The modern Internet has wrought tremendous changes in the world; allowing individuals to connect easily across continents, business to be conducted in innovative ways, and for nearly instantaneous access to formerly unimaginable stores of information. With all of the changes, the Internet has also altered the landscape of risk – allowing for new opportunities and exposing individuals and groups to novel threats. The world has been quick to adopt the Internet and its attendant technologies but has not always considered what steps would be necessary to prevent or even mitigate these new threats. While there were previously warning signs, the past few years have highlighted the dangers individuals, and society at large, face if we continue to fail to address these threats.

The world now relies on the Internet of Things to watch over and secure their homes; hospitals and cities store their essential data digitally, either locally or in the cloud; and utilities rely on industrial control systems to maintain service over vast geographic areas. While these changes have improved the lives of many, security is too often a secondary thought – if that. Both hospitals and cities have repeatedly been the victims of ransomware attacks. Utilities, including water treatment facilities and electric grids, have been the focus of cyber-attacks. Even our homes have suffered the consequences of inadequate security. These trends are unlikely to reverse course and may intensify if COVID-19's effect on remote work lasts.

Immediate action is necessary to improve the cyber defense of the United States. To that end, this is the first article in a series which will evaluate what can be done to reduce the risks posed to American civilian computer systems by connected technologies and systems. In doing so it will consider what steps can be taken and suggest reasonable steps that can be taken by different governmental bodies as well as actions that private industry should consider taking on their own. Some changes can be implemented in a top-down approach where laws or regulations force new behaviors. Other improvements will require cultural changes such as recognizing the value of secure products even if might cost more or in improving cyber literacy. These actions will take time to have their full effect and no one action can sufficiently reduce risk; however, taken together, these actions will reduce the staggering financial and national security costs of cyber-attacks.

While the threats posed by a failure to act are very real, it is important to remember the goal of information security. It is not to remove all threats by stopping any and all risky behavior. Instead, information security should seek to minimize reductions in functionality as it maximizes risk reduction. This equation does have a real up-front cost. Put simply, it costs more to add security controls to devices, systems, and programs. It will take time and effort to better educate individuals and organizations about good cyber practices. Unfortunately, these costs are not one-time expenses either. Importantly, however, these costs do pay dividends by saving companies money, securing the well-being and personally identifiable information of individuals, and by better protecting national interests and perhaps even constitutional rights.[1] By investing in these changes early on, the United States and its constituent individuals and organizations will reduce long-term costs and mitigate unforeseeable harms.

[1] The author, Kelsey Cora Skaggs, describes the effects of government surveillance on user behavior when they know they are being observed. This same effect is possible, perhaps even likely, when unknown malicious attackers are known to infiltrate and misappropriate specific systems.

The Internet is a global network of interconnected devices. As such, reducing risks posed to American civilian computer systems by connected technologies and systems will require international agreements in addition to any national efforts. It would be naïve to suggest that all nations will agree to simply cease the use of cyber weapons and deter individual actors from operating across borders. Yet there are some areas where improvements are possible and where international cooperation can be achieved. Successful international alliances, like NATO, have incorporated cyber defense into their understanding of collective defense. The United States also has extradition agreements which allow criminals, including cyber criminals, to face justice in the jurisdiction where their crimes were committed. These steps are necessary to America's cyber risk reduction efforts, but they are not sufficient.

While collective defense agreements can deter nation-state cyber-attacks, the rapidly evolving landscape of information security makes it very difficult to not only attribute who has taken what action – a prerequisite to lawful self-defense – but also to define what even is a cyber-attack. Data exfiltration, reconnaissance efforts, even destructive malicious acts are relatively routine and are generally not considered acts worthy of an armed response. These acts though do not take place in a vacuum; a ransomware attack on a hospital might lead to death or data exfiltration and publication could be seen as interfering with a state's internal governing. Different governments and leadership personalities may make a substantially similar act in one country result in a wholly different response. While this is somewhat true with traditional arms as well, and countries have certainly manufactured reasons to attack, there are still laws that prohibit these actions. These prohibitions create a deterrent, but also allow a range of retaliatory action from non-involved nations to punish the wrongdoer. Calls for international agreement on a set of similar rules in cyberspace are not new, but the problem is likely to only worsen without some established rules.

International Agreements govern nation state action and, in many instances, malicious cyber acts come from sub-state actors. While proxy groups for nations can be dealt with under the umbrella of state action, unaffiliated groups such as terrorist organizations and criminal syndicates pose a more difficult agreement. Unaffiliated groups are rarely parties to international agreements and, even in situations where such groups might be involved, not all malicious groups would be covered. These groups pose additional difficulties in that they operate from countries that may simply ignore the problem or are unable to respond to the issues themselves. Extradition and law enforcement assistance provide some help in resolving these issues, as does coordinated law enforcement action. More, however, is needed to reduce risk to an acceptable level for American civilian computer systems.

