The Honorable Michael J. Rogers
Responses to Questions for the Record
Committee on Oversight & Reform Hearing, 15 July 2020

Questions for the Honorable Michael J. Rogers Former Member of Congress Questions from Chairwoman Carolyn B. Maloney

1. As we discussed during the hearing, a key responsibility of the National Cyber Director would be to establish and implement a National Cyber Strategy.
    a. Can you expand on how the National Cyber Strategy required by H.R. 7331 would be different from the 2018 National Cyber Strategy currently in place? What key elements do you recommend for inclusion?

It is less about how the strategy would be different and more of how it will be implemented. Right now, in the absence of a National Cyber Director, the cyber strategy is a well-thought-out, but ultimately hollow document. It offers but does not mandate, guidance. The National Cyber Director would coordinate the budgets, ensure that they are aligned against the strategy, and with the power of the purse direct federal agencies and departments to adopt better (and ideally best) practices. To truly be effective the National Cyber Strategy needs to look at the challenge as whole-of-government and whole-of-nation.

In the case of the former, this means coordinating across all agencies and departments and raising standards and practices from the lowest common denominator. It will do us no good to have the National Security Agency at one level and the Department of Health and Human Services at another—both have critical missions and invaluable sets of data. In the case of the latter, we need to build an ecosystem of cooperation between the government and the private sector that goes beyond merely customer and client, but to one of a partnership. The private sector is leading the way on cybersecurity innovation and development, and Washington must leverage this progress if it is to protect citizens' data and prepare for the future.

    b. Would development, implementation, and oversight of the National Cyber Strategy as required by H.R. 7331 advance the current Administration's policy goals concerning China? If so, how?

The National Cyber Director would enable the White House to have a single office and individual charged with overseeing and coordinating the country's cyber defenses—something that is missing today. By empowering this office and mandating that it align the budgets against a stated and defined strategy, we will work to close off a major systemic vulnerability to our country's federal cyberinfrastructure. Right now, there are duplicative programs, wasted spending, and outdated equipment and software, all of which are ripe for exploitation by China.

If we correct this, while building for the future threats and opportunities, we will narrow a potential attack vector. Note that this is not an issue of "closing" but "narrowing"—in the cybersecurity realm, it is an ongoing cycle of attack and defense, one in which we will never be 100% secure. This budgetary and organization alignment will also send a signal to the private

sector, setting standards for best practices that will, ideally, have a follow-on effect to boost the overall cybersecurity posture of the country.

c. Your testimony describes how China and Russia are aligning their budgets to pursue their goals of digital, 5G, and artificial intelligence dominance. What will happen if the U.S. fails to align its cybersecurity priorities and budgets around common strategic goals?

Russia and China recognize the value of taking the lead and attempting to dominate advanced technologies. This was something the United States understood but has since become complacent about at a national-policy level. Our entrepreneurs are still unrivaled, globally, but that is despite, not because of, Washington. If we fail to align our budgets and pursue a concerted, focused strategy on AI and next-generation technologies, we will cede the advantage to Moscow and Beijing.

The resulting impacts will be significant—we will lose the competitive edge militarily, economically, and politically. If we fail to align our cybersecurity budgets to a coherent strategy, we will find ourselves in an increasingly perilous and vulnerable position. We will waste time, energy, and resources attempting to correct the mistakes and vulnerabilities of previous generations of software and hardware, and be ill-equipped to address the threats of today and tomorrow.

2. China is playing an aggressive role in setting international standards for new technologies, which can substantially impact which countries most benefit from them economically and strategically. In 2013, the Chinese government committed resources and attention to actively coordinate across its government and with industry on early 5G development standards. The government also provided state support to companies like Huawei to speed research and development toward early patents, which can often inform the foundations of subsequent technical standards. By early 2019, Huawei led the world with more than 1,500 of these "standards-essential patents" for 5G technology.
    a. How has Huawei's dominance in 5G technology fundamentally reshaped America's national and economic security?

Huawei has radically reshaped the national and economic security landscape. For the first time in history, you've seen a company backed by the power of a nation-state corner the market for next-generation technology. They've done this by outright theft, corporate espionage, violation of sanctions, money laundering, and other illegal and unethical practices that would have seen any American, British, or German company shutdown. By using the financial largess of the Chinese Communist Party, Huawei undercut competitors' prices and driven them out of the industry leaving them one of the few remaining players in a critical next-generation industry.

While we first warned about this threat in 2012, it has taken the intervening years for the country and our allies to wake up to what Huawei is and what it represents. I'm pleased to see that the FCC under Chairman Pai has worked to aggressively open up the spectrum for 5G development and that the Administration has worked to ensure that Huawei and ZTE equipment is not allowed onto (or is removed from) our country's communications infrastructure. This

threat is far from over, but we are finally taking the right steps forward to preventing China from dictating our future.

b. How could the National Cyber Director reverse these trends and contribute to the establishment of more fair and favorable international standards?

