of the escalating and persistent challenges in global security, it is vital to support a preemptive approach in protecting the digital systems of the U.S. critical infrastructure from malign actors to stay ahead of potential threats. **Therefore, we strongly support the administration's request for $262 million for the U.S. Cyber Command's Hunt Forward Missions.**

Energy & Water

- The Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads the department's efforts to strengthen the cybersecurity and resilience

of the energy sector and serves as the Sector Risk Management Agency. 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 to follow, a critical step in closing the maturity gap between SRMAs and establishing a common baseline of effective performance across government. **To that end, we support the President's budget request of $200 million for the Office of Cybersecurity, Energy Security, and Emergency Response.**

Financial Services and General Government

- Since its establishment pursuant to Section 1752 of the FY21 NDAA, the Office of the National Cyber Director (ONCD) 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 is leading many of the initiatives to implement 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 $19,126,000 for salaries and expenses at the Office of the National Cyber Director.**

- The Office of Personnel Management (OPM) 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 for the federal government. However, these tools are not widely utilized or understood in many hiring offices across the federal government. Enhanced OPM support for federal hiring offices would ensure that existing cybersecurity compensation flexibilities and direct hire authorities are used to the fullest extent possible. **We support the administration's requested increase of $6,984,795,000 for the Workforce Policy and Innovation account at the Office of Personnel Management to enhance the federal government's strategic workforce planning and talent acquisition.**

- 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 $50 million increase to its Cybersecurity Enhancement Account, which includes $12,000,000 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 $75 million for the Technology Modernization Fund.**

- The Department of the Treasury's **Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)** serves as the Sector Risk Management Agency for the financial services sector, managing much of the day-to-day engagement on cybersecurity issues between the federal government and private-sector entities. OCCIP facilitates information sharing, advocates for the use of best-practice security measures, and aids critical infrastructure owners and operators in responding to significant incidents. Despite the increasing cybersecurity risks to the financial services sector and the growing demand for the office's SRMA functions, 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 FY25** to increase funding available for additional personnel in order to support communication and coordination with the financial services sector.

Interior, Environment, and Related Agencies

- As the Sector Risk Management Agency for the water and wastewater systems sector, the Environmental Protection Agency (EPA) 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 underscores the urgent need for robust funding for EPA's SRMA duties. However, EPA has historically lacked the resources necessary to effectively execute its mission in this area. This funding gap poses a significant risk, given the potential consequences of cybersecurity threats to our drinking water and wastewater systems. **Therefore, we strongly recommend an increase of $3 million over the FY25 request for the Homeland Security project of the Science and Technology activity at the Environmental Protection Agency. We further support the administration's request for $25 million in a competitive grant program to bolster cybersecurity measures within the water and wastewater systems sector.**

Homeland Security

- Last year, CISA proposed a new Cyber Analytics and Data System, a significant step forward in the Agency's efforts to enhance partnerships across the cybersecurity ecosystem through timely and effective information sharing. In FY25, CISA requested a funding increase and more personnel to scale operational infrastructure to increase efficiency and to support additional data analysis and cross-correlation of 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 requested increase of $19,142,000 over the FY24 enacted for the Cyber Analytics and Data Protection System at Cybersecurity and Infrastructure Security Agency. We further support the administration's request for the Joint Collaborative Environment PPA.**

- 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 of critical infrastructure, a single coordinator will be insufficient to meet the requirements to provide a more mature risk analysis and measurement 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 the Cybersecurity and Infrastructure Security Agency's (CISA) 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."

- 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. The FY25 request contains additional funding to support CISA's integrated cyber, physical, and communications operations center, which would strengthen the agency's overall operational preparedness. **We support the administration's request of $107,966,000 for the Operations Coordination and Planning PPA for Integrated Operations at 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 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 increase of $10 million over the FY25 request for Cybersecurity Education Training Assistance Program through the Stakeholder Engagement Division. We also recommend the following report language:**

  "*Cybersecurity Education and Training Assistance Program (CETAP).*—The Committee provides an additional $10,000,000 to enhance Cybersecurity Education and Training Assistance

Program (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."

