S. HRG. 114–398

UNITED STATES CYBERSECURITY POLICY AND THREATS

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 29, 2015

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.fdsys.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
22–270 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma	JACK REED, Rhode Island
JEFF SESSIONS, Alabama	BILL NELSON, Florida
ROGER F. WICKER, Mississippi	CLAIRE MCCASKILL, Missouri
KELLY AYOTTE, New Hampshire	JOE MANCHIN III, West Virginia
DEB FISCHER, Nebraska	JEANNE SHAHEEN, New Hampshire
TOM COTTON, Arkansas	KIRSTEN E. GILLIBRAND, New York
MIKE ROUNDS, South Dakota	RICHARD BLUMENTHAL, Connecticut
JONI ERNST, Iowa	JOE DONNELLY, Indiana
THOM TILLIS, North Carolina	MAZIE K. HIRONO, Hawaii
DAN SULLIVAN, Alaska	TIM KAINE, Virginia
MIKE LEE, Utah	ANGUS S. KING, JR., Maine
LINDSEY GRAHAM, South Carolina	MARTIN HEINRICH, New Mexico
TED CRUZ, Texas	

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

CONTENTS

SEPTEMBER 29, 2015

UNITED STATES CYBERSECURITY POLICY AND THREATS

TUESDAY, SEPTEMBER 29, 2015

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:30 a.m. in Room SD–G50, Dirksen Senate Office Building, Senator John McCain (chairman) presiding.

Committee Members Present: Senators McCain, Inhofe, Sessions, Wicker, Ayotte, Fischer, Cotton, Rounds, Ernst, Tillis, Sullivan, Lee, Reed, Nelson, McCaskill, Manchin, Gillibrand, Donnelly, Hirono, Kaine, King, and Heinrich.

OPENING STATEMENT OF SENATOR JOHN MCCAIN, CHAIRMAN

Chairman MCCAIN. Good morning. The committee meets today to receive testimony from Deputy Security of Defense Robert Work, Director of National Intelligence James Clapper, and Admiral Mike Rogers, the Commander of U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. We thank each of the witnesses for their service and for appearing before the committee.

We meet at a critical time for the defense of our Nation from cyberattacks. In just the past year, we all know the United States has been attacked by cyberspace—in cyberspace by Iran, North Korea, China, and Russia. Indeed, since our last cyber hearing in March, the attacks have only increased, crippling or severely disrupting networks across the government and private sector, and compromising sensitive national security information.

Recent attacks against the Joint Chiefs of Staff, the Pentagon, and the Office of Personnel Management are just the latest examples of the growing boldness of our adversaries in their desire to push the limits of acceptable behavior in cyberspace. New intrusions, breaches, and hacks are occurring daily. The trends are getting worse. But, it seems the administration has still not mounted an adequate response. They say they will, quote, "respond at the time and manner of our choosing," unquote, but then either take no action or pursue largely symbolic responses that have zero impact on our adversaries' behavior.

Not surprisingly, the attacks continue, our adversaries steal, delete, and manipulate our data at will, gaining a competitive economic edge and improving their military capability. They demonstrate their own means to attack our critical infrastructure. And they do all of this at a time and manner of their choosing. More

and more, they are even leaving behind what Admiral Rogers recently referred to as, quote, "cyber fingerprints," showing that they feel confident that they can attack us with impunity and without significant consequences.

Just consider the recent case with China. After much handwringing, it appears the President will not impose sanctions in response to China's efforts to steal intellectual property, pillage the designs of our critical weapon systems, and wage economic espionage against U.S. companies. Instead, last week's state visit for the President of China simply amounted to more vague commitments not to conduct or knowingly support cyber-enabled theft of intellectual property.

What's worse, the White House has chosen to reward China with diplomatic discussions about establishing norms of behavior that are favorable to both China and Russia. Any internationally agreed-upon rules of the road in cyberspace must explicitly recognize the right of self- defense, as contained in Article 51 of the U.N. Charter, along with meaningful human rights and intellectual property rights protections. The administration should not concede this point to autocratic regimes that seek to distort core principles of the international order, to our detriment.

Make no mistake, we are not winning the fight in cyberspace. Our adversaries view our response to malicious cyberactivity as timid and ineffectual. Put simply, the problem is a lack of deterrence. As Admiral Rogers has previously testified, the administration has not demonstrated to our adversaries that the consequences of continued cyberattacks against us outweigh the benefit. Until this happens, the attacks will continue, and our national security interests will suffer.

Establishing cyberdeterrence requires a strategy to defend, deter, and aggressively respond to the challenges to our national security in cyberspace. That is exactly what the Congress required in the Fiscal Year 2014 National Defense Authorization Act. That strategy is now over a year late, and counting. And, while the Department of Defense's 2015 cyberstrategy is a big improvement over previous such efforts, it still does not integrate the ends, ways, and means to deter attacks in cyberspace.

Establishing of cyberdeterrence also requires robust capabilities, both offensive and defensive, that can pose a credible threat to our adversaries, a goal on which the Congress, and specifically this committee, remains actively engaged.

The good news here is that significant progress has been made over the past few years in developing our cyberforce. That force will conclude—will include a mix of professionals trained to defend the Nation against cyberattacks, to support the geographic combatant commands in meeting their objectives, and to defend DOD networks. This is good. But, the vast majority of our DOD resources have gone toward shoring up our cyberdefenses. Far more needs to be done to develop the necessary capabilities to deter attacks, fight, and win in cyberspace. Policy indecision should not become an impediment to capability development.

We do not develop weapons because we want to use them. We develop them so as we do not have to. And yet, in the cyberdomain, as Admiral Rogers testified in March, quote, "We're at a tipping

point." He said, quote, "We've got to broaden our capabilities to provide policymakers and operational commanders with a broader range of options." We must invest more in the offensive capabilities that our cybermission teams need to win on the cyber battlefield. The fiscal year 2016 NDAA [National Defense Authorization Act] seeks to address this challenge in a number of ways, including a pilot program to provide the Commander of Cyber Command with limited rapid acquisition authorities.

Finally, we know the Defense Department is in the process of assessing whether the existing combatant command structure adequately addresses the mission of cyberwarfare, and whether to elevate Cyber Command to a unified command. There are worthwhile arguments on both sides of this debate. I look forward to hearing Admiral Rogers' views on this question and his assessment of how an elevation of Cyber Command might enhance our overall cyberdefense posture.

I also look forward to hearing from our witnesses what, if any, progress has been made on addressing disagreements within the interagency on the delegation and exercise of authority to use cyber capabilities.

I thank the witnesses again for appearing before the committee. I look forward to their testimony.

Senator Reed.

STATEMENT OF SENATOR JACK REED

Senator REED. Thank you very much, Mr. Chairman. And let me commend you for scheduling this very important hearing. It's an appropriate to discuss a number of important cyber issues with our witnesses, especially in light of the cyber agreements announced last Friday between President Obama and the President of China.

I want to thank Director Clapper, Deputy Security Work, and Cyber Command Commander Admiral Rogers for their testimony today and for their service to the Nation. Thank you, gentlemen, very much.

Let me start with a series of cyber agreements with China. The apparent commitment by China to cease stealing United States intellectual property for their economic gain is notable. And I expect we will have a robust discussion about China's compliance and our course of action if it does not. China's leaders must be aware that its reputation and standing in the eyes of the American people will continue to decline if this piracy does not stop, which ultimately will have a tremendously negative impact on our relations with China.

I would also emphasize potential importance of China embracing a set of international norms in cyberspace developed by the United Nations which includes a commitment to refrain from attacks on other nations' critical infrastructure.

Next, I would highlight that we are facing the recurring issue of whether or when to elevate Cyber Command from a sub-unified command to a full unified command, and whether to sustain the current dual-hat arrangement under which the Commander of Cyber Command also serves as the Director of the NSA [National Security Agency]. I understand that the Department may be near-

ing a recommendation to the President that the next unified command plan elevate Cyber Command to a unified command.

The committee, in the past, has questioned whether Cyber Command is mature enough to warrant elevation to a unified command, and whether the dual-hat arrangement should continue when a decision is made to elevate the Command. Put simply, if Cyber Command is so reliant on NSA that common leadership is still necessary, is the Command ready to stand on its own as a unified combatant command? This is an issue that Senator McCain has drawn attention to, and it's something that I think is very critical, going forward, for this committee.

Directly related to that question of the maturity of Cyber Command is the status of the military cyber mission units that the Department only began fielding over the last 2 years. Commendably, the Department is meeting its schedule for standing up these units with trained personnel; but, by its own admission, the equipment, tools, and capabilities of these forces will remain limited. Indeed, the committee's proposed FY16 National Defense Authorization Act includes a mandate that the Secretary of Defense designate executive agents from among the services to build a so-called "unified platform," persistent training environment, and command-and-control systems that are necessary for these forces to operate effectively. It will take a number of years to build these—capability.

We are behind in developing these military capabilities for our cyber forces because the Defense Department was persuaded that the systems and capabilities that NSA already has would be adequate and appropriate for use by Cyber Command. This is an important example of an assumed critical dependency on NSA and an assumed commonality between intelligence operations and military operations in cyberspace that, in some cases, has turned out to be inaccurate.

For a number of years, this committee has been urging the executive branch to work diligently to identify all practical methods to deter malicious actions in cyberspace and to articulate a strategy for implementing them. Some believe that retaliation in kind in cyberspace is a necessary and effective component of such a strategy. I look forward to hearing the views of our witnesses on this matter.

As my colleagues and our witnesses are well aware, the Senate went into recess for the August break having reached an agreement for bringing the cyber information-sharing bill to the floor for debate. I know the Chairman is in full agreement on the need to debate, amend, and pass that legislation this year in the interest of national security, and so am I.

We must also recognize the Defense Department and intelligence community are not operating alone to protect America's cyber infrastructure, most notably rely on the Department of Homeland Security for protection of America's critical infrastructure. The use of overseas contingency operations funding to avoid the Budget Control Act caps in defense does nothing to help the DHS [Department of Homeland Security] or other nondefense partners avoid the effects of sequestration. This is yet another argument for why we need a comprehensive solution to the problem of sequestration.

Finally, I think it is important that we hear from our witnesses on the subject of encryption. Post-Snowden, U.S. technology companies fearful of losing business at home and abroad are encrypting communications and offering encryption services for which even the companies themselves have no technical capability to unlock. FBI Director Comey has given multiple speeches warning the law enforcement agencies and intelligence agencies that they will be going dark, with serious consequences for public safety and national security.

These and other questions, gentlemen, are vitally important. And I look forward to your testimony.

Chairman MCCAIN. I thank the witnesses.

Director Clapper, I've tried to impress on members of this committee to show deference to old age, and so we'd like to begin with you.

STATEMENT OF HON. JAMES R. CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE

Director CLAPPER. Chairman McCain, Ranking Member Reed, members of the committee, when I testified on the intelligence community's worldwide threat assessment at the end of February, cyberthreats again led our annual threat report for the third year in a row. We're here today to respond to the several requests in your invitation letter, and I will focus on an overview of cyberthreats, briefly, that face our Nation, and their attendant national security implications. And then Secretary Work, Admiral Rogers will follow, as well.

We will, as you understand, perhaps run into some classified aspects that we won't be able to discuss as fully in this open televised hearing.

I do want to take note of and thank the members of the committee who are engaged on this issue and have spoken to it publicly, as the two of you just have.

So, by way of overview, cyberthreats to the U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. Although we must be prepared for a large, Armageddon-scale strike that would debilitate the entire U.S. infrastructure, that is not, we believe, the most likely scenario. Our primary concern now is low- to moderate-level cyberattacks from a variety of sources which will continue and probably expand. This imposes increasing costs to our business, to U.S. economic competitiveness, and to national security.

Because of our heavy dependence on the Internet, nearly all information, communication technologies, and IT networks and systems will be perpetually at risk. These weaknesses provide an array of possibilities for nefarious activity by cyberthreat actors, including remote hacking instructions, supply-chain operations to insert compromised hardware or software, malicious actions by insiders, and simple human mistakes by system users.

These cyberthreats come from a range of actors, including nation-states, which fall into two broad categories, those with highly sophisticated cyberprograms, most notably Russia and China, are our peer competitors, and those with lesser technical capabilities, but more nefarious intent, such as Iran and North Korea, who are also

more—but who are also much more aggressive and unpredictable. Then there are non-nation-state entities—criminals motivated by profit, hackers or extremists motivated by ideology.

Profit-motivated cybercriminals rely on loosely networked online marketplaces, often referred to as the "cyber underground" or "dark web," that provide a forum for the merchandising of illicit tools, services, and infrastructure and stolen personal information and financial data. The most significant financial cybercriminal threats to U.S. entities and our international partners come from a relatively small subset of actors, facilitators, and criminal forums.

And terrorist groups will continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities.

