Center for a New American Security

December 12, 2018

Testimony before the Senate Judiciary Committee

China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses

Peter E. Harrell, Adjunct Senior Fellow
Energy, Economics, and Security Program, Center for a New American Security

Chairman Grassley, Ranking Member Feinstein, and Honorable Members of the Committee, it is a pleasure to be invited to speak to you today about one of the most important trade and national security issues that the U.S. confronts today: China's unconventional espionage against the United States.

I will address three issues in my testimony before you this morning.

First, I will offer an assessment of aspects of the threat. It is a pleasure to be joined by two distinguished co-panelists who will also speak about the threat and I will focus on the aspects of the threat that I am most familiar with: how China uses unconventional, economic espionage as a component part of a comprehensive strategy to promote China's own high-tech industries.

Second, I will assess the policy responses that the U.S. has pursued to date to respond to this threat.

And third, I will offer some recommendations on additional policy responses that the United States should consider going forward.

The Threat:

I will focus my remarks on two aspects of China's unconventional espionage threat. The first is "economic espionage," which is intended to provide China with commercial advantage over U.S. firms. I will also briefly touch on China's espionage tools with respect to U.S. universities and other non-governmental organizations here in the United States and in allied nations.

When it comes to economic espionage, it is important to keep in mind that espionage is but one element in a broader Chinese strategy to modernize its economy and to promote China as the world leader in a range of technologies that will be critical to both economic and military power in the years ahead. China is pursuing a whole-of-society approach to its technological capabilities that includes purchasing innovative companies through overseas investments, requiring western companies to transfer cutting edge technologies to China as a condition of market access, providing vast state resources to finance domestic technological development, and financing training for top

Chinese students and researchers overseas and paying a hefty premium to attract talent back to China. Outright theft of U.S. and western intellectual property (IP) is a key piece of China's strategy, but it is only a piece.

The United States generally distinguishes between Chinese economic espionage intended to provide Chinese companies with a commercial advantage and "traditional" espionage intended to obtain information about the U.S. government, U.S. military capabilities, and other sensitive government and government-related information. While the U.S. government must continue hardening its defenses against all espionage, China's spying on the U.S. government fits within a long practice of government spycraft and should be addressed with traditional types of tools.

U.S. policymakers however, have rightly sought to aggressively deter and punish Chinese espionage intended to steal trade secrets and other IP from the U.S. private sector that is then transferred to Chinese companies for commercial advantage, and to crack down on other forms of unconventional espionage that threaten America's technological, economic, and military edge. This represents a new and different threat to America's long-term leadership and must be addressed forcefully.

Of course, China is neither the first nor the only foreign government to use its intelligence services to promote commercial interests. The French engaged in economic espionage throughout the 1980s. Former U.S. Defense Secretary Robert Gates said in an interview that "there are probably a dozen or 15 countries that steal our technology." In 2015 a South Korean company plead guilty to conspiring to steal proprietary DuPont information about Kevlar, the body armor material, and paid more than $300 million in fines and restitution. A 2018 National Counterintelligence and Security Center (NCSC) report on foreign economic espionage in cyberspace stated that in addition to China, Russia and Iran were engaging in significant cyber-enabled economic espionage activities.

But China is by far the most active practitioner of economic espionage today. While it is challenging to accurately estimate the costs of such espionage, in 2017 the U.S. China IP Commission estimated that the total cost of China's theft of IP, which also includes more prosaic forms of IP theft like piracy and counterfeiting, costs the U.S. economy at least $225 billion annually and possibly as much as $600 billion. A 2014 estimate by the Center for Responsible Trade and Enterprise (CREATe) and PriceWaterhouseCoopers argued that the cost of trade secret theft could amount to between 1 percent and 3 percent of GDP annually. Former National Security Agency Director Keith Alexander has called China's IP theft "greatest transfer of wealth in history." And as the 2018 NCSC report noted, the threat is growing due to expanded cloud-based computer networks and the internet of things (the home appliances, cars, and other things that will be connected to the internet)--which, according to the NCSC "will create an incalculably larger exploitation space for cyber threat actors."