- To support cybersecurity workforce development, CISA awarded grants in FY21 under the **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 for the second year in a row. 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 for the Non-Traditional Training Provider grant program of the Cyber Defense Education & Training within the Stakeholder Engagement Division and the following report language:**

  "Non-Traditional Training Providers.—The Committee rejects the proposed decrease to the Non-Traditional Training Provider (NTTP) grant funding included in the request, and directs the Cybersecurity and Infrastructure Security Agency 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."

- Two years 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 $115,918,000 for FY25 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 $4,085,000 to the Mission Support PPA and $10,869,000 to the Other Operations and Enforcement PPA for cybersecurity from the FY24 request.**

- The cybersecurity of the maritime transportation system (MTS) subsector remains a top priority in safeguarding U.S. economic security. As the co-Sector Risk Management Agency, the U.S.

Coast Guard plays a central role in federal cybersecurity efforts for the MTS. Yet, each year, the Coast Guard receives little to no funding for its SRMA responsibilities and continues to suffer from a shortage of personnel to support this mission. Similarly, the FY25 request contained no funding for the Coast Guard's office that coordinates SRMA work.

In the coming years, the U.S. Coast Guard anticipates increased responsibilities related to the safeguarding of vessels, harbors, ports, and waterfront facilities cybersecurity. The administration's recent Executive Order 10173 amended the Coast Guard's role in engaging with its public and private partners and critical infrastructure owners and operators of MTS. Thus, inadequate funding could have severe consequences in securing the MTS infrastructure from cyber threats. **To equip the U.S. Coast Guard as the co-Sector Risk Management Agency of the maritime transportation systems subsector, we recommend providing $3,000,000 in funding dedicated to building operational capacity. Of that, $90,000 for recruitment and incentive funding** to build a pool of sector-specific cybersecurity expertise of the MTS and close the cyber workforce gap within the U.S. Coast Guard to ensure that the Service is able to meet its mission needs for the MTS subsector.

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

- To effectively protect K-12 school systems from rising cyber threats, it is imperative that the Department of Education, the Sector Risk Management Agency for K-12 schools, is adequately resourced to carry out its duties. However, the President's budget request shows no specific details on K-12 cybersecurity critical infrastructure protection and lacks clarity as to whether the Office of Chief Information Officer is focused on carrying out SRMA duties in addition to enhancing the Department's internal enterprise cybersecurity. K-12 schools are vulnerable to rising cyberattacks, including ransomware incidents and phishing scams that jeopardize the integrity of student records and create disruptions to education services. Ensuring robust cybersecurity defenses is vital to safeguard the privacy and security of students, educators, and administrators. **We recommend ensuring that there is an office dedicated to carrying out the Sector Risk Management Agency duties at the Department of Education to prevent and address cybersecurity threats at K-12 schools, with a minimum of $3,000,000 allocated to carry out its duties.**

- Among the 16 critical infrastructure sectors, cyberattacks are surging against the healthcare and public health sector, with 133 million individuals affected by data breaches in 2023.[2] Cyberattacks against hospital systems impact patient care and could even cause loss of life; as such, mitigating cybersecurity risks to the sector is of critical importance. The Department of Health and Human Services' (HHS) Sector Risk Management Agency duties fall under the Division of Critical Infrastructure Protection within the Administration for Strategic Preparedness and Response (ASPR CIP). By HHS's own admission, ASPR's budget has been insufficient to execute its SRMA responsibilities.[3] **While we support the $12 million increase above the FY23 enacted levels for the Administration for Strategic Preparedness and**

[2] https://finance.yahoo.com/news/133-million-breached-patient-records-150000280.html
[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

Response's Division of Critical Infrastructure Protection, we are concerned that funding for a grant program to help the sector implement basic cybersecurity measures will not provide funds to operators until FY27 at the earliest. We recommend the following report language:

"Healthcare and Public Health Sector Cybersecurity Performance Goals.—The Committee notes its significant concerns with cybersecurity threats to the Healthcare and Public Health Sector, and urges the Department to rapidly roll out its proposed program to support the implementation of essential cybersecurity performance goals."