Cyber espionage criminal and terrorist entities all undermine data confidentiality. Denial-of-service operations and data-deletion attacks undermine availability. And, in the future, I think we'll see more cyberoperations that will change or manipulate electronic information to compromise its integrity. In other words, compromise its accuracy and reliability instead of deleting it or disrupting access to it.

As illustrated so dramatically with the OPM [Office of Personnel Management] breaches, counterintelligence risks are inherent when foreign intelligence agencies obtain access to an individual's identity information—of course, a problem that the Department of Defense has encountered. Foreign intelligence agencies or nonstate entities could target the individual, family members, coworkers, and neighbors, using a variety of physical and electronic methods, for extortion or recruiting purposes.

And speaking of the OPM breaches, let me say a couple of words about attribution. It is not a simple process, involves at least three related but distinct determinations: the geographic point of origin, the identity of the actual perpetrator doing the keystrokes, and the responsibility for directing the act. In the case of OPM, we have differing degrees of confidence in our assessment of the actual responsibility for each of these three elements.

Such malicious cyberactivity will continue and probably accelerate until we establish and demonstrate the capability to deter malicious state-sponsored cyberactivity. And establishing a credible deterrent depends on reaching agreement on norms of cyberbehavior by the international community.

So, in summary, the cyberthreats to U.S. national and economic security have become increasingly diverse, sophisticated, and harmful. There are a variety of Federal entities that work the cyber problem in DHS, FBI, NSA, and other law enforcement, intelligence, and sector-specific agencies, like Treasury and Energy. Every day, each of these centers and entities get better at what they do individually. I believe now we've reached the point where we think it's time to knit together all the intelligence these separate activities need to defend our networks, because, while these entities may be defending different networks, they are often defending against the same threats. So, that's one reason the President directed me to form a small center to integrate cyberthreat intelligence. And I strongly believe the time's come for the creation of such a center to parallel the centers that we operate for counter-

terrorism, counterproliferation, and counterintelligence and security.

With that, let me turn to Deputy Security Work.

[The prepared statement of Director Clapper follows:]

Statement for the Record

U.S. Cybersecurity and Policy

Senate Armed Services Committee

James R. Clapper

Director of National Intelligence

September 29, 2015

STATEMENT FOR THE RECORD

Worldwide Cyber Threats

September 29, 2015

INTRODUCTION

Chairman McCain, Ranking Member Reed, Members of the Committee, thank you for the invitation to offer this Statement for the Record. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

Information available as of September 28, 2015 was used in the preparation of this Statement for the Record.

Worldwide Cyber Threats

Overview

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology (ICT) networks that support U.S. Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a "Cyber Armageddon" scenario that debilitates the entire U.S. infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security.

- Several nations-including Iran and North Korea-have undertaken offensive cyber operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises.

Risk. Despite ever-improving network defenses, the diverse possibilities available through remote hacking intrusion, supply chain operations to insert compromised hardware or software, actions by malicious insiders, and mistakes by system users will hold nearly all ICT networks and systems at risk for years to come. In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed. Moreover, the risk calculus employed by some private sector entities does not adequately account for foreign cyber threats or the systemic interdependencies between different critical infrastructure sectors.

Costs. We continue to witness an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information (PII) compromised, or remediation costs incurred by U.S. victims. For example:

- Earlier this year, the Office of Personnel Management (OPM) discovered that a number of its systems were compromised. In April 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been compromised. Further, in the course of investigating this initial incident, OPM discovered that additional systems had been compromised, including those that contain background investigation records of current, former, and prospective Federal government employees and

contractors. OPM and the interagency incident response team have concluded with high confidence that sensitive information from the background investigation databases on as many as 21.5 million individuals, was potentially compromised.

- After the 2012-13 distributed denial of service (DDOS) attacks on the U.S. financial sector, JPMorgan Chase (JPMorgan) announced plans for annual cyber security expenditures of $250 million by the end of 2014. After the company suffered a hacking intrusion in 2014, JPMorgan's CEO said he would probably double JP Morgan 's annual computer security budget within the next five years.

- The 2014 data breach at Home Depot exposed information from 56 million credit/debit cards and 53 million customer email addresses. Home Depot estimated the cost of the breach to be $62 million.

- In August 2014, the U.S. company, Community Health Systems, informed the Securities and Exchange Commission that it believed hackers "originating from China" had stolen PII on 4.5 million individuals.

Attribution. Although cyber operators can infiltrate or disrupt targeted ICT networks, most can no longer assume that their activities will remain undetected indefinitely. Nor can they assume that if detected, they will be able to conceal their identities. Governmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions.

- In May 2014, the U.S. Department of Justice indicted five officers from China's Peoples' Liberation Army on charges of hacking and economic espionage against U.S. companies to steal information that would be useful to Chinese competitors.

- In December 2014, computer security experts reported that members of an Iranian organization were responsible for computer operations targeting U.S. military, transportation, public utility, and other critical infrastructure networks.

Determining attribution or responsibility for a malicious cyber activity is a complicated process, and we can have differing levels of confidence in our assessment of where geographically the activity came from, who conducted it, and who made the decisions or gave the orders. Publicly naming the malicious actor responsible for an intrusion or other malicious cyber act is a step that, once taken, cannot readily be undone, and that the U.S.

Government will consider using when it furthers our ability to impose costs or otherwise hold those actors accountable.

Deterrence. Numerous actors remain undeterred from conducting economic cyber espionage or perpetrating cyber attacks. The absence of universally accepted and enforceable norms of behavior in cyberspace has contributed to this situation, although some progress is being made on issues of mutual concern to all states (e.g., refraining from cyber attacks against critical infrastructure in peacetime). The motivation to conduct cyber attacks and cyber espionage will probably remain strong because of the relative ease of these operations and the gains they bring to the perpetrators. The result is a cyber environment in which multiple actors continue to test their adversaries' technical capabilities, political resolve, and thresholds. The muted response by most victims to cyber attacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation. Additionally, even when a cyber attack can be attributed to a specific actor, the forensic attribution often requires a significant amount of time to complete. Long delays between the cyber attack and determination of attribution likewise reinforce a permissive environment.

Threat Actors

Politically motivated cyber attacks are a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile. In addition, those conducting cyber espionage are targeting U.S. government, military, and commercial networks on a daily basis. These threats come from a range of actors, including: (1) nation states with highly sophisticated cyber programs (such as Russia or China),
(2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea), (3) profit-motivated criminals, and (4) ideologically motivated hackers or extremists. Distinguishing between state and non-state actors within the same country is often difficult-especially when those varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber tools.

Russia. Russia's Ministry of Defense is establishing its own cyber command, which-according to senior Russian military officials-will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations.

- Computer security studies assert that Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software ("malware") designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates, according to private sector cyber security experts.

China. Chinese cyber-enabled theft of U.S. companies' intellectual property for commercial gain remains a significant issue. Although China is an advanced cyber actor in terms of capabilities, Chinese hackers are often able to succeed in establishing access to their targets using less sophisticated cyber tools and techniques. Improved cyber security would require these hackers to use more sophisticated capabilities and would make China's economic espionage more costly and difficult to conduct.

Iran. Iranian actors have been implicated in the 2012-13 DDOS attacks against U.S. financial institutions and in the February 2014 cyber attack on the Las Vegas Sands casino company. Iran very likely views its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes, as well as a sophisticated means of collecting intelligence.

North Korea. North Korea is another state actor that uses its cyber capabilities for political objectives. The North Korean Government was responsible for the November 2014 cyber attack on Sony Pictures Entertainment (SPE), which stole corporate information and introduced hard drive erasing malware into the company's network infrastructure, according to the FBI. The attack coincided with the planned release of a SPE feature film satire that depicted the fictional assassination of the North Korean leader.

Profit-motivated criminals. Profit motivated cyber criminals rely on loosely networked online marketplaces, often referred to as the cyber underground, that provide a forum for the merchandising of illicit tools, services, infrastructure, stolen PII and financial data. As media reports have documented, cyber criminals continue to successfully compromise the networks of retail businesses and financial institutions in order to collect financial information, biographical data, home addresses, email addresses, and medical records that serve as the building blocks to criminal operations that facilitate identity theft and healthcare fraud. The most significant financial cyber criminal threats to U.S. entities and our international partners can be attributed to a relatively small subset of actors, facilitators, infrastructure, and criminal

forums.

However, our Federal law enforcement colleagues continue to have successes capturing key cyber criminals by cooperating with international partners. For example, in late June, the Department of Justice and the United States Secret Service worked with their German counterparts to extradite Ercan Findikoglu, a Turkish national, responsible for multiple cyber crime campaigns that targeted the U.S. financial sector stealing $55 million dollars between 2011 and 2013. Findikoglu was apprehended by the German Federal Police after U.S. Secret Service agents confirmed he was traveling through Germany in December 2013. Additionally, this month an FBI-led coalition of international partners from 20 countries dismantled an online criminal forum known as Darkode. According to the Department of Justice, this forum represented one of the gravest threats to the integrity of data stored on computers in the United States and elsewhere.

Terrorists. Terrorist groups will continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers will probably conduct low-level cyber attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors.

With respect to the Islamic State of Iraq and the Levant (ISIL), since last summer, the group began executing a highly strategic social media campaign using a diverse array of platforms and thousands of online supporters around the globe. The group quickly builds expertise in the platforms it uses and often leverages multiple tools within each platform. ISIL and its adherents' adept use of social media allows the group to maximize the spread of its propaganda and reach out to potential recruits.

Integrity of Information

Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data- deletion attacks undermine availability. In the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e. accuracy and reliability) instead of deleting it or disrupting access to it. Decision-making by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.

- Successful cyber operations targeting the integrity of information would need to

overcome any institutionalized checks and balances designed to prevent the manipulation of data, for example, market monitoring and clearing functions in the financial sector.

Counterintelligence

Internet users are disclosing more information about themselves through social media platforms, online transactions, and search engine queries. New business models for online services often require disclosure of personal information or consent to allow corporate monitoring of one's online activities. Governments and third parties digitize public records and share them on the Internet for accessibility, making online records an unavoidable byproduct of living in a digitized society.

Counterintelligence risks are inherent when foreign intelligence agencies obtain access to an individual's PII or virtual identity information. Foreign intelligence agencies could target the individual, family members, coworkers, and neighbors using a variety of physical and electronic methods. The methods foreign intelligence agencies use to exploit targets require a comprehensive mitigation effort that involves Cl awareness not only from the individual, but also from family members and coworkers that might have their data compromised as part of the individual's investigation.

An Integrated Approach

As the President has said, and as is evident from my testimony today, cyber threats pose one of the gravest national security dangers to the United States. As with our counterterrorism efforts, the United States Government is taking a "whole-of-government" approach to defend against and respond to these threats. The creation of the Cyber Threat Intelligence Integration Center (CTIIC) is a crucial part of this effort. The CTIIC will be a national cyber threat intelligence center that will "connect the dots" regarding malicious foreign cyber threats to the nation so that relevant departments and agencies are aware of these threats in as close to real time as possible. The CTIIC will provide integrated all-source analysis of foreign cyber threats and cyber incidents affecting U.S. national interests, help ensure that the U.S. government centers responsible for cybersecurity and network defense have access to the intelligence needed to perform their missions, and facilitate and support efforts by the government to counter foreign cyber threats.

In my view, the CTIIC will improve our situational awareness, enhance indications and

warning, and strengthen cyber unity of effort for the U.S. government. It will ensure indicators of malicious activity are downgraded to the lowest possible classification level to facilitate seamless intelligence flows among centers, including those responsible for sharing with the private sector. Most importantly, the CTIIC will augment that "whole-of-government" approach by providing policymakers with a cross-agency, integrated view of foreign cyber threats, their severity, and potential attribution.

Conclusion

In summary, the breadth of cyber threats posed to U.S. national and economic security has become increasing diverse, sophisticated, and impactful. Cyber intelligence -- collecting, analyzing, and disseminating intelligence on the intentions, capabilities, and operational activities of foreign cyber actors - is one of the core objectives in the National Intelligence Strategy we produced last year to guide the information and guide the activities of the IC. Ensuring the integration of such activities in support of our policy makers and national security is a core mission for the Office of the ODNI, and was one reason the President, directed me to form CTIIC. I look forward to working with the Senate and my interagency colleagues to enable the IC in general and CTIIC in particular to better support our nation in this vital area. Thank you.

STATEMENT OF HON. ROBERT O. WORK, DEPUTY SECRETARY OF DEFENSE

Mr. WORK. Chairman McCain, Ranking Member Reed, distinguished members of the committee, thank you very much for inviting us here this morning to talk about the threats of cyber. This committee has led the way in discussing the threats and the response to these threats, and the Department looks forward to working with the committee to get better in this regard.