Countries should consider international agreements that promote cyber resilience by sharing best risk reduction practices. International trade agreements could also be used as a tool to improve information security by offering lower tariffs to goods that meet an established baseline. Given the shortage of information security professionals nationally and globally, the assessment of new goods might be left to a trusted international organization. By lowering tariffs in this manner countries will not only reduce the price of secure hardware for consumers, but manufacturers of these products will also have an incentive to spend more on secure designs now rather than face higher tariffs down the road. Secure software is more difficult to incentivize via tariffs given online availability, however, countries can promote visa expeditions for software security

positions. Moreover, to reduce the risk of malicious personnel, governments might consider mandating security checks for sensitive positions being filled by foreign actors. As this will impose a cost on the security investigator, government financed investigations or other financial offsets can be implemented to reduce any added burden.

Information sharing agreements can also be used between trusted partners to alert parties of newly discovered vulnerabilities. Though this has limited application to scenarios where the vulnerabilities are not publicly exposed, additional cooperation will reinforce or build trust. These information sharing agreements can also be used among trusted partners to help with attributions for malicious acts by building a shared library of cyber incidents and known actor information. This would allow faster, more certain attribution and therefore improved responses. The library may also assist stakeholders to build more resilient systems.

A strictly national solution to this international problem is unlikely to adequately reduce the risks the United States faces. While international agreement can take some time to build, by working towards these ends now, nations will be better equipped to address the problems of today and tomorrow. By focusing on reducing the risks posed by a multitude of actor types, countries can better protect not only their national security but also that of their civilian computer systems. Working with our partners and allies, while also building international agreement on norms of behavior, is a critical component to securing connected American civilian computer systems.

Reducing the risks posed to American civilian computer systems by connected technologies and systems – as described in the first article of this series – will require more than one entity taking action. As mentioned in the second article, even international governments taking cooperative steps towards establishing cyber norms and promoting information sharing among allies will only do so much to mitigate the threats posed to civilian networks – including American civilian networks. More is needed. To that end, all levels of government and industry will need to work with each other and with other partners such as universities and research and development centers. These partnerships can utilize industry subject matter experts to better understand the technologies and capabilities that companies have at their disposal. Government specialists can serve as information hubs which collect and disseminate information on industry threats and best practices. Moreover, the government is capable of implementing a wider range of deterrent and response actions to include prosecuting cyber criminals and imposing economic sanctions. Rather than being mired in responding to incidents as they occur, research and development centers are excellent resources to consider long-term, big idea problems and solutions. It is only with largescale, coordinated action that the daunting scope of the threats discussed in this series can be addressed.

There has been some recognition within the United States of the need for such coordinated action to address these threats. For example, Congress established a Cyberspace Solarium Commission in its National Defense Authorization Act for the fiscal year 2019. The Commission includes stakeholders from government, the private sector, and academia and has achieved some success in spurring action. Yet the Commission is far from enough. In the time since the Commission has been created, new and pressing issues have continued to arise at a pace that it cannot keep apace of. From building out the nation's 5G networks securely to continuously improving responses to data breaches of private and public sector organizations, more robust coordinated action is needed. One shortcoming of the Commission is its inability to *require* changes. The recommendations made by the Commission are just that, recommendations. Government agencies, like the Cyber Security and Infrastructure Security Agency ("CISA"), are tasked with securing the nation's cyber infrastructure but are also largely limited to recommending changes to private organizations. Requiring specific action is likely untenable given the myriad organizations and their diverse capabilities; however, providing additional resources to aid organizations looking to improve their security coupled with increasing the liability for poor security practices could provide a working "carrot and stick" method of raising the baseline security posture of the nation's civilian cyber infrastructure.

Private companies enacting change at an organizational level will help reduce cyber risk but increasing individual knowledge of these risks and how to mitigate them is also necessary. Cybersecurity training programs within companies are one method to improve each organization's security within specific systems while likely offering some benefit to individuals in their personal lives. Funding for education programs for K-12 students will help improve cyber literacy generally and provide a higher baseline from which to continue risk mitigation education. Additional funding to universities for cybersecurity education, even as a general education course for various majors would help improve the national risk posture. The funding could also result in filling the millions of open cybersecurity roles and providing additional resources for research. Providing additional resources for research and development might help get the nation out from behind the curve and able to better anticipate coming challenges.

Improved cyber literacy might also increase the government's ability to keep pace of technological challenges rather than relying on laws created decades ago with few updates provided over that time.