The National Cyber Director must be part of a broader diplomatic effort to ensure that the United States is well represented at standard-setting international governing bodies. We have, sadly, allowed our engagement and participation to atrophy, thereby allowing the Chinese Communist Party to bully and buy their way into these organizations. Rather than push back or engage more aggressively, we've simply packed up our notes and walked away. The National Cyber Director would be an international signal that we as a nation are taking cybersecurity seriously, and not treating it as an administrative or bureaucratic football that comes and goes depending on the political mood or the administration in office. We cannot do this alone—we must work with our partners and allies in Europe and Asia, all of whom are threatened by the Chinese Communist Party's perfidious influence.

3. Last month, Google's chief of threat analysis, Shane Huntley, stated on Twitter, "Recently TAG [threat analysis group] saw China APT [advanced persistent threat] targeting Biden campaign staff." In his statement, Mr. Huntley confirmed that Chinese hackers had not successfully penetrated Vice President Biden's campaign, but the attacks exemplify a troubling trend that has been growing for years. Since at least 2008, the Justice Department has been aware of state- sponsored hackers from countries like China, Iran, and Russia, attempting to undermine the integrity of our elections by targeting private campaign and candidate emails and data. This includes reported attempts by Iranian-backed hackers to target the Trump campaign with phishing attacks.
    a. Given the increase in state-sponsored cyberattacks against political campaigns, is our current process for combatting cyberattacks— particularly those aimed at our elections—adequate?

Put simply, no. We have been slow to respond to the threat of foreign interference in our elections and even slower to react to the threat of foreign influence in our elections. While the protection of the voter rolls and votes themselves is of paramount importance, what we missed was the attempts by Russia, China, and even Iran to influence the voters' opinions and perspectives through social media. We don't yet have a handle on how to counter these disinformation and misinformation campaigns.

b. How many different agencies must work together to identify, review, and address any election-related cyberattacks?

Responding to election-related cyberattacks requires a truly whole-of-government response from the intelligence community's identification of foreign malicious actors, to the Department of Homeland Security's issuance of guidance and warnings, to the Department of State for naming and shaming malign actors. This is to say nothing of the tech companies like Facebook and Twitter through which many of these influence and interference activities are being conducted, or the state and local governments which administer the elections themselves.

Additionally, this will invariably require Congressional involvement and action to address these weaknesses, as well as provide oversight and accountability for the agencies themselves. There is an inherent tension in the securing of elections that requires a balance for openness and protection, between states' rights and national-level cybersecurity. This is a difficult road to navigate, but if we are to sustain our democracy into the future, we must find this balance.

c. Why is the establishment of a National Cyber Director an important step in safeguarding our democracy?

Our adversaries, whether seeking to steal our data, influence the elections, or attack our power grids, will seek the path of least resistance. Unfortunately, right now there are several paths open to them because of the fragmented approach our government has to cybersecurity. The National Cyber Director will work to correct that by raising the standards and aligning the budgets against the National Cyber Strategy. If we cannot protect our citizens' data, whether it is their security clearances, food stamp information, social security benefits, or any number of other data points, the population will lose faith in the fundamental tenet of our country's founding—protection of the citizenry. This is the case even if the data isn't lost, but if people believe that our country is vulnerable and that they cannot believe in the systems established to protect them. This is too great a risk to leave to chance.

4. Your written testimony states, "When the tech industry looks at Washington, it sees a byzantine structure that is inefficient, does not know what it wants (let alone what it needs), and believes that process is progress for its own sake. In many ways, industry is not wrong."
    a. How would H.R. 7331 improve the partnership between the federal government and industry on cybersecurity issues?

If approved, the National Cyber Director would be the single point of contact and coordination office for the country's cyber defenses. Right now, this authority is scattered across the numerous agencies and departments, all of whom have their interpretation of the National Cyber Strategy, and align their budgets against that interpretation, accordingly. The relationship with the private sector is, as a result, largely customer and client. If department X needs something, they issue a request for proposal and then companies bid for that contract. By the time that contract is signed, the technology is already out of data and the threat has evolved. We need to change the mentality of customer-client and shift to a partnership.

By coordinating the budgets and ensuring a united effort against the National Cyber Strategy, the National Cyber Director would send a signal to the private sector that Washington is taking this problem seriously and is taking steps to address its problems. Perhaps more than anything else, getting the right person in that seat is critical. If you put a tech-savvy, forward-thinking person in that seat, they will excel and be able to work with Silicon Valley and others. If you put someone who doesn't get technology or the threats, you will lose out on the buy-in from tech companies and we will be right back where we started.

b. What would be the greatest national benefit of creating a National Cyber Director responsible for improving this partnership?