As the DNI [Director of National Intelligence] Clapper has said, cyberintrusions and attacks by both state and nonstate actors have increased dramatically in recent years, and particularly troubling are the increased frequency and scale of state-sponsored cyberactors breaching U.S. Government and business networks. These adversaries continually adapt and evolve in response to our cyber countermeasures, threatening our networks and systems of the Department of Defense, our Nations' critical infrastructure, and U.S. companies and interests globally.

The recent spate of cyberevents, to include the intrusions into OPM, the attacks on Sony, and the Joint Staff networks by three separate state actors, is not just espionage of convenience, but a threat to our national security. As one of our responses to this growing threat, we released, in 2015, the DOD [Department of Defense] Cyber Strategy, which will guide the development of our cyberforces and strengthen our cybersecurity and cyberdeterrence posture. That is its aim.

The Department is pushing hard to achieve the Department's three core missions as defined in the strategy. The first and absolutely most important mission is to defend DOD network systems and information. Secretary Carter has made this the number-one priority in the Department, and we are really getting after it now. Second, to defend the Nation against cyberevents of significant consequence. And third, to provide cybersupport to operational and contingency plans. And, in this regard, the U.S. Cyber Command may be directed to conduct cyberoperations, in coordination with other government agencies, as appropriate, to deter or defeat strategic threats in other domains.

Now, my submitted statement, Mr. Chairman, contains additional detail on how we're moving out to achieve these three strategic goals, but I'd like to highlight the particular focus on deterrence, especially since I know this is key in the minds of most of the members here.

I want to up—acknowledge, up front, that the Secretary and I recognize that we are not where we need to be in our deterrent posture. We do believe that there are some things the Department is doing that are working, but we need to improve in this area, without question. And that's why we've revised our cyberstrategy.

Deterrence is a function of perception. It works by convincing any potential adversary that the costs of conducting the attack far outweigh any potential benefits. And therefore, our three main pillars of our cyberdeterrence strategy, in terms of deterrence, are denial, resilience, and cost imposition. Denial means preventing the cyberadversary from achieving the—his objectives. Resilience is ensuring that our systems will continue to perform their essential military tasks, even when they are contested in the cyber environ-

ment. And cost imposition is our ability to make our adversaries pay a much higher price for their malicious activities than they hoped for.

I'd like to briefly discuss these three elements:

To deny the attacker the ability to adversely impact our military missions, we have to better defend our own information networks and data. And we think the investments we have made in these capabilities are starting to bear fruit. But, we recognize that technical upgrades are only part of the solution. Nearly every single one of the successful network exploitations that we have had to deal with can be traced to one or more human errors which allowed entry into our network. So, raising the level of individual cybersecurity awareness and performance is absolutely paramount. Accordingly, we're working to transform our cybersecurity culture, something that we ignored for a long time, by—the long term, by improving human performance and accountability in this regard.

As part of this effort, we have just recently published a cybersecurity discipline implementation plan and a scorecard that is brought before the Secretary and me every month. And they are critical to achieving this goal of securing our data and our networks and mitigating risk to DOD missions. This scorecard holds commanders accountable for hardening and protecting their end points and critical systems, and also have them hold accountable their personnel, and directs, as I said, the compliance reporting to the Secretary and me on a monthly basis. The first scorecard was published in August of this year, and it is being added to and improved as we go.

Denial also means defending the Nation against cyberthreats of significant consequence. The President has directed DOD, working in partnership with our other agencies, to be prepared to blunt and stop the most dangerous cyberevents. There may be times where the President and the Secretary of Defense directs DOD and others to conduct a defensive cyberoperation to stop a cyberattack from impacting our national interests, and that means building and maintaining the capabilities to do that—just that.

This is a challenging mission requiring high-end capabilities and extremely high-trained teams. We're building our cyber mission force and deepening our partnership with law enforcement and the intelligence community to do that.

The second principle is improving resiliency by reducing the ability of our adversaries to attack us through cyberspace and protecting our ability to execute missions in a degraded cyber environment. Our adversaries' view DOD cyber dependency as a potential wartime vulnerability. Therefore, we view our ability to fight through cyberattacks as a critical mission function. That means normalizing cybersecurity as part of our mission assurance efforts, building redundancy whenever our systems are vulnerable, training constantly to operate in a contested cyber environment. Our adversaries have to see that these cyberattacks will not provide them a significant operational advantage.

And the third aspect of deterrence is having the demonstrated capability to respond, through cyber or noncyber means, to impose costs on a potential adversary. The administration has made clear that we will respond to cyberattacks in a time, manner, and place

of our choosing. And the Department has developed cyber options to hold aggressor at risk in cyberspace, if required.

Successfully executing our missions requires a whole- of-government and whole-of-nation approach. And, for that reason, DOD continues to work with our partners and the other Federal departments and agencies and the private sector and our partners around the world to address the shared challenges we face.

Secretary Carter has placed particular emphasis on partnering with the private sector. The Department doesn't have all of the answers and is working with industry. We think it will be very, very critical.

Finally, our relationship with Congress is absolutely critical. The Secretary and I very much appreciate the support provided to DOD cyberactivities throughout, from the very beginning, and we understand, and we are looking forward to the National Defense Authorization Act to see if there are other improvements that we have—we can do.

I encourage continued efforts to pass legislation on cybersecurity information-sharing—we think that is absolutely critical—data breach notification, and law enforcement provisions related to cybersecurity, which were included in the President's legislative proposal submitted earlier this year.

I know you agree that the American people expects us to defend the country against cyberthreats of significant consequence. The Secretary and I look forward to working with this committee and Congress to ensure we take every step possible to confront the substantial risks we face in the cyber realm.

Thank you again for inviting us here today and giving the attention that you have always given to this urgent matter.

I'd like to pass it off now to Admiral Rogers, if that's okay, Mr. Chairman.

[The prepared statement of Mr. Work follows:]

PREPARED STATEMENT BY ROBERT O. WORK

Chairman McCain, Ranking Member Reed, and members of the Committee, thank you for inviting me to discuss Department of Defense (DOD) efforts in cyberspace. The Department of Defense is currently implementing the DOD Cyber Strategy, published in April 2015, to improve our Nation's capabilities to conduct cyberspace operations and deter potential adversaries from engaging in malicious cyber activity against the United States.

CYBERSECURITY RISKS TO DOD NETWORKS AND INFRASTRUCTURE

Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting government and business activities, and imposing significant costs to the U.S. economy. State and non-state actors are conducting cyber operations, expanding their capabilities and targeting the public and private networks of the United States, our allies, and partners. These cyber threats continue to increase and evolve, posing greater risks to the networks and systems of the Department of Defense, our Nation's critical infrastructure, and U.S. companies and interests globally.

External actors probe and scan DOD networks for vulnerabilities millions of times each day and foreign intelligence agencies continually attempt to infiltrate DOD networks. Unfortunately, some incursions—by both state and non-state entities—have succeeded. The intrusion into the Office of Personnel Management security clearance systems compromised the personal information of millions of U.S. Government employees, their families, and their associates. In recent years, there have been several notable cyber intrusions on DOD networks, to include the Joint Staff

intrusion, and interception of DOD data not residing on DOD networks, e.g. the TRANSCOM and OPM intrusions.

Cyberattacks also pose a serious risk to networks and systems of critical infrastructure. The Department of Defense relies on U.S. critical infrastructure, as well as the critical infrastructure of our international partners, to perform its current and future missions. Intrusions into that infrastructure may provide access for malicious cyber actors who wish to disrupt critical systems in a time of crisis. Because of the potentially severe consequences, DOD is working with our partners in the interagency, private sector, and international community to ensure these systems are better protected and more resilient.

At DOD we are also increasingly concerned about the cyber threat to companies in our Defense Industrial Base. We have seen an unacceptable loss of intellectual property and sensitive DOD information that resides on or transits Defense Industrial Base unclassified systems. This loss of key intellectual property has the potential to damage our national security as well as impede economic growth by eroding U.S. technical superiority.

CYBER THREATS

Malicious actors are also targeting U.S. companies. At the end of last year, North Korean actors attacked Sony Pictures Entertainment in the most destructive cyberattack against a U.S. company to date. North Korea destroyed many of Sony's computer systems, released personal and proprietary information on the Internet, and subsequently threatened physical violence in retaliation for releasing a film of which the regime disapproves. The President stated that the United States will pursue an appropriate response to the incident—which he said would be reserved for a time, place, and manner of his choosing. To date the United States has publicly attributed the attack to the North Korean government, and in January 2015 the President signed new sanctions Executive Order in response to North Korea's provocative, destabilizing, and repressive actions and policies.

North Korea isn't our only adversary that has engaged in cyberattacks. Iran has also conducted cyberattacks against private sector targets to support its economic and foreign policy objectives, at times concurrent with political crises. Iranian actors have been implicated in the 2012–13 DDOS attacks against US financial institutions and in the February 2014 cyberattack on the Las Vegas Sands casino company. Iran very likely views its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes, as well as a sophisticated means of collecting intelligence.

Chinese cyber espionage continues to target a broad spectrum of US interests, ranging from national security information to sensitive economic data and US intellectual property. Although China is an advanced cyber actor in terms of capabilities, Chinese hackers are often able to gain access to their targets without having to resort to using advanced capabilities. Improved US cybersecurity would complicate Chinese cyber espionage activities by addressing the less sophisticated threats, and raising the cost and risk if China persists.

Russia's Ministry of Defense is establishing its own cyber command, which—according to senior Russian military officials—will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations. Computer security studies assert that Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures. Unknown Russian actors successfully compromised the product supply chains of at least three ICS vendors so that customers downloaded malicious software (malware) designed to facilitate exploitation directly from the vendors' websites along with legitimate software updates, according to private sector cyber security experts.

Non-state actors also continue to be very active in conducting malicious cyber activities. Terrorist groups, including ISIL, experiment with hacking which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers conduct low level cyberattacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors. With respect to ISIL, since last summer, the group began executing a highly strategic social media campaign using a diverse array of platforms and thousands of online supporters around the globe.

Profit motivated cyber criminals continue to successfully compromise the networks of retail businesses and financial institutions in order to collect financial information, biographical data, home addresses, email addresses, and medical records that serve as the building blocks to criminal operations that facilitate identity theft

and fraud. These criminals rely on loosely networked online marketplaces, often referred to as the cyber underground, that provide a forum for the merchandising of illicit tools, vulnerabilities, services, infrastructure, stolen personal identifying information, and financial data.

The combination of these diverse cyber threats results in a complex and challenging threat environment. To conduct a disruptive or destructive cyber operation against a military or industrial control system requires expertise, but a potential adversary need not spend millions of dollars to develop an offensive capability. A nation-state, non-state group, or individual actor can purchase destructive malware and other capabilities through the online marketplaces created by cyber criminals, or through other black markets. As cyber capabilities become more readily available over time, the Department of Defense assesses that state and non-state actors will continue to seek and develop malicious cyber capabilities to use against U.S. interests.

DOD'S CYBER STRATEGY

In response to the growing cybersecurity threats and to guide the Department's efforts to defend our Nation against cyberattacks of significant consequence, we developed the 2015 DOD Cyber Strategy. Our new cyber strategy, the Department's second, guides the development of DOD's cyber forces and strengthens our cybersecurity and cyber deterrence posture.

The strategy focuses on building cyber capabilities and organizations for DOD's three primary cyber missions: to defend DOD networks, systems, and information; defend the Nation against cyberattacks of significant consequence; and provide cyber support to operational and contingency plans. To accomplish these missions, the strategy sets five strategic goals:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;
2. Defend the DOD information network, secure DOD data, and mitigate risks to DOD missions;
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages; and,
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

In support of these goals, we are building the Cyber Mission Force, training it to conduct full-spectrum cyberspace operations, and equipping it with the tools and infrastructure it needs to succeed. This force is composed of four types of teams: 68 Cyber Protection Teams to defend priority DOD networks and systems against significant threats; 13 National Mission Teams to defend the United States and its interests against cyberattacks of significant consequence; 27 Combat Mission Teams to provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations; and 25 Support Teams to provide analytic and planning support to the National Mission and Combat Mission Teams. Once fully manned, trained, and equipped in Fiscal Year 2018, these 133 teams will execute DOD's three primary missions with nearly 6,200 military and civilian personnel. However, many of these developing teams are already adding significant cyberspace capabilities to DOD now, as they actively conduct critical ongoing missions while building their operational capacity.

As we continue to strengthen the Cyber Mission Force, we recognize the need to incorporate the strengths and skills inherent within our Reserve and National Guard forces. Each Service, therefore, has developed Reserve Component integration strategies that provide a total force cyber capability and leverage the Reserve and National Guard strengths from their experience in the private sector. Up to 2,000 Reserve and National Guard personnel will also support the Cyber Mission Force by allowing DOD to surge cyber forces in a crisis.