What does the threat look like in practice?

Casual discussions of Chinese economic espionage often focus on high-end cyber intrusions into U.S. corporate networks. And this is a pervasive reality. A recent report by cybersecurity firm Carbon Black found that 68 percent of surveyed cybersecurity incident response professionals reported that they were seeing cyberattacks from China and the half of all investigations focused on China and Russia. Department of Justice indictments and private sector reports in recent years have accused Chinese hackers of breaking into the corporate networks of U.S. and western companies

including defense contractors, non-profits, semiconductor firms, healthcare companies, industrial manufacturers, aerospace companies, media companies, solar companies, and electronics companies, among others. As former Cisco CEO John Chambers once said, "There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."

But the reality is that China also engages in economic espionage using a wide range more traditional of techniques, many of which have been publicly identified over the past several years by U.S. corporate disclosures, researchers, published U.S. government reports, and Department of Justice prosecutions of suspected Chinese spies. For example, China and Chinese companies have repeatedly paid off corporate insiders at U.S. and western companies to simply walk out the door with high-value trade secrets. Chinese agents have also physically broken in to U.S. corporate offices.

What types of technology and information does China target?

China has aggressively targeted technologies central to its Made in China 2025 industrial strategy, a fact that should come as little surprise given the importance China attaches to the strategy. In 2017 and 2018, suspected China-linked hackers have targeted U.S. firms operating in sectors including cloud computing, artificial intelligence, internet connected devices, biotechnology, energy, robotics, transportation, agricultural machinery and other agricultural technology, and high-end medical devices. The U.S. recently charged Chinese spies and companies with trying to steal trade secrets from the semiconductor industry, and charged a Chinese agent with collecting information on Chinese nationals working in the U.S. for possible recruitment by China's spy agencies. Unsurprisingly, China is also targeting sectors critical to U.S. military dominance, like aerospace, according to a recent indictment.

But China does not only steal corporate "crown jewels" like trade secrets: It targets a wide variety of information that can provide Chinese companies with commercial advantage. For example, U.S. prosecutors have accused Chinese hackers of stealing cost and pricing information from a U.S. solar company, which was probably intended to help Chinese competitors develop their own pricing strategy. The Department of Justice has even indicted Chinese spies for stealing strategy information from a U.S. labor union that strongly opposed Chinese trade practices. China has also tried to hack think tanks to understand policy and think tank engagement with government officials. Zach Cooper at AEI published a report on China's cyber strategy this past fall that compiled dozens of examples of the kinds of information China tries to steal. The bottom line is that if there is information out there that China thinks is of value, the odds are that China has or will try to steal it.

Colleges and Universities

I also want to offer brief remarks on the second, partly overlapping type of unconventional Chinese espionage that merits a forceful U.S. response: espionage against U.S. colleges and universities.

In recent years we have broadly seen two types of Chinese espionage targeting U.S. colleges and universities. The first of these is espionage targeting cutting edge research and technologies being developed by U.S. universities, including technology that has U.S. military applications. In many respects, the goals of this kind of espionage are similar to economic espionage—to capture technological advances that could prove valuable to Chinese firms and potentially to the Chinese

military. But universities risk being fertile place for this kind of espionage, given the open, international, and collaborative nature of most university research and universities' legitimate interest in encouraging international collaboration. I do not want to overstate the risk: the vast majority of research collaboration benefits the U.S. And the U.S. benefits from the world-class students and researchers we are able to attract to the U.S., many of whom—if they can get visas to stay—help found and build cutting edge companies in the U.S. But universities do need to take appropriate precautions to ensure that China is not able to use academic collaboration to steal U.S. intellectual property or engage in other activities that might harm U.S. national security.