Building public-private partnerships helps maximize the utility of the country's cybersecurity knowledge and expertise. Collaboration across the national landscape not only provides a diversity of thought, it also builds a sense of engagement. By investing time and resources into cooperative agreements and projects, each party will have a better sense of how the outcome will affect them and be able to provide valuable input into the effort. Reducing the risks posed to American civilian computer systems by connected technologies and systems is not a project that can be accomplished alone; it will require nationwide – and international – input and cooperation.

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.

As the arm of U.S. government tasked with faithfully executing the laws passed by Congress, the executive branch is responsible for ensuring that all laws – such as those proposed in part four of this series – are given effect. To that end, executive agencies are responsible for prosecuting cybercrimes, representing the United States in negotiating cyber agreements and treaties, and, to the extent that cyber actions constitute armed conflict, responding with military force. The President, therefore, has a greater ability than any other individual to influence the nation's reduction of risks posed to American civilian computer systems by connected technologies and systems.[2] While part four of this series noted additional legislation and funding that would improve the nation's cyber risk posture, the executive branch already has significant tools at its disposal to accomplish this end. Some changes, however, are needed to maximize the benefit of already existing authorities and functions.

The President, in addition to authorities granted to the office by Congress, has at his or her disposal the ability to set – or at the very least influence – the country's national priorities. When, as is the case at the time of this article's publication, the President's party controls both chambers of Congress, this power to influence is at its zenith. Given the pressing risks posed today,[1] the President should place additional emphasis on improving the nation's cyber risk posture. This can be accomplished a number of ways. In addition to requesting legislation be drafted, the President has the responsibility of proposing a budget for each fiscal year. While Congress is not required to accept the budget proposal, the President is able to highlight his or her priorities. Moreover, the President is able to veto the budget passed in Congress if it fails to satisfy those priorities. While the tradeoffs of taking such a forceful action must be well considered, the President can use this power if necessary or even as a lever of negotiation.

Currently, however, the President has an additional vehicle for which to make improving the nation's cyber risk posture a priority – his $2 trillion infrastructure plan. Using this plan fits in a number of ways. First and foremost, much of what the plan hopes to achieve is technology based. For example, $100 billion is proposed for improving the nation's power grid with another $100 billion for improving high-speed broadband access. Both of these priorities would benefit greatly from spending at least some of the proposed funds on securing and making more resilient the networks used. While the bill is certain to face political fights, cybersecurity – and national security more generally – is somewhat less controversial. Even with unified political control, the Senate requires 60 votes to overcome a filibuster. Additionally, crafting bipartisan laws should, at least in theory, help improve bills by including a diversity of thought. Perhaps most importantly, however, less controversial bills are more likely to gain buy-in. Including a cybersecurity purpose is unlikely to change the minds of many lawmakers, but it may prove beneficial in gaining national support.[3] Additionally, providing additional funding for cybersecurity makes sense from a risk reduction perspective. Building security into existing devices can be a significant challenge but building the networks with security in mind helps "bake in" security throughout the device lifecycle.[4] If President Biden's infrastructure plan is

[2] For more discussion on and analysis of these risks, please see the first article in this series.
[3] While this poll focused primarily on ransomware attacks, it did note that 61% of Americans would support an increase in the federal income tax to help fund government efforts to defend against cyber-attacks.
[4] The link discusses DevSecOps in the context of software security. This same concept can be utilized in the building of physical networks as well as choosing what software to use on the networks.

passed, even if it is a smaller version than the one proposed, it should include a portion of the funding for improving each of the bill's proposed project's cybersecurity.

While certainly helpful in improving the nation's risk posture, action cannot be limited to only new projects. One area where the executive branch can help address existing cybersecurity (?) risks is to provide further grant opportunities through the Department of Homeland Security's Federal Emergency Management Agency. Some of these grants already have a cybersecurity nexus but more appropriations should, to the extent permitted by law, be used to combat cyber threats. Additionally, FEMA can make use of the cybersecurity expertise of its fellow DHS agency, the Cybersecurity and Infrastructure Security Agency (CISA). While FEMA would be the granting agency, as required by law, CISA can work with FEMA to identify areas where improvement is most needed and help to ensure that the funds are used as efficiently and effectively as possible. If Congress were to act and give CISA grant authority, as suggested in the fourth article of this series, CISA could benefit greatly from FEMA's expertise on grant management. In sum, the executive branch must make use of its existing grant authorities to address the nation's most critical risks.

The President should not feel limited to charting this new course with only domestic actions. As discussed in the second article of this series, international efforts are also needed. The President is able to enter into executive agreements without Congressional action, however, more active or binding measures would require Senate approval. The needs of this moment require that international efforts be taken in conjunction with domestic action. Moreover, Presidential direction and executive agency action is needed immediately to reduce the risks posed to American civilian computer systems by connected technologies and systems. At a time of unified government, even if only narrowly so, the moment must be seized to improve the nation's cyber risk posture.