As Secretary Carter has stated, the development of a cadre of cyber experts—both in and out of uniform—is essential to the future effectiveness of U.S. cyber capabilities, and we are committed to ensuring that the workforce for the cyber domain is world class. To that end, we must develop and retain a workforce of highly skilled cybersecurity specialists with a range of operational and intelligence skill sets. This cyber workforce must include the most talented experts in both the uniformed and civilian workforce, as well as a close partnership with the private sector.

The Department is taking a hard look at barriers and challenges to recruitment, retention, employment, compensation, promotion, and career progression for DOD's cyberspace workforce. We are developing recommendations that could provide the

Department, USCYBERCOM, and the Service Cyber Components with the workforce management authorities and flexibilities that would strongly enable the successful execution of their cyberspace missions and responsibilities. Section 1104 of the National Defense Authorization Act currently under conference is a vitally important step to help DOD attract, hire, and retain a world class cyber workforce.

The Department is aggressively implementing our Cyber Strategy across all three missions and five goals. We have developed detailed outcomes, milestones, timelines, and metrics for each objective in the DOD Cyber Strategy. Additionally, in accordance with Section 932 of the Fiscal Year 2014 National Defense Authorization Act, we have established a cross-functional, interdepartmental team to support the Principal Cyber Advisor to oversee its execution, coordinating with all DOD stakeholders, and proactively addressing potential obstacles. As we implement the strategy, we are also taking a number of steps to improve budgeting and accounting for the Cyber Mission Force across the Department and appreciate your continued support on these issues.

DETERRENCE

Deterrence is a key mission for the Cyber Mission Force in the new DOD Cyber Strategy. Deterrence is a function of perception; it works by convincing a potential adversary that the costs of conducting an attack outweigh any potential benefits. DOD needs the ability to deter or prevent disruptive and destructive cyberattacks, preempt an imminent cyberattack, halt an ongoing cyberattack, and respond to cyberattacks. To do that, DOD must develop on-the-shelf capabilities that could have the ability to affect an adversary's behavior by shaping the environment, controlling escalation, and imposing costs. Additionally, we must strengthen our overall resilience posture so that DOD networks and systems can continue to operate even while under attack. Denial, resilience, and response are key components to a holistic deterrence strategy, expanding well past just the cyber domain.

DENIAL

First, as a part of our strategy we must increase our denial capabilities to tilt any adversaries' cost-benefit analysis in our favor. To deny an attack from adversely affecting our military missions, we must first defend our own information, networks, data, and systems. We are focused on two aspects of denial: strengthening DOD's cybersecurity; and defending the nation against cyberattacks of significant consequence.

As Secretary Carter has said, the first of our three missions is to defend our own information networks, data, and systems. Without secure systems, we cannot do any of our missions. So, the DOD is working to implement best in class technical solutions. We are standardizing our boundary defenses under the Joint Information Environment, providing linkages from our intelligence capabilities for early warning, while including state of the art commercial technologies to create comprehensive capabilities across the cyber kill chain and enable dependable mission execution in the face of highly capable cyber adversaries. As a foundational element to achieve this, we are globally deploying the Joint Regional Security Stacks (JRSS) to significantly reduce the avenues of attack into our unclassified and classified networks, support advanced threat analytics and improve responsiveness to attack. This will allow increased security and visibility, ensuring that commanders can see and respond to threats in order to determine risk to mission. The Department has also embarked on a new scorecard system that will hold commanders accountable for hardening and protecting their endpoints and critical systems. However, we also recognize that technical upgrades and organizational changes are only part of the solution when it comes to effective cybersecurity. Nearly all successful network exploitations can be traced to one or more human errors, so raising the level of individual human performance in cybersecurity will provide us with tremendous leverage in defending DOD networks. Accordingly, we are closely considering how we can transform DOD cybersecurity culture for the long term by improving human performance and accountability.

The President has directed DOD to work in partnership with other agencies to be prepared to blunt and stop the most dangerous attacks from succeeding. There may be times when the President or the Secretary of Defense may direct DOD and others to conduct a defensive cyber operation to stop a cyberattack from impacting our national interests. This is DOD's mission: to defend the nation against cyberattacks of significant consequence—which may include loss of life, destruction of property, or significant foreign and economic policy consequences. It means building and maintaining capabilities to prevent or stop a potential cyberattack from achieving its effect.

This is a challenging mission. It requires high-end capabilities and highly trained teams. We are building our Cyber National Mission Force and deepening our partnerships with law enforcement and the intelligence community to do it.

RESILIENCE

Improving DOD's resilience will reduce the incentive for adversaries to attack us through cyberspace and protect our ability to execute missions in a degraded cyber environment. This means normalizing cybersecurity as part of our mission assurance efforts, building redundancy wherever our systems are vulnerable, and training constantly to operate in a contested cyber environment. To deter our adversaries, they must see that cyber-attacks will not provide them with significant operational advantage.

DOD also relies on civilian and international infrastructure to execute its missions. We partner with the interagency, the private sector, and other countries to ensure the cybersecurity and resilience of the critical infrastructure on which we all rely. Organizations across the country are beginning to recognize the importance of resilient systems. IT companies and critical infrastructure owners and operators are driving market supply and demand towards more secure IT products and services, and that is great news.

RESPONSE

Finally, in the event of a potential cyberattack on U.S. interests, the United States must be able to respond through cyber or non-cyber means to impose costs on a potential adversary. Throughout this Administration, we have made clear that the United States will respond to cyberattacks in a time, manner, and place of our choosing.

Therefore a key objective of the DOD Cyber Strategy is to develop cyber options to hold an aggressor at risk in cyberspace if required. To support our deterrence posture, DOD is investing significantly in our Cyber Mission Force, including robust intelligence and warning capabilities to better identify malicious actors' tactics, techniques, and procedures in order to improve attribution in cyberspace. These attribution capabilities have increased significantly in recent years, and we continue to work closely with the intelligence and law enforcement communities to maintain and continue to improve them through intelligence collection and forensics.

But in many instances, non-cyber capabilities may provide a more appropriate or effective response. The Administration reviews the whole range of options, such as diplomatic engagement, network defense and law enforcement measures, economic or financial sanctions, or even the use of kinetic capabilities. Responses will be selected on a case by case basis, and be conducted consistent with law.

BUILDING STRONG PARTNERSHIPS

Successfully executing our missions in cyberspace requires a whole-of-government and whole-of-nation approach. DOD continues to work with our partners in other federal Departments and agencies, the private sector, and countries around the world to address the shared challenges we face. We work particularly closely with our partners in the Department of Homeland Security and Department of Justice to ensure collaboration in cyber operations and information sharing across the federal government, and we have seen tremendous advancement in our ability to work as a single, unified team.

We also work closely with our partners and allies to ensure that we maintain a strong collective defense against cyber threats. Through cooperation, shared warning, capacity building, and joint training activities, international engagement provides opportunities for an exchange of information and ideas to strengthen our cybersecurity as well as that of our allies and partners. Our partners are increasingly prioritizing cybersecurity as a key national security issue, creating opportunities and new areas for cooperation. We cooperate with, and assist, a wide range of partners.

Additionally, Secretary Carter has placed a particular emphasis on partnering with the private sector. We need to be more creative in finding ways to leverage the private sector's unique capabilities and innovative technologies. The Department does not have all the answers, and working with industry will be critical to we remain at the cutting edge of technology to protect our nation. We are examining ways to expand our collaboration with industry and are developing incentives and pathways to bring more cyber expertise into the Department.

Finally, our relationship with Congress is absolutely critical. As the President has said many times, Congressional action is vital to addressing cyber threats. I appreciate the support provided for DOD cyber activities throughout the 2016 National

Defense Authorization Act. And, I encourage continued efforts to pass legislation on cybersecurity information sharing, data breach notification, and law enforcement provisions related to cybersecurity, which were included in the President's legislative proposal submitted earlier this year.

CONCLUSION

It is my job is to make sure that our strategy is effectively implemented across the Department, and ensure that DOD is moving forward coherently and comprehensively in performing its assigned cybersecurity roles. The American people expect us to defend the country against cyber threats of significant consequence, and I look forward to working with this Committee and the Congress to ensure we continue to take every step necessary to confront the substantial cybersecurity risks we face. Thank you, again, for the attention you are giving to this urgent matter. I look forward to your questions.

STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN, COMMANDER, U.S. CYBER COMMAND; DIRECTOR, NATIONAL SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICES

Admiral ROGERS. Chairman McCain, Ranking Member Reed, and distinguished members of the committee, I am honored to appear before you today to discuss U.S. cyber policy and the state of cyberthreats worldwide. I'd like to thank you for convening this forum and for your efforts in this important area.

I'm also honored to be sitting alongside Director Clapper and Deputy Secretary of Defense Work.

It gives me great pride to appear before you data—today to highlight and commend the accomplishments of the uniformed and civilian personnel of U.S. Cyber Command. I'm both grateful for and humbled by the opportunity I have been given to lead our cyber team in the important work they do in the defense of our Nation and our Department.

We are being challenged as never before to defend our Nation's interests and values in cyberspace against states, groups, and individuals that are using sophisticated capabilities to conduct cybercoercion, cyberaggression, and cyberexploitation. The targets of their efforts extend well beyond government and into privately-owned businesses and personally identifiable information. Our military is in constant contact with agile, learning adversaries in cyberspace, adversaries that have shown the capacity and the willingness to take action against soft targets in the United States.

There are countries that are integrating cyberoperations into a total strategic concept for advancing their regional ambitions. They use cyberoperations both to influence the perceptions and actions of states around them and to shape what we see as our options for supporting allies and friends in a crisis. We need to deter these activities by showing that they are unacceptable, unprofitable, and risky for the instigators.

U.S. Cyber Command is building capabilities that can contribute to cross-domain deterrence, and thus, make our commitments even more credible. We are hardening our networks and showing an opponent cyberaggression won't be easy. We are creating the mission force, trained and ready like any other maneuver element that is defending DOD networks, supporting joint force commanders, and helping to defend critical infrastructure within our Nation. We are partnering with Federal, foreign, and industry partners, and exercising together regularly to rehearse concepts and responses to de-

structive cyberattacks against critical infrastructures. We are generating options for commanders and policymakers across all phases of the conflict, and particularly in phase zero, to hold at risk what our adversaries truly value.

The demand for our cyberforces far outstrip supply, but we continue to rapidly mature, based on real-world experiences and the hard work of the men and women of U.S. Cyber Command and our service cybercomponents, as well as our broader partners.

I'd like to assure the committee that U.S. Cyber Command has made measurable progress. We are achieving significant operational outcomes, and we have a clear path ahead.

With that, thank you again, Mr. Chairman and members of the committee, for convening this forum, inviting all of us to speak. Our progress has been made possible in no small part because of the support from this committee and other stakeholders. Unity of effort within our Department and across the U.S. Government in this mission set is essential. And I appreciate our continued partnership as we build our Nation's cyberdefenses. And I welcome your questions.

[The prepared statement of Admiral Rogers follows:]

PREPARED STATEMENT BY ADMIRAL MICHAEL S. ROGERS

Chairman McCain, Ranking Member Reed, and distinguished members of the Committee, thank you for the opportunity to speak to you today about the implementation of our military strategy in cyberspace. It is an honor to appear today beside Director James Clapper and Deputy Secretary of Defense Robert Work as well. Let me also mention the great and justified pride I take in the privilege of speaking on behalf of the men and women of United States Cyber Command (USCYBERCOM) and the vital work they undertake to defend our nation. Their efforts, guided by the new DOD Cyber Strategy and supported by the indispensable contributions of the National Security Agency (which I also head), are improving our cyber security with the Department of Defense (DOD) and our ability to generate a greater range of options with cyber to support policy makers and operational commands. All of this helps keep our fellow citizens safe and advance our national interest overseas.

In line with the DOD Cyber Strategy, USCYBERCOM and its components perform three primary missions. First, we are responsible for securing, operating, and defending Department of Defense systems and networks, which are fundamental to the execution of all Department of Defense missions. Second, the Department of Defense and the nation rely on us to build ready cyber forces and to prepare to conduct cyber operations to deter or defeat strategic threats to the nation. Third, we work with the Combatant Commands to integrate cyber operations into broader military missions. Our military is already engaged in cyberspace. Potential adversaries scan DOD networks for vulnerabilities millions of times daily. As we have repeatedly seen, vulnerability in one place can be a weakness across an entire network and systems built as "administrative" networks are now on the front lines of our operations. This reality has serious implications for our nation's security, as well as for our military.