The second type of Chinese espionage targeting U.S. colleges and universities has been espionage aimed at intimidating Chinese students and professors critical of Chinese policies, and to a lesser extent American students and academics. As a recent report by the Hoover Institution and the Asia Society put it, Chinese-backed associations on American campuses can provide "a ready channel or entry point for the political departments of China's embassy and consulates in the US to gather information and coordinate action. Sometimes pressure is even applied by China's security services on the family members of those students it finds speaking out in unacceptable ways back in China." These types of activities represent an assault against core American values in a bid to stifle legitimate and necessary debate about China.

Recent U.S. Government Responses:

The U.S. government has steadily increased its response to the threat of China's unconventional espionage. Broadly speaking, the government response can be divided into three parts: encouraging better defense; prosecuting spies; and increasing costs in an effort to punish and deter unconventional spying.

The first line of response has been to encourage companies to harden their networks against cyber intrusions and to bolster defenses against other types IP theft, such as by corporate insiders. Beginning under President Obama and continuing under President Trump, the Department of Homeland Security (DHS) has launched programs to encourage the private sector to harden defenses. DHS is also investing in research into technologies and public-private partnerships that may be able to improve cybersecurity practices and in education and outreach programs designed to improve corporate cybersecurity practices. Just last month, a new law reorganized the cyber security operations of DHS in order to improve their effectiveness, including establishing DHS's Cybersecurity and Infrastructure Security Agency.

The U.S. government has also worked to sharply limit the deployment of Chinese technology and equipment here in the U.S. that China could potentially use to facilitate its unconventional espionage in the years ahead. For example, the Trump Administration and this Congress have taken action to restrict the use of Chinese-made network equipment in U.S. telecommunications networks over concern that such equipment could facilitate Chinese espionage in the U.S. The State Department has recently pressed U.S. allies to similarly restrict the use of high-risk Chinese-made network equipment in their national telecommunications networks.

The second major U.S. government response has been increasingly aggressive Justice Department efforts to prosecute Chinese spies. The Department of Justice has in recent years indicted numerous

Chinese spies, hackers, and companies for their involvement in stealing U.S. IP. In a major coup, this past October Justice for the first time managed to extradite a suspected Chinese spy from a third country to the U.S. to face trial for his involvement in stealing U.S. trade secrets.

Last month, under former Attorney General Jeff Sessions, the Department of Justice expanded on several years of increasing prosecutorial efforts by launching an important new initiative to combat Chinese economic espionage, which Assistant Attorney General Demers is leading. The initiative will prioritize cases of Chinese economic espionage and ensure that they are appropriately resourced. This initiative will also work to use tools like the Foreign Agent Registration Act (FARA) to require better disclosure of Chinese activities across the United States. This initiative is a welcome step and I commend the Justice Department and the National Security Division for launching it.

The third major line of response has been to increase costs to China over its espionage program and to take action against specific Chinese companies that engage in and/or profit from unconventional espionage. This has taken several forms.

The Obama administration issued two Executive Orders, E.O. 13694 (2015) and E.O. 13757 (2016) that authorize the Treasury Department to impose sanctions on entities that engage in various forms of cyber hacking and on companies that steal trade secrets or other high-value IP via cyber-enabled means, or which benefit from such stolen IP. Although the Obama administration never sanctioned any Chinese individuals or companies using these authorities, it did use the potent threat of sanctions, as well as criminal prosecutions and significant high-level diplomatic engagement, to convince China to enter into a 2015 agreement in which Chinese President Xi agreed that China would not knowingly support cyber-enabled theft intellectual property for commercial gain. This was a narrow agreement in that it did not preclude the theft of intellectual property for other purposes, such as for improving defense capabilities, or the theft of U.S. government information, but it did at least temporarily represent a step by China toward reducing its espionage against U.S. commercial targets. The two countries appeared to quietly reaffirm the agreement in October 2017.

