U.S. CYBERSPACE SOLARIUM COMMISSION
POTOMAC GATEWAY SOUTH
2900 CRYSTAL DRIVE, SUITE 250
ARLINGTON, VA 22202

April 22, 2021

Dear Chairwoman DeLauro and Ranking Member Granger:

As the two U.S. Representatives serving as members of the Cyberspace Solarium Commission,[1] we write to request that you substantially increase the national defense budget function (050) 302(b) allocation for the Homeland Security Subcommittee to support the efforts of the Cybersecurity and Infrastructure Security Agency (CISA) to strengthen our nation's cybersecurity. **The Homeland Security Subcommittee requires a 302(b) 050 allocation increase of at least $400 million to support CISA's budget for FY22.** Forgoing such an increase will delay implementation of key authorities Congress just passed to strengthen CISA and perpetuate gaps in federal network security that have been exposed by the rising threats in this new domain.

Recent months have seen two significant malicious cyber events targeting the U.S. government and critical infrastructure. The SolarWinds campaign, carried out by Russia, has led to network compromise in nine government agencies, while the damage resulting from the Microsoft Exchange Server vulnerability is still unfolding. As part of the U.S. government response to both, CISA played a central role, providing cyber defenders in its sister agencies and critical infrastructure providers across the country with timely and reliable information on the threat and indicators of compromise. Meanwhile, CISA continues to provide services to the rest of the U.S. government to identify threats and harden federal networks against future attacks, to the extent that their resources allow.

Despite the critical functions that CISA is currently performing, far more is required of the agency in order to build meaningful security in federal networks and national resilience to significant cyber incidents. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021[2] took historic strides by authorizing sweeping efforts that will strengthen American cybersecurity. Among its many cybersecurity provisions, the bill included 27 provisions drawn from the work of the Cyberspace Solarium Commission. This encompassed a number of CISA specific sections including: conducting a force structure and resource requirement assessment;[3] standing up a Joint Cyber Planning Office;[4] expanded authorities to hunt for threats on Federal agency networks;[5] and codifying support for cybersecurity education.[6]

As CISA's statutory mission set grows, appropriations must grow to match the mandate. For FY21, the Commission recommended five different appropriations provisions which together amounted to more than $100,000,000 in increases to the CISA budget. We expect some of the activities the Commission recommended in FY21 for defending federal networks will be implemented with funding made available

[1] https://www.solarium.gov
[2] Pub. L. 116-283
[3] Section 1745
[4] Section 1715
[5] Section 1705
[6] Section 2217

through the American Rescue Plan Act of 2021 (ARPA).[7] Funding appropriated by ARPA is expected to enable critical steps in remediating gaps in federal network resilience, but that funding only covers one part of CISA's work.

CISA's mandate and programs extend beyond federal networks and are intended to improve security in critical infrastructure, which is largely in private sector hands and heavily influenced by state, local, tribal, and territorial (SLTT) governments. Many of the Commission's recommendations call for expanding, improving, or creating programs that are rooted in this cross-sectoral aspect of CISA's work. For example, FY21 NDAA Section 9002 strengthens connectivity between critical infrastructure sectors and the federal government by codifying the roles and responsibilities of sector risk management agencies (SRMAs). CISA serves both as the executive agent in public-private partnerships between SRMAs and their various critical infrastructure sectors, and as the SRMA for eight individual sectors. Programs like this are critical to national cybersecurity but fall outside the scope of the federal civilian cybersecurity efforts requested by President Biden as part of ARPA.

In FY22, CISA requires additional funding to significantly expand non-federal network resilience efforts. Under those broad headings, investments in five lines of effort will have immediate impact in furtherance of the Commission's recommendations.