We are at a strategic inflection point where the great promise and opportunity offered by cyberspace innovation has also made it easier for potential adversaries to find vulnerabilities that they can use to threaten us. The DOD Cyber Strategy seeks to generate and align a multi-faceted effort within the Department against an unprecedented and growing challenge. In announcing the Strategy last April, Secretary Carter noted that threats are proliferating and diversifying. Digital tools in cyberspace give adversaries cheap and ready means of doing something that until recently only one or two states could afford to do: that is, to reach beyond the battlefield capabilities of the U.S. military. They have demonstrated the capacity to hold "at risk" our military and even civilian infrastructure. In lay terms, that means that decades of military investment is now imperiled, because as Secretary Carter says, our forces depend on the functioning of our military networks and combat systems, without which they, and we, are far less effective in all domains.

How do we know this, and what does it mean? Recent events have made this trend clear, and we know it because of our intelligence analysis. We have recently seen Russian and Chinese-sponsored intrusions in United States information systems—penetrations that were designed to (and in some cases did) gain persistent presence in the targeted networks. And of course, no one missed the North Korean attack on Sony Pictures Entertainment last year, when a state turned its cyber capabilities against a private U.S. corporation, stealing its intellectual property, damaging its property, disrupting its operations, invading the privacy of its employees and affiliates, and threatening its customers and suppliers. We have also observed that energy firms and public utilities in many nations (including the United States) have had their networks compromised by state cyber actors.

Secretary Carter has also noted the risk of miscalculation and escalation resulting from malicious cyber actions, and Deputy Secretary of Defense Work recently told an audience in London that conventional deterrence is eroding to a worrisome degree. Addressing that risk in the cyberspace domain is the point of the DOD Cyber Strategy—to defend, and show we can defend, and thus to preserve the effectiveness of our "traditional" instruments of national power. Let me illustrate one important way in which we are implementing this strategy, with a quick historical detour for context.

PREPARING TO RESPOND

Our military has found ways to adapt to new technologies, strategies, and tactics in the past. For instance, we exercised the U.S Army in Louisiana in April 1940 and learned that the sort of trench warfare that had dominated battlefields in the last World War had subsequently been overtaken by events—or more precisely, by tanks, dive bombers, and mobile infantry, all coordinated by radio. The Fall of France to the German blitzkrieg barely two months later showed what happened to nations that failed to heed recent advances in military art—a German force with fewer tanks and guns routed the French and British armies in just six weeks. Our War Department incorporated this lesson and returned to Louisiana in the summer of 1941 to test its new concepts. This time the U.S. Army, augmented by National Guard formations, ran two maneuvers, ultimately involving half a million troops. The first phase showed that the blitzkrieg could indeed be stopped, and the second showed that our Army could mount a blitzkrieg of its own. Those extended exercises gave us invaluable experience, prompting changes to doctrine, weapons, and concepts.

The Louisiana Maneuvers could not foreordain victory in World War II, of course, but they helped prepare our military for a new and global conflict by giving officers and soldiers the opportunity and latitude to experiment and even fail at employing new weapons, tactics, and modes of operation. Those maneuvers also drove home the point of the experimentation: to practice being agile, not just defending but being ready and able to go on the offensive and hit back, taking the fight to the opponent. That is just the sort of experimentation we must continue doing today. Then-Army Chief of Staff George C. Marshall was questioned about the expense of such large maneuvers by a Senator who also pointed out that the exercises had witnessed a lot of mistakes by the forces involved. Marshall characteristically responded respectfully but firmly: "I want the mistake [made] down in Louisiana, not in Europe." Discovery learning in the midst of real-world operations, as the British and French experienced in 1940, can be disastrous. The DOD Cyber Strategy is intended to enable us to learn in peacetime how to succeed in cyberspace operations under all conditions. Today we have "lessons learned" instead of mistakes, of course, and we are doing so in Virginia, where last summer we staged for the fourth time our large, annual exercise that we call CYBER GUARD.

We inaugurated the CYBER GUARD exercise series to test the "whole of nation" response to a major cyber incident affecting the DODIN and U.S. critical infrastructure. USCYBERCOM offices work with experts from the Joint Staff and the joint cyber headquarters elements, Cyber Mission Force teams, U.S. Northern Command, National Guard, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), state governments, allies, and the private sector. Our defenders battle in the exercise networks against a world class "opposing force" to make this nearly three-week event as realistic as possible. The idea is to train our forces to operate as they would in an actual cyber crisis—i.e., against live opposition and alongside the federal, state, allied, and industry partners who would also have authorities and equities in such an event. Over a thousand participants, including representatives from critical infrastructure partners and National Guard teams from 16 states, practice how to collectively protect the nation along with DOD networks. Participants from the Department of Defense practice lending appropriate support

to civil authorities, and doing so on a complex exercise network that takes months to fine tune in advance of CYBER GUARD.

This latest iteration of CYBER GUARD was the largest and most realistic yet. Participants got to "maneuver" in cyberspace—seeking to see, block, and ultimately expel from the network adept opponents who had the advantages of knowing what they wanted to take (or break) and who swiftly learned their way around "our" systems. Our defenders thus experienced some of the fast-paced uncertainty of a real cyber campaign, when major decisions have to be made on the fly without the benefit of full insight into the adversary's intentions and capabilities. Players at CYBER GUARD fought through a relentless pace of events and learned that they have to trust each other for their efforts to mesh together and prove effective. To build that trust, moreover, there is no substitute for the sharing of both their information and experiences. Exercises like CYBER GUARD not only teach commanders and units how to see, block, and maneuver in cyberspace, they teach our Soldiers, Sailors, Airmen, and Marines to be teammates, both with one another and with colleagues in other parts of the federal government and private sector who we work beside to make cybersecurity effective.

CYBER GUARD showed us ways to improve our exercising of the total force and also highlighted areas where our attention is needed. This will sound familiar to many Members here assembled. I raise them to provide you with an accurate picture of the challenges in building capability and operating in the dynamic cyberspace domain.

A good analogy here is to the way our military has developed special operations forces. Our special operations forces are as good as any in the world, as we have seen over the last decade and more. Few people realize, however, what it takes for a special operations team in the field to execute a mission. They have an intensive need for critical enablers. This is the case for any maneuver element, and cyber teams are no exception. We have through CYBER GUARD and other exercises and operations a host of mission critical requirements that we are actively acquiring, building, or seeking. The Department and the government are reviewing the scope of authority for our cyber forces, including command and control relationships, manpower guidance, and development authorities to acquire the specialized tools and service we require. We are training cyber warriors and educating cyber professionals, both in the Service schoolhouses and in tailored settings. We are building out the Cyber Mission Force teams, aligning them to missions, customizing their intelligence support, assigning them to commanders, and assessing their readiness (indeed, CYBER GUARD served as a certification event for several teams; among them were teams deployed on real-world missions just weeks later). Across the cyber workforce we are setting the right mix of military and civilian personnel, and working to harmonize the several civilian hiring and career systems that take care of our people who work under parallel but not always equivalent institutional templates.

In particular, we are building a dedicated, persistent training environment, like DOD utilizes in each of the other domains. Let me explain what it is that we are doing. CYBER GUARD took place in Joint Staff facilities in Suffolk, Virginia, giving us the opportunity to practice in a controlled but more or less realistic cyber environment that we did not have to set up ourselves and then tear down after the exercise finished. Nonetheless, this was not the same as exercising in an environment specifically designed to mimic conditions on the Internet and the real world of cyberspace, where industry partners, for instance, are independently taking steps (such as updating malware signatures and even outing cyber actors) to defend their own systems. While we defend DOD networks, of course, we are helping our federal partners to guard US Government systems as well. We need greater realism to reflect this reality in our training. With the help of the DOD Central Information Officer and others, we are now building out and testing a new exercise environment and working on interagency exercises and testing environments with partners including DHS.

Last but not least is our requirement for vital cyber infrastructure improvements to operate DOD systems safely even under attack. I have explained our need for the Unified Platform and the Joint Information Environment in previous hearings, but I will reiterate how important they are to the defense of DOD's systems and our ability to operate and deliver effects outside the United States. These improvements are the future, for they represent a revolutionary and much-needed change to the Department of Defense Information Networks (DODIN). In addition, though information sharing alone is not a silver bullet, it is critical that the government and private sector be able to share information that will enhance the situational awareness we need to protect our nation and its interests. I am encouraged by the work that has gone into cybersecurity information sharing legislation in both the House

and the Senate. But it is imperative that we finish that work and pass a cybersecurity information sharing bill as soon as possible. Cyber criminals are not waiting to steal intellectual property or financial data, so neither should Congress wait to pass this important legislation. These steps are needed to ensure that cyber remains a strategic asset, not a liability, at this strategic inflection point.

IMPLEMENTING THE DOD CYBER STRATEGY

Recall Secretary Carter's earlier point: if we cannot defend the infrastructure that undergirds our DOD bases and forces from foreign-based cyber threats, then our nation's military capabilities are weakened and all our instruments of national power diminished. That leaves our leaders with a need for additional options to pursue short of open hostilities, and with fewer capabilities in an actual clash of arms. This raises risk for all by inviting instability and miscalculation, as the Secretary noted.

Our nation has peer competitors in cyberspace, with other nations and groups also striving to deploy advanced cyber capabilities. They do not match our entrepreneurial élan, our manufacturing skill, or our deep investment in the theory and machinery of cyberspace. Yet they have already hinted that they hold the power to cripple our infrastructure and set back our standard of living if they choose. They know, of course, that we can hit back, and that potentially devastating cyberattacks against U.S. interests would ripple across the global economy. But they could well count on deterring us in a regional crisis, making our leaders hesitate and muffle American responses to aggression overseas. Such delays could give them time to continue their encroachments, attain their objectives, and consolidate their gains.

We need to understand the systemic-level implications of what is happening. We are, in effect, being strategically shaped by potential adversaries. They also feel entitled to turn the resources of their states against private business, research labs, academic institutions, and even individual citizens in the West to steal the fruits of our creativity, or negatively impact the enjoyment of human rights and fundamental freedoms, including the freedom of expression.

This context adds the sense of urgency we feel at USCYBERCOM and across the Department of Defense. How do we prevent potential adversaries from shaping us and deterring our defense of America's interests and allies? We know that the DOD Cyber Strategy gained the attention of countries overseas—this enhances deterrence right here. But that is only one step of many. We need to take several more steps as we implement that Strategy.

First, we have to continue the whole-of-government coordination that makes our words and actions far more meaningful to potential adversaries. As Secretary Carter stated in announcing the DOD Cyber Strategy, we need synchronized inter-agency measures to bring all the powers and authorities of the U.S. Government to bear on malicious cyber actors. Individual sanctions, indictments and other steps are effective tools, but they might not be sufficient by themselves because potential adversaries believe they have too much to gain from continued cyber-enabled theft of our intellectual property and continued intimidation of their neighbors through cyberspace (among other mechanisms, of course).

Second, we must deepen our partnerships. Organizations across the U.S. Government must create consistent, complementary approaches for operating with private sector and international partners—leveraging the comparative advantages of civilian, homeland security, law enforcement, intelligence community, and military entities. Many departments and agencies share the authorities and responsibilities to guard critical infrastructure in the United States, and we look to DHS' Industrial Control Systems Computer Emergency Readiness Team (ICS–CERT) for information-sharing, incident response and mitigation. We as a nation need to enhance governing policies and legal frameworks to enable a robust defense of the defense industrial base and other sectors of our critical infrastructure. This could include efforts across the Government to identify and manage risks to our critical infrastructure and key resources in the near term, while transitioning from a reactive to a deterrent posture over the long term.

Finally, we must forge a consensus on when we can and should respond to cyber activity directed against the United States. Such a consensus should clarify the proper role of the military in a whole-of-nation approach to improving our security in the cyberspace domain. The President has stated that we reserve the right to respond with all instruments of national power to cyberattacks against our critical infrastructure. Here is where we particularly need to build trust in the ability of the U.S. Government—on the civilian and military sides—to exercise its powers and capabilities responsibly to defend the nation, consistent with international law and norms. I see my job in this entailing an effort to better explain certain concepts like

"offensive cyber operations" and the Cyber Mission Force. I welcome your ideas on this.

CONCLUSION

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak on behalf of USCYBERCOM about the vital topic of cyberspace strategy. Our Command is helping the Department and the federal government mitigate risk while unleashing the promise and opportunity inherent in cyberspace in ways consistent with our values as a nation. As you can tell from the foregoing, I take pride in the accomplishments of our men and women. I know they will give their all in executing our Command's missions and in forging cyber forces that offer our nation's leaders a full suite of options in cyberspace and beyond. With their great efforts and your continued support, I know we can be positioned for success, despite the seriousness of the current situation. There is no single technical or engineering fix alone that is going to solve these challenges, but instead we will require a great deal of the fortitude, creativity, and determination that we Americans have repeatedly shown we can muster. I look forward to your questions and to advancing this important dialogue.

Chairman MCCAIN. Well, thank you, Admiral. And thank the witnesses.