Reviews of the 2015 agreement have been mixed. A number of cyber security firms reported a drop in suspected China-linked attacks in the year following the agreement, and in late 2016 the CEO of the CrowdStrike cybersecurity firm called the change in China's behavior "the biggest success we've had in this arena in 30 years." However, Justice Department indictments and U.S. government reports indicate that there has been a substantial uptick in Chinese hacking over the past year, and so it remains unclear how much the agreement has or will affect Chinese behavior over the long-term. In addition, there has been a debate in the community about the extent to which the apparent reduction in attacks simply represented Chinese efforts to restructure how China engages in cyber operations, rather than a genuine change in Chinese intentions. Regardless, it seems likely that China will continue to deploy hacking as a tool of gaining U.S. IP as U.S. policy developments like export control reform and new restrictions on Chinese investment in the U.S. restrict China's ability to legally and overtly acquire its desired technologies.

The Trump administration has expanded U.S. government efforts to impose costs on China over its economic espionage. Chinese theft of U.S. intellectual property has been one of the major legal and policy rationales for the Trump administration's Section 301 finding on China and subsequent imposition of tariffs on some $250 billion in Chinese goods imported into the United States. Senior

administration officials made clear prior to President Trump's recent trade policy-focused meeting with Chinese President Xi that reductions in IP theft are a major administration priority, and reductions in Chinese IP theft should be a be a major U.S. demand in the U.S.-China trade negotiations that will occur over the next three months.

The Trump administration has also begun to deploy targeted trade measures against Chinese beneficiaries of IP theft. In late October, the U.S. Commerce Department put a Chinese semiconductor firm, Fujian Jinhua Integrated Circuit Company, on its "entity list," which prohibits U.S. companies from selling Fujian Jinhua technology and products. The Trump administration has accused Fijian Jinhua of benefiting from trade secrets that were stolen from Micron Technologies, a large U.S. semiconductor firm, and the Commerce action was a welcome, important development that signals to Chinese companies that stolen IP isn't free.

In addition to these Executive Branch actions, companies and Congress have played an important role in America's response.

Individual victims of Chinese IP theft have begun to resort to legal measures to fight back against companies that steal their trade secrets. The International Trade Commission (ITC) has authority to ban the import of products that are made with stolen U.S. IP, and in recent years U.S. companies have successfully petitioned the ITC to ban such products from entering the U.S. market. Some U.S. companies have also succeeded in obtaining court orders in other countries to prohibit Chinese companies from selling products based on stolen U.S. IP in those markets.

Congress has also played an important role. In 2016 broad bipartisan majorities of Congress passed the "Defend Trade Secrets Act," which expanded the rights of U.S. companies to sue Chinese firms and other foreign competitors that steal their IP. This has allowed U.S. companies such as Micron Technologies to sue Chinese companies in federal court for the Chinese companies' theft of U.S. IP. Congressional cybersecurity legislation enacted in 2014 has also played an important role in improving U.S. government efforts to harden U.S. defenses against Chinese and other attacks.

Policy Recommendations:

As I said earlier, I commend the work of the Department of Justice, the FBI, the Department of Homeland Security, USTR and other federal agencies to address China's unconventional espionage threat. I urge the government to continue its existing lines of effort, including continuing to ensure that U.S. telecommunications networks are robustly defended against Chinese unconventional espionage and to continue aggressively prosecuting China's espionage efforts.

The U.S. also needs to start getting a handle on the vast quantity of Americans' personal information that is all too readily available to make sure that it cannot be exploited by spies. Members of the Committee may have seen recent press reports about marketing firms and hedge funds buying cell phone location data showing the near-real time locations of tens of millions of Americans going about their daily routines. Even putting aside general issues of individual privacy, from an espionage perspective this kind of data can be a gold-mine, especially when combined with other data that the Chinese have access to. For example, if China purchased this information, it could cross-reference location information with data it stole from the Office of Personnel Management about U.S.

government employees, or against public record data about corporate executives. This would let China determine exactly where government officials and corporate executives work, where they spend the night, what doctors they visit, and their travels, among other information—all of which would provide valuable information to Chinese spies and companies. And getting access to this information would not even really be espionage as we typically think of it--the Chinese could simply set up a front company to buy the data commercially.