- **Sector Engagement Capacity -** We must significantly expand CISA's critical infrastructure sector engagement capacity. Added resources, particularly increased personnel and funds to reimburse interagency detailees, would enable CISA to more effectively support all sixteen critical infrastructure sectors and their corresponding SRMAs, bolster sector-specific expertise, and improve the agency's ability to support critical infrastructure in identifying and responding to cybersecurity incidents, especially in light of the new SRMA requirements.
- **Outreach and Services** - Funding to support targeted outreach, such as low-overhead simulations, and sector-tailored services will enhance connectivity with the broad pool of stakeholders that shape national cybersecurity—actors like municipal service providers and state and local governments. These investments are multiplicative in that they also increase the effectiveness and utilization of the technical services and security assessments that CISA already offers.
- **Expanding Federal Network Resilience** - Congress has recently made significant down payments to improve visibility across civilian networks; however, these investments are insufficient to reach across the entire Federal .gov domain. Additional resources will ensure that CISA, through the Continuous Diagnostics and Mitigation program, can more quickly deploy necessary tools.
- **Enabling a Secure Ecosystem -** CISA is responsible for increasing operational resilience in the non-federal space by driving secure behaviors and secure-by-design planning across the national cyber ecosystem. CISA has the structures and programs in place to achieve this impact on national cyber defense, but it needs funding for program personnel and physical space and equipment to allow its teams to grow into this role.
- **Cyber Response and Recovery Fund** - The proposed FY22 budget for CISA includes $20 million for a Cyber Response and Recovery Fund. This fund, which is itself based on a

[7] Pub. L. 117-2. Section 4009 provides $650 million for CISA.

recommendation from the Solarium Commission,[8] is vital to ensuring that incident response capabilities can be brought to bear rapidly to assist non-Federal partners, particularly state, local, tribal, and territorial governments.

In order to make any of these appropriations considerations possible, a required first step is to increase CISA's 302(b) allocations for FY22 to allow CISA to grow and meet its legally required mandate. The large majority of funding for CISA's critical cybersecurity functions comes from the National Defense Budget Function (050). In FY20, only $69.4 million of the just over $2 billion in total funding for CISA came from functions other than 050. That number saw a modest increase in FY21 to $83.5 million, while $1.94 billion was enacted from 050 funding.

We estimate that funding appropriated to CISA will need to grow from just over $2 billion included in the Consolidated Appropriations Act for FY21 to no less than $2.425 billion for FY22. This is despite the fact that total budget authority for FY21 and FY22 will be higher than regularly appropriated amounts due to ARPA funding. In addition to expected increases to base funding due to normal maturation at the agency, expansions to the agency's role due to new authorizations and as a response to emerging cybersecurity incidents place new funding requirements on CISA. **We recommend an increase of at least $400 million for the FY22 appropriation to respond to these changing requirements.**[9] This would mean the overall 050 allocation to the Subcommittee on Homeland Security would increase from $2.551 billion, as specified in the FY21 appropriations agreement, to no less than $2.951 billion for FY22. It is worth noting that cost escalation in the U.S. Coast Guard and Federal Emergency Management Agency portions of the 050 funding — as well as the need to recapitalize Coast Guard assets — will likely necessitate an even greater increase in the national defense budget function allocation.

Figure: CISA Budget Authority by Fiscal Year

(In 1,000s)	FY20 (enacted)	FY21 (enacted)	FY22 (proposed)
CISA Appropriations	2,015,622	2,024,978	2,134,978
ARPA - One Time Pro-rated per month 1Apr21-30Sep22		216,667	433,333
CSC Recommendation			290,000
CISA Total Budget Authority	2,015,622	2,241,645	2,858,311

Looking into the future, CISA will incur further funding requirements for FY23 in order to sustain new federal network resilience efforts. While some of the activities enabled through ARPA funding will be one-time capital investments and discrete projects that will end by FY23, many of the most impactful

[8] Solarium Recommendation 3.3 - Codify a "Cyber State of Distress" tied to a "Cyber Response and Recovery Fund"

[9] President Biden's discretionary funding request for Fiscal Year 2022 includes an increase of $110 million for CISA. While this is an important start, it is wholly insufficient to address the many capacity and capability gaps CISA continues to face. The FY22 increase will not cover the extension of capabilities fielded in response to SolarWinds across the Federal government, much less the urgently needed growth in the non-Federal mission set.

expenditures — which we estimate could amount to $200-250 million — will require sustained funding in order to maximize the benefit to national security. Spending in future years will be further shaped by the need to sustain these new efforts to secure federal civilian networks.

Without increases to the 050 302(b) allocation for the subcommittee, determining appropriations for CISA in the coming fiscal year would be an exercise in limiting damage to existing programs while triaging new responsibilities, and CISA would fall far short of the strong and effective cybersecurity agency the U.S. badly needs. Congress has very wisely chosen to expand and reinforce CISA's role in protecting the nation against ever-growing cyber threats. The Homeland Security Subcommittee needs an increased 050 302(b) allocation to reflect the growing importance of a resilient and secure cyberspace on American lives and livelihoods.

Thank you for your consideration of these requests.

Mike Gallagher
Member of Congress

James R. Langevin
Member of Congress