Director Clapper, recently former Chairman of the Joint Chiefs Dempsey was asked about various threats to the United States security, and he said that, in a whole range of threats, we have a significant advantage, except in cyber. Do you agree with that assessment?

Director CLAPPER. It's probably true. We haven't, I guess, exhibited what our potential capability there is, so I think that's one of the implicit reasons why I have highlighted cyberthreats in the last three years of my worldwide threat assessments.

Chairman MCCAIN. I thank you. And you have done that, I think, at least great effect before this committee. As a result of the leader—the Chinese leader in Washington, there was some agreement announced between the United States and China. Do you believe that that will result in a elimination of Chinese cyberattacks?

Director CLAPPER. Well, hope springs eternal.

Chairman MCCAIN. Yeah.

[Laughter.]

Director CLAPPER. I think we will have to watch what their behavior is, and it will be incumbent on the intelligence community, I think, to depict—portray to our policymakers what behavioral changes, if any, result from this agreement.

Chairman MCCAIN. Are you optimistic?

Director CLAPPER. No.

Chairman MCCAIN. Thank you.

Admiral Rogers, you recently stated, quote, "There's a perception," there is, quote, "little price to pay for engaging in some pretty aggressive behaviors, and, because of a lack of repercussions, you see actors, nation-states, indeed, willing to do more." And that was what you stated. What is required? What action is required to deter these attacks, since there's little price to pay? What do we have to do to make it a heavy price to pay?

Admiral ROGERS. So, I think we have to clearly articular, in broad terms, what is acceptable and unacceptable, norms, if you will, of behavior. I think we have to clearly articulate that, as a nation, we are developing a set of capabilities, we are prepared to use those capabilities if they're required. They're not necessarily our preference. We clearly want to engage in a dialogue with those

around us. But, on the other hand, we do have to acknowledge the current situation we find ourselves in. I don't think there's anyone who would agree that it is acceptable and that it is in our best long-term interest as a Nation.

Chairman MCCAIN. Well, I say with respect, I understand it's not acceptable, but, in other words, what would enact a price? Would it be relations in other areas? Would it be counterattacks? What—in other words, what actions would be in our range of arsenals to respond?

Admiral ROGERS. So, I think it's potentially all of those things. The first comment I would make, I think Sony is a very instructive example. One of the things I always remind people of, we need to think about deterrence much more broadly, not just focus within the cyber arena. I thought the response to Sony, where we, for example, talked about the economic options as a Nation we would exercise, was a good way to remind the world around us that there's a broad set of capabilities and levers that are available to us as a Nation, and that we're prepared to do more than just respond in kind, if you will.

Chairman MCCAIN. One of the—Director Clapper, one of the things that's been disappointing to the committee is that, in the fiscal year defense authorization bill, as you know, it required the President to develop an integrated policy. The strategy is now a year late. Can you tell us where we are in that process and what you feel is—what might bring the administration in compliance?

Director CLAPPER. You're asking me about policy development?

Senator REED. Yes.

Director CLAPPER. I think I would defer to Secretary Work on that.

Mr. WORK. Well, Mr. Chairman, as we have said over an over, we believe our cyberdeterrence strategy is constantly evolving and getting stronger.

Chairman MCCAIN. I'm talking about a policy, not a strategy, Mr. Secretary. It required a policy, the Fiscal Year '14 National Defense Authorization Act.

Mr. WORK. The policy is still in development. We believe we have a good cyberstrategy. The policy has been outlined in broad strokes by the——

Chairman MCCAIN. Not broad enough, I would think. Does it describe what our—whether we deter or whether we respond or whether we—in other words, as far as I know and the committee knows, that there has been no specific policy articulated in compliance with the requirement to—in the Defense Authorization Act. If you believe that it has, I would be very interested in hearing how it has.

Mr. WORK. I believe the broad strokes are, we will respond to——

Chairman MCCAIN. I'm not asking broad strokes. Suppose there is an attack—a cyberattack like the one on OPM. Do we have a policy as to what we do?

Mr. WORK. Yes, we do.

Chairman MCCAIN. And what is that?

Mr. WORK. The first is to try—first, we deny and then we would—we first find out—we do the forensics——

Chairman MCCAIN. I'm not asking the methodology. I'm asking the policy. Do you respond by counterattacking? Do you respond by trying to enact other measures? What do we do in case of a cyberattack?

Mr. WORK. We respond in a time, manner, and place of our choosing.

Chairman MCCAIN. Does that mean that we counterattack?

Mr. WORK. That may be one of the options. It's as——

Chairman MCCAIN. That's not a policy, Secretary Work. That is a—that is an exercise in options. We have not got a policy. And for you to sit there and tell me that you do, "a broad-stroke strategy," frankly, is not in compliance with the law.

Senator Reed.

Senator REED. Well, thank you very much, Mr. Chairman.

Director Clapper, we are constantly engaged in, euphemistically, information operations with many other nations, and they're involved with information operations, trying to, as you indicated in your testimony, influence the opinion, disguise activities, disrupt, et cetera. What agencies are—under your purview or outside your purview, are actively engaged in information operations to the United States in the cyberworld?

Director CLAPPER. Actually, sir, in—from an intelligence perspective, we would feed that, in that we don't, at last in what I can speak to publicly, engage in that as a part of our normal intelligence activity. So, we feed other arms, support other arms of the government, not only the State Department and those responsible for messaging.

Senator REED. Right.

Director CLAPPER. The National Counterterrorism Center has an office that is devoted to, in a countering-violent- extremism context, helping to develop themes or recommending themes based on what we glean from intelligence as—for potential vulnerabilities and messages that would appear to various groups, to obfuscate the message, disrupt it, or compete with it. But, generally speaking, intelligence, writ large, doesn't actively engage in information operations.

Senator REED. From your perspective, are these other agencies that you provide information to adequately resourced and staffed so they can use it effectively, or are they getting a lot of good insights and sitting around wondering what they can do——

Director CLAPPER. If I were king, which I am not, I think I would have a much more robust capability from the standpoint of the resource commitment to countermessaging.

Senator REED. And that would fall with—outside the purview of intelligence, more the State Department and some other agencies.

Director CLAPPER. Correct.

Senator REED. And I think we're all going to remember the Voice of America, when it was a—you know, a pretty dominant sort of—source of information.

Director CLAPPER. Well, personal opinion only, not company policy, I would, I think perhaps, you know, a USIA on steroids that would address these messages more broadly and more robustly. But, that's strictly personal opinion.

Senator REED. But, I think, in terms of what you're observing, particularly some of our competitors have a—extraordinarily robust operation. They don't lack for resources or personnel, and they're constantly engaged in these types of information operations—enhancing their image, discrediting their opponents, actively engaging local groups in other countries of interest, et cetera—and we're sort of on the sidelines more.

Director CLAPPER. I think that's quite right. And our—in contrast to us, the Russian intelligence services are very active and very aggressively engaged in messaging.

Senator REED. Thank you.

Admiral Rogers, to this issue of encryption that Director Comey pointed to, I think your thoughts would be very helpful.

Admiral ROGERS. So, the issue that we find ourselves—this is less for me, on the U.S. Cyber Command side and much more on the NSA side—is—communications in the world around us increasingly going to end-to-end encryption, where every aspect of the path is encrypted, and the data and the communication is protected at a level that, with the current state of technology, is difficult to overcome. Clearly, that's in the best interests of the Nation, in broad terms. And strong encryption is important to a strong Internet defense, and a well-defended Internet is in our best interests as a Nation and the world's best interests.

Within that broad framework, though, the challenge we're trying to figure out is—realizing that that communication path is used by very law-abiding citizens, nation-states, and companies engaged in lawful activity, it is also being used by criminals, terrorists, nation-states who would attempt to generate advantage against the United States and against our allies and partners. And so, we're trying to figure out, How do we balance these two important imperatives of privacy and security? And realizing that it's a technical world around us, and it's changing in a foundational way. And so, we're trying to come to grips, broadly, with, How do we deal with the reality of the technical world around us, and yet the broader legal and social imperatives we have?

I'm the first to acknowledge we do not have a defined way ahead here. In the end, I think this is about, How do we get the best minds together as a nation to address this? Because, when I look at our capabilities as a nation, there is no problem we can't overcome when we work together in an integrated way to—in the private sector, industry, business, the academic world. I think that's the way ahead here, in broad terms.

Senator REED. Thank you very much.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Sessions.

Senator SESSIONS. Thank you, Mr. Chairman.

Senator Inhofe is chairing an EPW Committee. That's why he couldn't be here today.

You've given us a good summary on the threats that we face and the threats that are actually occurring today. And I appreciate that.

Senator McCain asked you about reporting on other policy that Congress has asked you to report on, and that not having been done. Mr.—Secretary Work, in the 2014 NDAA, the Senate and

House agreed on a provision that required the services to report on the cyber vulnerabilities of weapons and communication systems connected by networks. That's something that came out of our Strategic Subcommittee on a bipartisan basis, and was eventually expanded to include all weapon systems, not just satellites and missiles and national missile defense. We don't have that final report. I believe it's overdue. This budget, I believe, has 200 million in it to help fund this effort. What can you tell us about that?

First, let me say, it may take some time. If it does, that's—I understand. But, I don't think we've had any report from the DOD to state that—what progress you've made and how much longer it will take.

Mr. WORK. Well, again, on both of the points—on the policy, we expect that is in the final deliberations. It's an interagency effort. You know, generally, trying to establish norms and deterrence is central to the policy. Again, it's the denial, resilience, and cost-imposition. I'm the first to admit that we are the farthest ahead on the denial and the resilience part. Those are the areas where we are moving faster. The cost-imposition part, because we have elected to retain the retaliatory mechanism of cyberattacks at the national level, just like nuclear weapons, because of the risk of escalation——

Senator SESSIONS. What about the——

Mr. WORK. As far as the—oh, I'm sorry, sir.

Senator SESSIONS.—the other——

Mr. WORK. Yes, sir. As far as——

Senator SESSIONS.—the vulnerabilities of our weapon systems?

Mr. WORK. It is a big, big problem. Most of the—many of the weapon systems that we have now were not built to withstand a concerted cyberthreat. So, going through every single one of the weapon systems, what Frank Kendall has done is, he's prioritized the weapon systems, and he is working through very carefully. And I expect this work to be done very soon. We now have new requirements in our KPPs, our key performance parameters——

Senator SESSIONS. So, you have assigned a—an individual——

Mr. WORK. Absolutely.

Senator SESSIONS.—to be responsible for this?

Mr. WORK. Yes. Frank Kendall is the one who is going through all of the different—working with, obviously, our CIO [Chief Information Officer], also the Cyber Command, and the—all of our cyber experts. But, he's responsible for taking a look at the weapon systems and also requiring KPPs [Key Performance Parameter], key performance parameters, for new weapon systems so that, when we build them, they will have cyberdefenses built in from the beginning.

Senator SESSIONS. What about our defense contractors, Admiral Rogers? They maintain and build these systems and have highly sensitive information. Are we satisfied they're sufficiently protected?

Admiral ROGERS. So, we certainly acknowledge there's a vulnerability there. We've been very public about our concerns about foreign nation-states trying to access some of our key operational technology through penetrations in the clear defense contract arena for us. We've made changes to the contractual relationships be-

tween us and those companies, where they have to meet minimum cybersecurity requirements, they have to inform us, now, of penetrations. We're clearly not where we need to be, but we continue to make progress.

Senator SESSIONS. Well, I think it's a bipartisan commitment on Congress to help you with that.

Secretary Work, if it takes more money, let us know. We'll have to evaluate it. And I also understand that some of the protections can be done without much cost; some may require considerable cost. So, we hope that you will complete that.

Admiral Rogers, you, I believe, last week, reported, in the Los Angeles Times, about the threat from China. You note one thing, that they are involved in obtaining U.S. commercial and trade data in a foreign nation, advanced nation, ally of ours. I was told that they—one of their companies bid on a contract, and that the Chinese had got all the bid data from the Web. And his comment was, "It's hard to win a bid when your competitor knows what you're bidding."

Admiral ROGERS. Yes, it is.

Senator SESSIONS. Is that kind of thing happening?

Admiral ROGERS. It has been. We've very—been very public of it. I think that's reflected in the agreement that you saw raised during the President of China's visit last week, where we were very explicit about that concern.

Senator SESSIONS. Well, my time is up, but I would just ask——

You're not allowed—if you saw an American business being damaged through improper action, you're not allowed to advise them or share any information with them, while our adversaries do assist their businesses. Is that basically correct?

Admiral ROGERS. The way this works right now is, I would provide information and insight both in my intelligence hat as the Director of NSA, as well as the Commander of U.S. Cyber Command. If, under that authority, I became aware of activity, I would share the insights with DHS and the FBI, who have a mission associated with interfacing with the private sector in a much more direct way than I do.