American policymakers should continue to distinguish between China's economic espionage and more traditional spying targeting U.S. government agencies, defense contractors, and other parts of the national security establishment. While the U.S. government and defense contractors must continue to harden their defenses against Chinese espionage and the U.S. government must work aggressively to root out, expel, and prosecute Chinese spies, the framework for addressing this kind of espionage is well developed. Chinese economic espionage, on the other hand, is an unconventional threat and requires an unconventional response.

Responding to China's unconventional espionage threat will require a whole-of-society approach, not just a whole-of-government approach. Recent high-profile announcements such as the Marriott hotel company's acknowledgement last week that cyber intruders had accessed the personal information of 500 million customers bring home the fact that despite billions of dollars of corporate investment in cybersecurity in recent years, many corporate networks remain all too vulnerable. U.S. companies continue to need to make major investments in hardening their defenses against cyber threats and to train employees to be vigilant against Chinese espionage.

Similarly, much of the responsibility for responding to Chinese efforts to infiltrate U.S. academic institutions will fall on those institutions themselves. A recent Hoover Institution-Asia Society report offered a number of recommendations with respect to these operations that I endorse, such as promoting transparency and disclosure around Confucius Institutes and increasing the due diligence universities apply to grants and gifts from Chinese sources. I would add that U.S. universities should also increase the scrutiny of their collaborative research projects with Chinese institutions and researchers to make sure that U.S. institutions are not inadvertently facilitating the transfer of proprietary and/or sensitive technology and expertise to China, while continuing to engage in legitimate and positive research collaborations.

But government tools must also be an important part of the U.S. government response. For U.S. government leaders, I offer five specific recommendations:

First, the Trump administration should expand the use of U.S. legal authorities to target companies that engage in and/or benefit from economic espionage: Both the Chinese government and individual Chinese companies need to understand that economic espionage carries costs, not just benefits. The Trump administration should also continue deploying regulatory tools such as the October Commerce Department Action against Fujian Jinhua to impose real costs on Chinese companies that seek to benefit from economic espionage.

The Trump administration should also expand these efforts by deploying the sanctions authorities under E.O.s 13757 and 13694, which authorize Treasury to sanction people, companies, and entities that engage in a cyber-enabled espionage and other cyberattacks. To date these authorities have been

deployed against individuals and companies from Russia and Iran in response to cyberattacks, but have yet to be deployed against Chinese entities engaged in or benefiting from economic espionage or other cyberattacks against the U.S. In addition to implementing sanctions on appropriate Chinese targets under these existing Executive Orders, the Trump administration and Congress should examine whether the sanctions authorities are legally adequate as currently drafted or whether they should be broadened to cover the full range of Chinese unconventional espionage threats.

Sanctions need to be deployed carefully to avoid unintended consequences and, at least initially, should be used only against egregious violators. But targeted sanctions against Chinese entities engaged in economic espionage or benefiting from stolen U.S. IP would send a powerful deterrent against such activities. They would also generally restrict those companies' ability to sell products based on stolen IP not only to the United States, but also to other countries around the world.

Second, Congress should study ways to expand prohibitions on the import into the U.S. of items made with stolen U.S. IP, and the Trump Administration should work with allies to keep such products out of foreign markets. The International Trade Commission (ITC) has authority under Section 337 to investigate claims that an import uses stolen U.S. IP and to exclude infringing products, and has excluded a number of Chinese products in recent years. There has also been a large rise in Section 337 investigations. But Congress should examine whether the existing statutory provisions are broad enough and whether resources for Section 337 investigations are adequate. The Administration and Congress should also look for ways to make these kinds of tools multilateral, working with foreign governments to ensure that foreign countries do not import products made with stolen U.S. IP and that the U.S. does not import products made with stolen foreign IP.

