Testimony Before the House Appropriations Subcommittee on the Legislative Branch, FY 2027, Concerning Enhancing Cybersecurity Support for House Staff through the House Chief Administrative Officer and Sergeant at Arms

Dear Chair Valadao, Ranking Member Espaillat, and members of the House Legislative Branch Appropriations Subcommittee:

Thank you for the opportunity to provide written public witness testimony. We commend the Committee's ongoing commitment to strengthening congressional operations and addressing critical security challenges facing the Legislative Branch. We respectfully request that the Committee direct the House Chief Administrative Officer, in coordination with the House Sergeant at Arms, to provide voluntary cybersecurity support, training, and security tools to help congressional staff secure their personal devices and accounts.

We submit this testimony on behalf of three organizations with a strong interest in congressional security and institutional effectiveness: Daniel Schuman, Executive Director, American Governance Institute; Haiman Wong, Resident Fellow, R Street Institute; Sean Vitka, Executive Director, Demand Progress Action.

Our testimony today concerns the essential need to enhance cybersecurity support for congressional staff, particularly for their personal devices and accounts. The Committee has rightly recognized the critical importance of robust cybersecurity practices across the Legislative Branch and endorsed continuous improvement.

Senate Appropriators recently directed the Senate Sergeant at Arms to improve personal cybersecurity advisories and best-practice guidance tailored to personal devices and accounts and to educate Members and staff. The Senate Sergeant at Arms was also encouraged to explore options—including options from the bipartisan Senators' Personal Cybersecurity Working Group's report—to provide voluntary cybersecurity assistance to Senators for their personal devices or accounts.

We support the House providing similar support to representatives. Furthermore, we would encourage more to be done to provide dedicated, practical personal cybersecurity support specifically for *congressional staff*.

Members of the House and congressional staff are valuable targets for malicious actors seeking to compromise the institution. Adversaries understand that staff members possess intimate knowledge of legislative processes, constituent issues, political

strategies, and sensitive communications. Moreover, the threat landscape is changing rapidly thanks to emerging technologies like AI, increasing the potency of cyber threats.

Compromises of staff in their personal capacities pose a grave danger to the actual work of Congress for several reasons:

- *Access to Sensitive Information*: While official work should occur on official systems, in practice, personal devices and accounts may be used for work-related communications, scheduling, or accessing documents, particularly when staff are mobile or working remotely. A compromised personal email account, for instance, can expose sensitive information.

- *Phishing and Social Engineering Vector*: Attackers frequently use personal information gathered from social media or compromised personal accounts to craft highly convincing spearphishing[1] or whaling attacks targeting staff. These attacks can trick staff into revealing credentials for official systems, clicking malicious links, or sharing confidential information.

- *Network Mapping and Intelligence Gathering*: Information gleaned from personal devices and online activities can help adversaries build profiles of staff, understand their connections (to Members, other staff, constituents, lobbyists), identify their routines, and gain insight into office dynamics or legislative priorities. This intelligence can then be used to tailor more effective attacks against the staffer or those they support.

- *Lateral Movement*: A compromised personal device or account could potentially be used as a stepping stone to access official systems if staff use the same or similar passwords, or if the personal device connects to the official network without sufficient security hygiene. While official networks have defenses, personal security hygiene is a critical layer.

- *Disruption and Coercion*: Compromising a staffer's personal accounts can be used for harassment, doxing, or even coercion, creating significant stress and distraction that hinders their ability to perform their official duties effectively and securely.

[1] Phishing is a form of social engineering used by intruders to gain access to information and systems. Spearphishing targets specific individuals, while whaling targets senior officials.

Essentially, the personal cybersecurity of staff is inextricably linked to the institutional security of the U.S. House of Representatives and its ability to function securely against sophisticated threat actors.

The good news is that a handful of basic, practical steps can dramatically increase personal cybersecurity for staff. These steps are well documented and include using strong, unique passwords managed through password managers; enabling multifactor authentication (MFA) on personal accounts; and using secure communications tools where appropriate. Providing staff access to password managers, hardware security keys, and similar tools—paired with training—would significantly strengthen the security posture of the House workforce.

While the House already provides some training on these topics, especially for those traveling overseas, making these practices widespread and providing necessary tools requires going further than providing advisories. Some staff members may lack the personal resources or technical expertise to implement these security measures effectively on their own – or merely need a push to do so. Providing free or low-cost access to tools like password managers, hardware security keys, or subscriptions to secure communication services would remove financial barriers and significantly enhance the security posture of the entire House community.

The cost of widely deploying password managers or hardware security keys is modest relative to the potential institutional risk posed by compromised staff accounts.

Accordingly, we respectfully request the Committee:

- *Direct the Chief Administrative Officer, in coordination with the House Sergeant at Arms, to establish a program providing voluntary cybersecurity support to Representatives and congressional staff for their personal devices and accounts*. This program should include tailored advice, training sessions focused on personal cybersecurity best practices (drawing on resources like those outlining password managers, MFA, and secure communications), and guidance on implementing basic security measures.

- *Provide sufficient funding for the Chief Administrative Officer, in conjunction with the House Sergeant at Arms, to procure and provide staff with free or heavily subsidized personal cybersecurity tools and resources*. This could include licenses for reputable password managers, hardware security keys, or access to secure communication platforms. These tools are essential complements to

training.

- *Include legislative language providing clear legal authority for the Chief Administrative Officer and House Sergeant at Arms to offer this personal cybersecurity support and provide these resources to staff*, explicitly stating that such support and resources are not for campaign purposes. This clarifies the permissible use of official resources for bolstering the overall security environment of the House workforce.

These steps represent a critical investment in the security and resilience of the House of Representatives by addressing a currently underserved vulnerability—the personal cybersecurity of the dedicated staff who are essential to its operations. Protecting the personal accounts and devices of congressional staff is not merely a matter of privacy; it is a matter of national security and the effective functioning of our legislative branch.

Thank you for your consideration of these important recommendations. We welcome the opportunity to discuss them further with the Committee.