Chairman MCCAIN. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

And thank all three of you for your service and for being here today.

Admiral Rogers, if—I'll start with you. Which country is the most committed, determined, and successful hacker of the U.S.?

Admiral ROGERS. Could you say that one more time, Senator?

Senator MANCHIN. Which country do you believe is the most committed, successful hacker of the U.S.?

Admiral ROGERS. If you look at volume, nation- statewide—nation-state-wides, I would—China, the PRC, has been the one that we've been the most vocal about. They're not the only one, by any stretch of the imagination.

Senator MANCHIN. I thought the last time you were here you said that—I recall you saying that you had more concerns over Russia having more of the ability or the expertise to do us damage.

Admiral ROGERS. I thought your question was really focused more on volume. If your—if the perspective is capability, if you

will, then we have been very public about saying I would probably put the Russians——

Senator MANCHIN. Russians.

Admiral ROGERS.—in a higher capability.

Senator MANCHIN. But, it seems like that China is more committed and determined to do it.

Admiral ROGERS. They certainly do it at a volume level——

Senator MANCHIN. Gotcha. I understand.

And, Director Clapper, if I may, I know that you just said no—emphatically no, you don't believe that this agreement that the President of China and our President has made last week will work. With that saying—what are the—is there any penalties in this agreement if one or the other violates it? Or is it just basically, well, we have agreed, and let it go at that?

Director CLAPPER. The terms that I——

Senator MANCHIN. As you understand it.

Director CLAPPER. The terms that I have seen, I don't think it treats, specifically, penalties. There certainly are implied penalties. I think the threat of economic sanctions that—which brought Minister Mung to this country, I think is illustrative of what would mean something to the Chinese if they transgress or violate this agreement.

And I think, as Admiral Rogers was discussing earlier, there—with respect to sanctions, there certainly whole- of-government possibilities here. Don't have to do, necessarily, a cyber eye for an eye. It can be some other form of retaliation.

But, I don't think—to answer your question, at least what I'm aware of—that there are specific penalties if the agreement is violated.

Senator MANCHIN. And that's why I think you were pretty quick in saying you don't think it'll work. You said no to that, I think, when the Chairman asked you.

Director CLAPPER. Well, the reason I said no, of course, is—the extent to which Chinese purloining of our data, our intellectual property, is pretty pervasive. I think there's a question about the extent to which the government actually orchestrates all of it, or not. So, I think we're in the—to model—to borrow a President Reagan term, "trust but verify" mode, at least as far as intelligence is concerned. And we are inherently skeptics.

Mr. WORK. Sir, could I add something?

Senator MANCHIN. If I could—I have a question for you, Secretary, and then you can go ahead and add to that.

There's a news—the recent news article that examined similarities between China's J–31 fighter and our F–35 strike finder and what they're been able to do in such a rapid period of time, without any R&D. Do you believe that that gives them a competitive advantage? I mean, you can—I understand there might be some differences as far as in the software or in the weaponry and this and that, but they're making leaps, which are uncommon, at the behest of us. And we know this, I understand, but we're not taking any actions against them.

Mr. WORK. Well, I'd like to work this in to your——

Senator MANCHIN. Yes.

Mr. WORK.—and follow up with your——

Senator MANCHIN. You go ahead.

Mr. WORK.—first question.

At the highest levels, we have made it clear that we believe that Chinese actions in the cybersphere are totally unacceptable as a nation-state. And we made that clear in a wide variety of different ways. And I would characterize the agreement that we have as a confidence-building measure with the Chinese, where we are asking them to prove to us that they are serious about what they say about what they will do to control these efforts.

So, we—there were really four things that we agreed to do. First, we would give timely responses to information when we say, "Hey, we believe that there is a problem here"—and we have agreed to exchange information on cybercrimes, we have agreed to possibly collect electronic evidence and to mitigate malicious cyberactivity if it's occurring on our soil. We both agree that we would not knowingly conduct cyber-enabled theft of intellectual property, which, as you say, Senator, has been a problem. We have told them it's a problem, that it's unacceptable. They have said that they will work to curb that. Then we've agreed to have common effort to promote international norms. And the final thing is, we'll have a high-level joint mechanism, where we can meet at least twice a year and say, "Look, this is just not working. You are not coming through with what you've said."

So, this isn't a treaty or anything like that. It's a confidence-building measure for us to find out if China is going to act responsibly. I agree totally with Director Clapper. They've got to prove to us. And we know that they have stolen information from our defense contractors.

Senator MANCHIN. Right.

Mr. WORK. And it has helped them develop systems. And we have hardened our systems through the Defense Industrial Base Initiative. And we're trying to make——

Senator MANCHIN. But, I'm saying we know the J–20 is pretty much mirroring our F–22. We know that their J–31 is pretty much mirroring our F–35. When we know this and the cost to the American taxpayers, and let them get—I mean, why wouldn't we tale hard actions against them? Or why wouldn't we come down—I just don't understand why we wouldn't retaliate——

Mr. WORK. Well——

Senator MANCHIN.—from a financial standpoint.

Mr. WORK. There are a wide variety of cost-imposition options that we have. They are developed through the interagency. And again, it's not necessarily kind—I mean, tit-for-tat. It is proportional response. And we're working through all of those right now.

Senator MANCHIN. My time is up, sir.

And if I could just follow up on that later, if we can meet with you later, I'd——

Mr. WORK. Absolutely, sir.

Senator MANCHIN.—very much appreciate it.

Director CLAPPER. Senator, if I may just add a word here about—this is a point Admiral Rogers has made in the past about, you know, terminology, lexicon, nomenclature definitions are important. And so, what this represents, of course, is espionage—economic——

Senator MANCHIN. Absolutely.

Director CLAPPER.—cyber espionage. And, of course, we, too, practice, cyber espionage. You know, in a public forum to, you know, say how successful we are, but we're not bad at it. So, when we talk about, "What are we going to do for—to counter espionage or punish somebody or retaliate for espionage," well, we—I think it's a good idea to at least think about the old saw about people who live in glass houses——

Senator MANCHIN. Gotcha.

Director CLAPPER.—shouldn't throw rocks.

Chairman MCCAIN. So, it's okay for them to steal our secrets that are most important——

[Laughter.]

Director CLAPPER. I didn't say that——

Chairman MCCAIN.—including our fighter, because——

Director CLAPPER. I didn't say that, Senator.

Chairman MCCAIN.—because we live in a glass house. That is astounding.

Senator Ayotte.

Director CLAPPER. I did not say it's a good thing. I'm just saying that both nations engage in this.

Senator AYOTTE. I want to thank all of you for being here.

With regard to the Chinese, I want to follow up on—we've talked about the stealing of the highest secrets, in terms of our weapon system, but what about the 21 million people whose background check and personal information has been, of course, associated publicly with the Chinese, and the fact that we know that 5 million sets of fingerprints, as well, leading to potential vulnerability for our citizens? And if you put that in the context of these other issues that we've raised, it seems to me—I looked very carefully, for example, Secretary Work, at some of the language you've been using. You gave a speech at the Royal United Services Institute in London. You said, "Deterrence must be demonstrated to be effective."

Secretary Clapper, in your prepared statement, you said, "The muted response by most victims to cyberattacks has created a permissive environment."

So, I'm trying to figure out, based on what you've said, how we're not in a permissive environment, in light of what they've stolen on our weapon systems, but also this huge infringement on 21 million people in this country.

And also, could you comment on the vulnerability of that data and where we are, in terms of how it could be used against us?

Director CLAPPER. Well, first, that is an assessment of what was taken. We actually don't know, in terms of specific—specifics. But, that's—I think frames the magnitude of this theft. And it is potentially very serious—has very serious implications, first, close to home, from the standpoint of the intelligence community and the potential for identifying people who may be under covered status, just one small example. And, of course, it poses all kinds of potential—and, unfortunately, this is a gift that's going to keep on giving for years.

So, it's a very serious situation. What we've tried to do is educate people what to look for and how to protect themselves. But, again, this is a huge threat—theft, and it has, potentially, damaging im-

plications for lots of people in the intelligence community and lots of people in the Department of Defense and other employees of the government.

Senator AYOTTE. So, I think what you're hearing from some of us up here is just a—″Now what are we going to do about it?" is the issue, as opposed to a shared agreement on generic principles with the Chinese. This is a pretty significant issue that is going to impact millions of Americans. I'm not hearing what we're going to do about it, but that may be a higher-level decision, going up to the President. But, seems to me if we're going to talk about deterrence, if we don't follow up with action, and if you look at that, combined with the testimony we heard last week about the artificial islands being built by the Chinese, and the fact that we won't even go within, I believe it's 12 nautical miles of those islands—if you put that all from the Chinese perspective, I think you think, "Hmmm, we can pretty much do what we want to do, because we haven't seen a response."

Now, I'm not asking for—from all of you—to answer that, because it probably needs to be answered by the President and his national security team, but it seems to me that they aren't seeing a response right now from us, and therefore, we're going to see—continue to see bad behavior from the Chinese.

Before I go, I have an important question on another topic, Secretary Work, and that is: Yesterday, we heard public reports about a potential violation of the INF Treaty by the Russians, and that, essentially, Russia tested—flight tested a new ground-launched cruise missile this month that United States intelligence agencies say further violates the 1987 INF Treaty. And, of course, this is going back, also, to the reports, as early as 2008, of the—Russia conducting tests of another ground-launched cruise missile, in potential violation of the INF Treaty that we've raised with them. And, when Secretary Carter came before our committee, on his confirmation, he listed three potential responses to these INF violations. So, now we have the Russians violating the INF Treaty yet again. And I guess my question is: Secretary Carter rightly identified that we should respond, either through missile defense, counterforce, or countervailing measures. What are we doing about it?

Mr. WORK. Senator, this is a longstanding issue that we have been discussing with the Russians. The system that you're talking about is in development, it has not been fielded yet. We are—we have had different discussions with them on our perception of the violation of the INF, and they have come back. This is still in discussions, and we have not decided on any particular action at this point.

Senator AYOTTE. So, are you saying that you don't think they violated the INF Treaty?

Mr. WORK. We believe very strongly that they did.

Senator AYOTTE. That's what I thought. So, what are we going to do about it? Because they're claiming that they haven't, going back to the 2008 violations, and now here we have another situation.

Mr. WORK. It's still under—because they have not fielded the system, we are still in the midst of negotiating this position. We

are giving ours. But, if they do field a system that violates the INF, I would expect us to take one of the three options that Secretary Carter outlined before the committee.

Senator AYOTTE. So, my time is up, but I see two consistent themes here, both with the Chinese and the Russian: a lot of talk, no action, unfortunately. And people take their cues from that. And that worries me.

Thank you all.

Chairman MCCAIN. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman.

Director Clapper, you testified before the House Intelligence Committee recently that the—while the United States makes distinctions between cyberattacks conducted for economic purposes or to gain foreign intelligence, I would—that's the espionage arena, I think, that you're referring to—or to cause damage, our adversaries do not. Would you consider the OPM breach, to the extent that we believe it is a state actor who did that, that that would be in the category of espionage?

Director CLAPPER. Yes.

Senator HIRONO. The——

Director CLAPPER. That was the tenor of the discussion at the HTSC hearing that Admiral Rogers and I engaged in. And, of course, that has to do with the—as I mentioned earlier to Senator Manchin, the importance of definition, nomenclature, and terms. So—and the definition of these terms—and so, what—the theft of the OPM data, as egregious as it was, we wouldn't necessarily consider it as an attack. Rather, it would——

Senator HIRONO. Yes.

Director CLAPPER.—be a form of——

Senator HIRONO. Well, and——

Director CLAPPER.—theft or espionage.

Senator HIRONO. And, as you say, other countries, including our own, engages in such activities.

My understanding of the recent agreement between the United States and China, though, has to do with commercial cybertheft. And I think that's a very different category that has to do with obtaining information about corporations, et cetera. And therefore, that that is in the category of economic attacks. So, Director Clapper, would you consider that kind of an agreement to be helpful? I realize that you are skeptical, but, to the extent that we are defining a particular kind of cyberattack, and that we're contemplating, through this agreement, an ability of our two countries to engage in high-level dialogue regarding these kinds of attacks, is that a helpful situation?

Director CLAPPER. Well, it would be very helpful if, of course, the Chinese actually live up to what they agreed to. So, if—and what the agreement pertained to was theft of data for economic purposes to give Chinese commercial concerns an advantage, or their defense industries an advantage, as opposed to—I don't believe they—that we've agreed with the Chinese to stop spying on each other.

Senator HIRONO. Yes.

Director CLAPPER. And so, there is a——

Senator HIRONO. The——

Director CLAPPER.—for purely espionage purposes—and there is a distinction.

