No American institution is better situated to address the national need for improved civilian cybersecurity as is Congress. As the legislative branch of government, Congress is responsible for creating the country's laws and one half of Congress – the Senate – must ratify international treaties. Not only does Congress provide Executive agencies with authority to act and regulate, it also controls the appropriations necessary to take action. Without these authorities and funding, the executive branch would be unable to address emerging risks posed to American civilian computer systems by connected technologies and systems. While these risks – described more fully in the first article of this series – can be mitigated through international action and cooperation between the various stakeholders, Congress has the ability to create the most substantial and lasting impact.

Congress has already recognized the urgent need to improve the nation's cybersecurity, however, more action is necessary. Providing more funding, some new authorities, and even creating a new Senate confirmed position, only do so much to make up the gulf between where the nation's cybersecurity posture was and where it needs to be. To start, the nation's division of government – federal, state, and local – provides a significant challenge in that there are not only multiple vectors to attack but that funding between states and localities can differ tremendously. Congress can address this by not only continuing to provide funding to states and local governments to improve their cybersecurity – as it has done, for example, in the COVID relief bills – but also by authorizing the Cybersecurity and Infrastructure Security Agency (CISA) to issue grants to state, local, tribal, and territorial (SLTT) governments. As the agency with the most interaction with SLTT governments, CISA has more insight into the specific needs of each while also possessing the subject matter expertise to prioritize among their needs and to assess how much funding will be needed to achieve each project's goal.

While Congress has taken some action to address the dearth of cybersecurity professionals in the federal government, it has also created a framework with overlapping authorities and no clear hierarchy of authority to address duplication and conflicts. Creating a system with some redundancy can be effective but creating such a system and leaving uncertainty as to who is to take the lead on what can do more harm than good. Moreover, these redundancies are likely to exacerbate the shortfall in cybersecurity professionals that the government and wider industry already face. Programs like the CyberCorps: Scholarship for Service can help to close the gap, but graduating only a few thousand students over a nearly twenty year period is insufficient to fill the tens of thousands of federal cybersecurity job vacancies. Congress must therefore take action to clarify the roles and responsibilities of the various federal agencies with parts to play in the nation's defense of its civilian networks. Congress must also urgently take action to train a workforce to fill the nearly 1 in 3 cybersecurity positions that are currently unstaffed. To achieve this end, Congress can also improve the diversity of thought in the field by creating additional funding and hiring programs targeted at diverse communities. By creating a workforce with diverse backgrounds, both demographically and academically, Congress will empower the cybersecurity profession to consider new points of view. These additional insights are critically important in a field that must constantly and continuously evolve in defending against new and emerging threats.

Laws like the Federal Information Security Modernization Act provide federal civilian agencies with subject matter expertise to help improve the cybersecurity posture of the federal

government; however, there are very few national laws that provide meaningful requirements as to private civilian cybersecurity. While laws like the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act provide some cybersecurity minimum standards, they do so only for specific industries. These sectoral laws also fail to provide significant guidance as to what the minimum standards require. While different industries may require different levels of protection – the discussion as to which is better, sector-specific laws or general regulation, requires its own, in-depth discussion – Congress can still act to set minimum standards nationally or to assign an executive agency with subject matter expertise the regulatory power to set specific requirements. After all, American civilian computer systems are reliant on a diverse and intricate network. Addressing only specific entities will not adequately manage the universe of relevant actors even within specific industries.

Congressional action is necessary under the United States' Constitution for many of the reforms needed to truly modernize the nation's cybersecurity posture. Private industry is free to take action without Congress, however, private companies are driven by market forces which have historically been inadequate to provide sufficient security. The Internet of Things is perhaps the best personification of this problem – security tends to be an afterthought in the drive to bring products to market quickly and cheaply. No federal agency currently has the necessary authority to enact widespread and substantial change nor can any SLTT government impose national mandates. Congress must act, and act soon, to address the risks posed to American civil computer systems by connected technologies and systems.