Third, the Trump administration should use Committee on Foreign Investment in the United States (CFIUS) authorities to prevent China from acquiring technologies that it is also trying to steal. As members of the Senate know, over the summer, Congress enacted the Foreign Investment Risk Review Modernization Act (FIRRMA), which overhauled the CFIUS review process for foreign investments in the United States. FIRRMA provides important new tools for the U.S. government to screen potential foreign investments in the U.S. for national security risks. The Trump administration should use CFIUS to block Chinese companies that have stolen U.S. technology from acquiring companies in the United States. Similarly, CFIUS should ensure that if the Chinese government has stolen or attempted to steal U.S. technology, no Chinese company should be able to acquire a U.S. company that designs or makes the technology that China attempted to steal. China needs to understand that if it tries to steal U.S. technology, it will not be able to benefit from it.

Fourth, Congress should consider amendments to the Foreign Agents Registration Act (FARA) or other legislation to require better disclosure about Chinese operations in the United States. As members of this Committee know, for many years the Department of Justice expended too little energy enforcing FARA, resulting in an explosion both here in Washington and across the country of unregistered agents working on behalf of foreign governments. Fortunately, efforts here in Congress, including by Chairman Grassley and other members of this Committee, have drawn public attention to this issue, and Assistant Attorney General Demers and the Department of Justice have significantly expanded FARA enforcement. But the underlying statute itself still arguably fails to cover a range of information collection and influence activities that China and other nations carry out in the United States. This Committee and the Congress as a whole should consider legislative

reforms to expand the reach of FARA or to adopt other disclosure legislation that would ensure that Chinese activities related to universities and other non-profits are fully subject to public disclosure requirements.

Fifth, I would encourage Congress to carefully study proposals to enable U.S. companies who are victims of Chinese economic espionage to "hack back." There are significant concerns about "hacking back" proposals but I believe the concept merits careful study.

The 1986 Computer Fraud and Abuse Act (CFAA) makes it illegal for Americans to access a computer without authorization. Congress passed the CFAA to prohibit hacking, but the law also prohibits "hacking back" in which victims of cyber espionage and other hacking take active steps to interfere with the hackers' computers. In recent years a number of members of Congress have introduced legislation that would amend the CFAA to authorize "hacking back" by victim companies under certain circumstances.

Proposals to allow "hacking back" are controversial because it is often difficult for a hacking victim to conclusively identify a hacker and there is concern that companies could "hack back" against an innocent party that was not actually involved in the original hacking. There have also been questions about how to limit "hacking back" so that a company engaged in "hacking back" is subject to appropriate U.S. government supervision and does not either intentionally or inadvertently escalate the situation.

"Hacking back" proposals would need to be carefully tailored to mitigate potential unintended consequences and to protect innocent parties, and the risks need to be carefully evaluated. That said, I recommend that Congress carefully consider "hacking back" proposals that would enable U.S. companies to take a broader range of active measures to defend themselves against cyber espionage and other cyber attacks.

Closing Remarks:

In closing, I would like to offer two general thoughts.

First, I firmly believe that the U.S. is more likely to be able to effectively combat Chinese unconventional espionage if the U.S. holds out the prospect for cooperation in the U.S.-Chinese overall relationship. I was glad to see President Trump and Chinese President Xi agree to 90 days of trade talks when they met two weeks ago at the G20 summit. U.S. Trade Representative Lighthizer and President Trump needs to demand major, systematic changes in a range of Chinese trade abuses before relenting on the tariffs and other measures the U.S. has imposed. But if China proves willing to make systemic changes, the administration should be willing to relax the trade remedies the U.S. has imposed, rather than locking the U.S. into an economic cold war with Beijing. If Beijing sees no path to a cooperative economic relationship with Washington and instead believes that it will face mounting U.S. pressure regardless of any concessions Beijing may offer, Beijing will have little incentive to curb its efforts to steal U.S. technology. Of course, China may well prove unwilling to make the necessary concessions. And the U.S. would need to take the Ronald Reagan line towards Soviet military commitments when it comes to Chinese concessions, "Trust, but verify"—with an emphasis on the "verify." But we should not foreclose the possibility of cooperation.

