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.[1] 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.[2] 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.[3] If President Biden's infrastructure plan is

[1] For more discussion on and analysis of these risks, please see the first article in this series.

[2] 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.

[3] 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.