Improving the United States' civilian cyber defense posture requires action from both the public and private sector. The government can and, as earlier articles in this series argue, must take action to incentivize and require increased cybersecurity measures. However, while the government can work to secure its own systems, by its very nature the Internet is an interconnected network. These connections cross between government systems into private networks and back again. To compound this, government networks are themselves made with privately sourced components. Private entities must therefore take ownership of the risks posed to their systems and share in the responsibility to defend against these risks. By addressing vulnerabilities, these entities not only benefit their customers, they also secure their intellectual property, protect their sensitive employee data, and promote the interests of their shareholders or other stakeholders.

One proven method of reducing risk is through organizational investment in training programs. Organizations like (ISC)^2 and CompTIA provide trainings and certifications to better prepare security professionals to address threats. Companies should look to utilize these opportunities to improve their organizational knowledge by investing in their workforce. The return on investment of such investments can be hard to measure – as are most investments in revenue negative components like security – however, organizations can look to improve their returns by offering education incentive agreements. Both the organization and the individual employee can realize benefits when companies offer their employee a free or reduced cost certification in exchange for an agreement to continue working at the organization for a set period of time. Organizations interested in maximizing employee retention might also consider coupling these agreements with other incentives to reflect the employee's improved ability to accomplish their assigned tasks. The improvements realized by these programs increase organizational security knowledge which in turn helps to reduce the risks posed to American civilian computer systems by connected technologies and systems.

Private companies must also look to increase their cybersecurity workforce. Training a competent staff is essential, however, the shortage of cybersecurity professionals discussed in the fourth article of this series is also having a serious effect on the private sector. While this need is being addressed somewhat – (ISC)^2 recently noted an additional 700,000 new cybersecurity professionals in one twelve-month period – it is still woefully shy of the estimated number needed to address the talent gap. Scholarship opportunities in exchange for an agreement to work are one tool that may work in the private sector as well; however, salaries for private sector cybersecurity work is already relatively high. As such, additional pay-based incentives may have diminished returns. One alternative, hiring from non-traditional academic programs such as a liberal arts degree or even from the industry workforce the security team is protecting, might be a more effective action. In addition to expanding the applicant pool, a diversity of thought and background can be invaluable when assessing and preparing for the ever-evolving risks cybersecurity professionals face.

Reducing cybersecurity risks is not only dependent on hiring and training a competent workforce, companies must also reevaluate how they prioritize security and profit. This can be a difficult change to make, especially when so much of business is driven by the demands of the market. Improving the security of devices, software, networks, and more does cost more and it is likely, if not certain, that some of these costs will need to be passed along to consumers. In some

markets, especially those that are very price sensitive like Internet of Things devices, these additional costs present added difficulties in the market and sale of products. Still, as new laws go into effect, such as California's Consumer Privacy Act (soon to be replaced by the California Privacy Rights Act), the cost of insecurity is likely to rise. Building a reputation for security now may help provide a competitive advantage early. Moreover, as more and more of the world's market considers the effects of insecurity, stockholders, regulators, and others become increasingly likely to see the business necessity of securing consumer devices. For companies purchasing hardware, software, or services, insecure devices may be cheaper at the time of purchase, but they carry additional risk and unforeseen future costs. This has been made all the more clear with recent cyber-attacks, especially the rise in ransomware attacks and supply chain incidents. As a result, companies must evaluate the cost of insecurity against their profitability, increased liability, reputation, and other market factors.

The size and nature of business should be considered against the specific needs of each individual company. While large companies in sensitive industries will require significant investment, small companies in non-sensitive industries may have reduced needs in addition to their smaller budgets. In this way, there is not one-size-fits-all security framework for private companies, however, private industry has a responsibility to improve upon their current security posture. Failure to do so is not only likely to result in harm to their organization, it is also likely to continue contributing to unnecessary and unacceptable risks. Mitigating these risks will help protect their companies and reduce the risk posed to their networks as well as the broader connected Internet.

As this series has tried to emphasize, a variety of players can have a direct impact in reducing the risks posed to American civilian computer systems by connected technologies and systems. While the specific actions available to each group or actor differ, all share in the collective risk and conversely, stand to benefit from the positive changes made by others. In this way, much like the Internet itself, all the parties are connected to one another. Even international organizations and friendly foreign nations stand to benefit from a more secure American civilian network. The proposals highlighted in this series provide a general roadmap to achieving this improved cybersecurity posture, but it will take decisive action by the actors discussed to make it a reality.