Testimony of Rep. Anna G. Eshoo

Member Day Hearing
House Committee on Administration
1310 Longworth House Office Building
November 21, 2019

Chairperson Zoe Lofgren, Ranking Member Rodney Davis, and Members of the Committee, thank you for the opportunity to testify today before the House Committee on Administration.

Because of the nature of our work, the House of Representatives attracts all types of cyber adversaries—hackers, criminals, and agents of foreign countries—who post real risk to our work and to our country. I thank this Committee, the Chief Administrative Officer (CAO), and your staff for the critical work you do day in and day out to secure official House servers, systems, and devices from cyberattacks.

However, I remain concerned that the digital activity of Members of Congress and our staff on personal devices and personal accounts represents a significant vulnerability for the House that is not currently being addressed. Although official business is conducted on House-managed devices and accounts, personal devices and accounts still represent significant cyber vulnerabilities for the House. For example, if an employee's personal cell phone is compromised by an adversary, that employee is likely carrying that compromised cell phone in official meetings where it could turn into a surveillance device. In today's highly connected world, we must begin to think of personal devices and accounts as risks to the House since these devices are with us 24 hours a day.

To address this issue, I request that the Committee authorize the development of a mandatory list of cyber hygiene best practices that are effective, user-friendly, and tailored for personal devices and accounts of individuals in the House community (including Members, Delegates, the Resident Commissioner, officers of the House, and all employees of the House). This list should include general best practices, such as the use of two-factor authentication and password managers, regularly patching software and operating systems, turning on screen locks on all devices, and using House-approved encrypted messaging services, in addition to any House-specific practices you recommend. As cybersecurity protocols and best practices are constantly evolving, this list should be regularly updated and widely distributed.

I also request that CAO staff be available to assist individuals in the House community in implementing the above best practices to secure their personal devices and accounts, including smartphones, computers, laptops, tablets, social media accounts, and email accounts. Assistance from CAO experts would provide those who are less familiar with cyber hygiene with the support they need to take essential steps to secure their online activity.

Chairperson Lofgren and Ranking Member Davis, I respect your strong leadership of this Committee, and I have confidence in your ability to mitigate cyber risks the House faces. If I can be helpful in your efforts, just let me know.