Similarly, even as the U.S. increases pressure on China's unconventional espionage, we should make sure that we do not inadvertently shut down or prevent valuable academic study, research and development, and other activities that benefit the U.S. For example, the U.S. derives major benefits from the hundreds of thousands of highly-skilled foreigners, including from China, who come to the U.S. to study, to work, and to start businesses. As a country we should work to capture that talent here and make sure that it stays in the U.S. Much research and development also works more effectively when scientists and engineers are able to collaborate across borders. We need to keep efforts that target China's espionage laser-focused on the small percentage of individuals and entities engaged in illicit behavior.

Finally, the investments we make at home to maintain America's technological edge are ultimately going to be more important than the steps we take to stop China's theft of American IP. It is absolutely essential to stop Chinese unconventional espionage. But China is investing billions of dollars in its own technological prowess and can draw on the expertise of millions of Chinese engineers and scientists who have studied at top universities globally. U.S. federal research and development (R&D) spending as a percentage of U.S. GDP, meanwhile, suffered through a multi-year decline before Congress finally began to reverse the trend—a welcome development—for fiscal year 2018, which saw the largest federal research spending increase in a decade.

Individual U.S. government agencies understand that increasing investment is the most important element to maintaining America's technological edge. The Defense Department's Defense Advanced Research Projects Agency (DARPA), for example, last year launched a $1.5 billion, five-year initiative to support advances in chip technology. Other U.S. agencies are also working to expand cutting-edge U.S. R&D. But R&D, and especially the kind of long-term, often basic research that the U.S. government is often more willing to fund than commercial enterprises—needs to be sustained and expanded over time to achieve results. If the United States does not continue to make and expand R&D here in the U.S., China will eventually overtake our technological edge, regardless of how effective we are at preventing China from stealing, buying, or otherwise acquiring U.S. IP.

Thank you again for the opportunity to testify today and I look forward to your questions.

Biography

Peter Harrell
Adjunct Senior Fellow, Energy, Economics, and Security Program, Center for a New American Security

PETER HARRELL is an adjunct senior fellow at the Center for a New American Security, where he focuses on the intersection of economics and national security. Research interests include economic statecraft, sanctions, trade policy, and energy. He has authored numerous public policy reports, and his articles and op-eds have appeared in publications including *Foreign Affairs,* the *Wall Street Journal*, the *National Interest*, *Politico*, and other leading publications.

From 2012-2014, Mr. Harrell served as the Deputy Assistant Secretary for Counter Threat Finance and Sanctions in the State Department's Bureau of Economic and Business Affairs. In that role, Harrell was instrumental in developing international sanctions against Iran, Russia, and Syria, and in the easing of sanctions on Myanmar. He also played a leading role in the U.S. government's efforts to counter terrorist financing, including work to combat the financing of the Islamic State (ISIL).

Mr. Harrell served on the State Department's Policy Planning Staff from March 2009 to June 2012, where he played a leading role in developing Secretary of State Hillary Clinton's economic statecraft agenda. He also worked on a variety of other trade and economic issues, with a particular interest in Asia, and authored and edited sections of the State Department's first-ever Quadrennial Diplomacy and Development Review (QDDR).

Before joining the State Department, Mr. Harrell served on President Barack Obama's 2008 campaign. He previously worked as a reporter for Congressional Quarterly in Washington, D.C., and is the author of one book, Rwanda's Gamble: Gacaca and a New Model of Transitional Justice. Mr. Harrell is a magna cum laude graduate of Princeton University and holds a J.D. from the Yale Law School. He is from Atlanta, Georgia.