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 has taken 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 support the $1.4 million increase above the FY24 request for the Bureau of Cyberspace and Digital Policy.**

- The FY23 NDAA established the Cyberspace, Digital Connectivity, and Related Technologies Fund, which was intended to allow CDP to provide assistance to countries to bolster civilian capacity by addressing national cybersecurity and deterrence in cyberspace. CDP's efforts can help reduce vulnerability in the ICT ecosystem and advance U.S. national and economic security objectives. CDP is authorized to provide funds to "advance a secure and stable cyberspace; protect and expand trusted digital ecosystems and connectivity; build the cybersecurity capacity of partner countries and organizations; and ensure that the development of standards and the deployment and use of technology supports and reinforces human rights and democratic values." The FY24 enacted budget provided $50,000,000 for the Cyberspace, Digital Connectivity, and Related Technologies Fund. The FY25 budget has no request for funds as this was a new start initiative that did not exist when the State Department budget was developed. **We support making $50,000,000 available for the Cyberspace, Digital Connectivity, and Related Technologies Fund. We further recommend the following report language:**

"*Cyberspace, Digital Connectivity, and Related Technologies Fund*.—The Committee recommends not less than $50,000,000 for the Cyberspace, Digital Connectivity, and Related Technologies Fund in accordance with Chapter 10 of Part II of the Foreign Assistance Act of 1961. That the authority of section 592(f) of such Act may apply to amounts made available for such Fund under the heading "Economic Support Fund" and such funds may be made available for the Digital Connectivity and Cybersecurity Partnership program consistent with section 6306 of the Department of State Authorization Act of 2023. The establishment of the Cyberspace, Digital Connectivity, and Related Technologies Fund was intended to allow the Bureau of Cyberspace and Digital Policy to provide assistance to countries to bolster civilian capacity to

address national cybersecurity and deterrence in cyberspace and can help reduce vulnerability in the ICT ecosystem and advance U.S. national and economic security objectives."

- **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 appropriations to four funds that support different aspects of international cybersecurity capacity building:

  1) We support the $80 million increase above the FY24 enacted levels for the Assistance for Europe, Eurasia, and Central Asia Fund for cyber capacity building. Cyber capacity building efforts in this region would improve security and cybersecurity globally by strengthening allies' and partners' capability to counter Russian influence and aggression.

  2) We support the FY25 request of $20 million for Cybercrime and Intellectual Property Rights 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.

  3) We recommend a $22.5 million increase above the FY25 request for the Digital Connectivity and Cybersecurity Partnership to support the partnership's focus on enhancing cybersecurity.

  4) We recommend a $55 million increase above the FY25 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 supports the use of funds appropriated 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 the International Narcotics Control and Law Enforcement Fund appropriated 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 $22,500,000 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 $55,000,000 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, but it also improves U.S. security by creating a community of capable, secure, like-minded countries. The **Economic Support Fund (ESF) is an important resource for this international cyber capacity building**, and the FY25 budget requests that $40.7 million from the ESF's Information and Communications Technology (ICT) and cyber capacity building programming be made available to the Bureau of Cyberspace and Digital Policy. The request would allocate a further $17 million from the International Technology Security and Innovation (ITSI) Fund to ESF, to be administered by CDP in order to promote the development and adoption of secure ICT networks and services. **We support the $40.7 million request for the Economic Support Fund's Information and Communications Technology cyber capacity building program. We also support the $42,250,000 budget allocation from the International Technology Security and Innovation Fund to defend ICT ecosystems. We further recommend the following language**:

  "*International Cybersecurity Capacity Building.*—The Committee supports the 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 the International Technology Security and Innovation 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 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. 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 recommend a $10 million increase above the FY25 request 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."

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