The greatest national benefit for this partnership is in the signal that it sends to Silicon Valley and others that Washington recognizes the threat and is working to address the challenge. Right now, Silicon Valley looks at Washington as an industrial era machine, clanking and banging away with steam and iron—slow to react, plodding along, and inefficient. That's not a terrible description of our cyber defenses. Washington needs to enter the information age, and a National Cyber Director is a step in that direction. We need to secure our citizens' data, but we can't do that alone. We need the support and assistance of the private sector in a cooperative, partnership-based relationship.

QUESTIONS FOR THE RECORD
On behalf of Ranking Member James Comer (R-KY) Committee on Oversight & Reform

1. How would you rate the level of the threat due to foreign economic espionage, particularly Chinese economic espionage conducted through cyber intrusions, to our national security?
    a. What authorities would the proposed National Cyber Director have over intelligence community and Defense Department led offensive and incident response activities to respond to such threats? Would the NCD office be a peer coordinating entity or would it have any actual ability to influence the activities of the nation's intelligence and defense functions?

The relationship between the National Cyber Director and the Intelligence Community and the Department of Defense must be close and continuous. While I don't envision the National Cyber Director having a hand in National Command Authority or decisions related to offensive or defensive operations, they will be a key part—if not the key part—of ensuring the government's protections are adequate and sustained. To do so, the National Cyber Director must know what the threats are, what they are forecast to be, and from what direction they are coming. It makes no sense to build a wall in the wrong place, and it would make no sense to defend against a threat that could never materialize.

2. The media recently reported that the Department of State, through their Global Engagement Center, produced a report on disinformation and propaganda by foreign adversaries, including Russia, China, and Iran. The propaganda runs the gamut of insinuating that the U.S. was the origin of the virus to claims those countries are managing the crisis well.
    a. What are your views of the success of this propaganda?

Measuring the impact of propaganda and disinformation campaigns is a challenge quite different from finding the "dog that didn't bark". What I believe matters more is that the country is seen to recognize the threat, address the threat, and communicate better with the public. To deny that it is happening, to downplay its efficacy, or to overreact is to feed into the hands of Beijing or Moscow. We must be wary not to create ten-foot-tall adversaries or see Russian boogeymen behind every tree, but we can no longer be ignorant of the threat we face.

    b. Do you recommend social media companies do anything in response to the propaganda and disinformation?

If we are to secure our democracy and protect against foreign interference in our elections, we must abandon the adversarial relationship that currently exists between social media companies and the government. Facebook, Twitter, and others cannot claim ignorance of the influence of their platforms in our American democracy, but Washington cannot lay the blame on the platforms alone. We need to build an active, working partnership with the FAANGs based on a mutual desire to protect our democracy and ensure free speech.

c. Do you believe this propaganda has resulted in any tangible harm to U.S. interests?

Our lack of imagination before the influence campaigns and our overreaction in the wake of their exposure has led to a lot of wasted energy and, as a result, harm to our interests. We need to accept that foreign interference, particularly over social media, is now normal. We need to educate the public on what it means, work with Twitter, Facebook, and others to identify and remove suspect activity, and name and shame those foreign actors who are conducting these efforts.

d. Is there any belief that there is a concerted cyber effort between China, Russian and Iran to coordinate on their propaganda messages?

As evidenced by the recent NCSC release on the forthcoming election, all three actors are keen to interfere in the election, but for different objectives and with different desired outcomes. I expect that Beijing, Moscow, and Tehran will use similar activities and vectors to interfere in the election, whether via social media, propaganda, active measures, or other dis/misinformation campaigns.

3. We have recently been briefed on threats originating from our very own universities, primarily researchers contracted through China's Thousand Talents Plan. While there's an economic espionage threat here, is there also a cyber threat?

The Chinese Communist Party's efforts to steal, buy, or borrow (without the intent of giving it back) technology are diverse and ongoing. The Thousand Talents Plan, of which many in the United States are now becoming aware, is one element of this program, but cyber activities remain very much a threat and will remain so for the foreseeable future. It is critical that the country become aware of these programs and who is behind or sponsoring them, and what the costs are in the long run.

A partnership today may appear lucrative, but when the resulting intellectual property is stolen or marketed by a Chinese company, we should not be surprised. This is one reason why it is so critical we secure our 5G future—we cannot allow any Chinese Communist Party-linked company to build out our communications network. To do so is tantamount to giving them access to any data that flows through those high-speed pipes.

4. What is the appropriate role for the Congress to play, and specifically this Committee, in conducting oversight of the key cyber organizations in the government?

As a former Committee Chairman, I believe that Congress and the oversight committees have one of the most important roles in our democracy. I believe that there are two roles the Committee can play concerning the oversight of the cyber organizations. First, ensuring that the programs, budgets, and expenditures are aligned against the threats we face today and tomorrow, not yesterday. Holding hearings that are forward-looking and probing, will force the agencies and departments to think beyond the immediate challenge—which they must address—and to the future, which is critical with next-generation technologies coming online. Second, I believe that

the Committee can help educate the public with its hearings and through its oversight ensure a more informed population. An educated citizenry is an empowered citizenry and we need that, now more than ever, to protect our democracy.