Senator HIRONO. Mr. Secretary, you can weigh on this also. To the extent that we've created an—a potential for a dialogue or an environment where there's a process to be followed, and the cases where we suspect commercial cyberattacks, that at least we have a way that we can talk to the Chinese. Because you also mentioned, Director Clapper, that attribution is not the easiest thing, although we are getting better at figuring out who actually were the actors who that did these cyberattacks. So, one hopes that, even with a great deal of skepticism, going forward, that this agreement may create the space for us to have a—more than a conversation, but one that would lead to some kind of a change in behavior on the part of these state actors.

Mr. Secretary, feel free to give us your opinion.

Mr. WORK. Senator, I think that's exactly right. I mean, as Director Clapper said, first you have to find out the geographical location from the—where the attack came from. Then you have to identify the actor, and then you have to identify whether the government of that geographic space was either controlling——

Senator HIRONO. Recognize that's not the easiest to do, yes.

Mr. WORK. And what we have done is, we have confronted China, and China, in some cases, has said, "Look, this was a hacker that was inside our country, but we had no control over him." What this allows us to do is say, "Okay, well, what are you going to do about that? That's a cybercrime. Are you going to provide us the information we need to prosecute this person? Are you going to take care of it on your own?" So, I believe this type of confidence-building measure and this way to discuss these things will—the proof will be in the pudding, how the Chinese react to this——

Senator HIRONO. Mr. Secretary, I think you mentioned that this particular agreement allows—contemplates meeting at least twice a year.

Mr. WORK. Yes.

Senator HIRONO. Is there anything that prevents more frequent dialogue between our two countries in suspected cases of commercial cyberattacks?

Mr. WORK. Senator, I believe, if there was a significant cyber event that we suspected the Chinese of doing or they suspected us, that we would be able to meet this. This is going to be a high-level joint dialogue. They'll—the Chinese will have it at the ministerial level. Our U.S. Secretary of Homeland Security and the U.S. Attorney General will co-lead on our part. We're going to have the first meeting of this group by the end of this calendar year, and then at least twice a year. So, I believe that, as Director Clapper is, I think all of us have some healthy skepticism about this, but I believe it's a good confidence-building measure and a good first step, and we will see if it leads to better behavior on the part of the Chinese.

Senator HIRONO. Thank you.

Chairman MCCAIN. Mr. Secretary, I can't help but comment. We have identified the PLA [People's Liberation Army], the building in which they operate. Now, please don't deceive this committee as if we don't know who's responsible for it. That's just very disingen-

uous. There have been public reports that we've identified the PLA building in which these cyberattacks come from.

Senator Ernst.

Senator ERNST. Thank you, Mr. Chair.

Thank you, gentlemen, for joining us today.

Admiral Rogers, I'll start with you, sir.

Admiral ROGERS. Okay.

Senator ERNST. Two of the President's nine lines of effort in defeating ISIL [Islamic State of Iraq and the Levant] are, first, exposing ISIS's [Islamic State of Iraq and Syria] true nature and, second, disrupting the foreign fighter flow. And, over the weekend, the New York Times reported that 30,000 recruits joined ISIS over the past year, and that's double the previous recruitment year.

Earlier this month in reference to ISIS recruiting, the State Department's Ambassador-at-Large and Coordinator for Counterterrorism said that ISIS's recruiting trend is still upward, and this information came of no surprise to her. The Ambassador also said the upward trend was primarily due to Internet and social media.

So, sir, do you believe the administration's efforts have so far succeeded on these two lines of effort in cyberspace and social media? Just, please, simple yes or no.

Admiral ROGERS. No.

Senator ERNST. Okay. In light of that, with the record recruiting numbers for ISIS, how would you then assess the effectiveness of the U.S. Government's counter-ISIS effort in cyberspace? So, what specifically is your assessment of the State Department's "think again, turn away" program in support of efforts to disrupt ISIS's online recruiting effort?

Admiral ROGERS. Senator, I'm not in a position to comment on State Department—the specifics of their program. I honestly am just not knowledgeable about it. I will say this, broadly, to get to, I think, your broader point. I have always believed that we must contest ISIL in the information domain every bit as aggressively as we are contesting them on the battlefield, that the information dynamic is an essential component of their vision, their strategy, and ultimately their success. And we have got to be willing to attempt to fight them in that domain, just like we are on the battlefield. And we clearly are not there yet.

Senator ERNST. I agree. I think we are failing in this effort. And some of the programs that we have seen obviously are not working. So, are there areas in—where you could recommend how the U.S. Government better partner with various NGOs [non-governmental organizations] or private entities to more effectively counter the ISIS propaganda?

Admiral ROGERS. Again, the contesting-the-propaganda piece, much broader than Cyber Command's mission. I will say, from a technical and operational perspective, we, broadly within the DOD, Cyber Command, Strategic Command, and CENTCOM, are looking at, within our authorities, within our capabilities, what's with—in the realm of the possible, in terms of, What can we do to help contest them in this domain?

Senator ERNST. Okay.

We have a larger problem coming forward, too, in regards to ISIS and ISIL in the Middle East. We seem to see the emergence of a

trifecta between Syria, Iran, and Russia. And now it seems that Iraq has begun information-sharing with Russia, with Iran, with Syria. Director Clapper, can you speak to that and the broader implications of Russia emerging as a leader in the Middle East while we seem to be frittering away our opportunity with ISIL?

Director CLAPPER. Well, that's certainly their objective. I think they have several objectives, here, one of which is that—I think, protect their base, the—their presence in Syria, ergo their buildup in the northwest part of Syria; clearly want to prop up Assad; and, I think, a belated motivation for them is fighting ISIL.

As far as the joint intelligence arrangement is concerned, I can't go into detail here in this forum, but I will say there are—each of the parties entering into this are a little bit suspicious of just what is entailed here, so we'll have to see just how robust a capability that actually provides.

Senator ERNST. Okay, I appreciate that.

And, Secretary Work, do you have any thoughts on the emergence of Russia with the intelligence-sharing, how that might impact the operations that we have ongoing in Iraq against ISIS?

Mr. WORK. Well, I think we were caught by surprise that Iraq entered into this agreement with Syria and Iran and Russia. Obviously, we are not going to share intelligence with either Syria or Russia or Iran. So, we are in the process—our—we are in the process of working to try to find out exactly what Iraq has said. Certainly, we're not going to provide any classified information or information that would help those actors on the battlefield. Really what we're trying to do is deconflict, and that is the primary purpose of the discussion between President Obama and President Putin yesterday—is, "If you are going to act on this battlefield, we have to deconflict."

The other thing we have made clear is—they would like to do a military first, followed by a political transition. We need—we believe those two things have to go in parallel, and that has been our consistent message. This is early days. We're still in the midst of discussing what exactly this means, so I don't have any definitive answers for you at this point, Senator.

Senator ERNST. Well, I am very concerned that we have abdicated our role in the Middle East as—and in so many other areas, as has been pointed out earlier. Grave concern to all of us. And I think we need to be working much more diligently on this.

Thank you, Mr. Chair.

Chairman MCCAIN. Senator Nelson.

Senator NELSON. Thank you, Mr. Chairman.

Gentlemen, thank you for your public service.

Admiral, I'm concerned about all of these private telecoms that are going to encrypt. If you have encryption of everything, how, in your opinion, does that affect Section 702 and 215 collection programs?

Admiral ROGERS. It certainly makes it more difficult.

Senator NELSON. Does the administration have a policy position on this?

Admiral ROGERS. No, I think we're still—I mean, we're the first to acknowledge this is an incredibly complicated issue with a lot of very valid perspectives. And we're still, I think, collectively, trying

to work our way through, "So, what's the right way ahead, here?"—recognizing that there's a lot of very valid perspectives.

But, from the perspective, as Cyber Command and NSA, that I look at the issue, there's a huge challenge us—for us, here, that we have got to deal with.

Senator NELSON. A huge challenge. And I have a policy position, and that is that the telecoms better cooperate with the United States Government, or else it just magnifies the ability for the bad guys to utilize the Internet to achieve their purposes.

Speaking of that, we have a fantastic U.S. military. We are able to protect ourselves. It's a—it's the best military in the world. But, we have a vulnerability now, and it's a cyberattack. Do you want to see if you can make me feel any better about our ability to protect ourselves, going forward?

Admiral ROGERS. So, I would tell you the current stated capability in the Department, if I just look at where we were eighteen months ago, two years ago, is significantly improved. We currently defeat probably 99-point-some-odd percent attempts to penetrate DOD systems on a daily basis. The capability, in terms of both the amount of teams, their capability, just continues to improve. Our speed, our agility. The challenge for us, fundamentally, to me, is, we are trying to overcome decades of a thought process in which redundancy, defensibility, and reliability were never core design characteristics for our networks, where we assumed, in the development of our weapon systems, that external interfaces, if you will, with the outside world were not something to be overly concerned with. They represented opportunity for us to remotely monitor activity, to generate data as to how aircraft, for example, or ships' hulls were doing in different sea states around the world. All positives if you're trying to develop the next generation, for example, of cruiser/destroyer for the Navy. But, in a world in which those public interfaces, if you were, increasingly represent also potential points of vulnerability, you get this class of strategies, if you will. And that's where we find ourselves now.

So, one of the things I try to remind people is, it took us decades to get here. We are not going to fix this set of problems in a few years. This takes dedicated prioritization, dedicated commitment, resources, and we've got to do this in a smart way. We've got to prioritize, and we've got to figure out what's the greatest vulnerability and where's the greatest concern for us?

Mr. WORK. Senator, is it okay if I jump in here for a second?

Senator NELSON. Yes. I just want to add to that. And for us to let our potential enemies understand that we have the capability of doing to them what they do to us. However, that gets more complicated when you're dealing with a rogue group of a dozen people stuck in a room somewhere that are not part of a nation-state.

Yes, sir. Mr. Secretary.

Mr. WORK. Well, I was just going to echo what Admiral Rogers said. When Secretary Carter came in, he said, "Look, we are absolutely not where we need to be," and he made job number one defense of the networks. So, we're going from 15,000 enclaves to less than 500. We're going to have—we're going from 1,000 defendable firewalls to less than 200, somewhere between 50 and 200. So, you are absolutely right, we have recognized this is a terrible vulner-

ability. We are working, first, to defend our networks, as we talked about earlier. We're looking at our systems. And we're also trying to change the culture. Right now, if you discharge a weapon, you are held accountable for that. That's a—you know, negligent discharge is one of the worst things you can do. What we need to do is inculcate a culture where a cyber discharge is considered just as bad, and make sure that that culture is inculcated throughout the force.

Senator NELSON. I agree. But, now the Admiral is assaulted by the telecoms, who want to tie his hands behind his back by doing all of the encryption.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman.

In our State, Naval Surface Warfare Center Crane has taken the lead on much of our efforts to protect against the threat of counterfeit electronics. And so, Secretary Work and Director Clapper, the global supply chain for microelectronics presents a growing challenge for cybersecurity. One of the things we saw recently, IBM [International Business Machines] sold its chipmaking facilities with DOD "trusted foundry" status to a foreign-owned competitor. So, I was wondering your top priorities in managing the risk posed by the globalization of our microelectronics manufacturing capabilities and our abilities to protect our systems in that area.

Mr. WORK. That's a big question, Senator. In fact, it's going to be one of the key things we look at in this fall review, because of the recent—as you said, the recent sale of the IBM chips.

Now, there are two schools of thoughts on this. Secretary Carter personally has jumped into this. And some say you do not need a trusted foundry. Another group says you absolutely have to have it. Having confidence in the chips that we put in our weapon systems is important. And I would expect that, come February, we'll be able to report out the final decisions through the fall review on how we're going to tackle this problem.

Senator DONNELLY. Who within DOD's leadership has primary responsibility for overseeing the supply chain risk management?

Mr. WORK. That would be Frank Kendall and also DLA. DLA has the supply chain, and Frank Kendall is really focused on the trusted chip, the fabrication of trusted chips.

Senator DONNELLY. One of the areas that we look at in regards to cyber—and, in some ways, you know, technology in particular parts of it not advancing has been a good thing in this respect—is in the nuclear area. And so, are there any specific groups that are focused just on protecting our nuclear efforts against cyber?

Mr. WORK. There's the National—the NNSA [National Nuclear Security Administration]. And also, we have a Nuclear Weapons Council, which is cochaired by, again, Frank Kendall, our Under Secretary of Defense for AT&L, and the Vice Chairman of the Joint Chiefs. They are the ones that work with DOE [Department of Energy] to make sure that our weapon system components are reliable and trusted, and to make sure that we have a safe, reliable, and effective nuclear deterrent.

Senator DONNELLY. Admiral, when we look at building a force of cyber warriors, a cyber team, how can we use the National Guard

and Reserves to help do that? Because it strikes me that that can help us in retaining highly qualified individuals who want to devote part of their life to helping their country. And it would seem to almost be a perfect fit for us.

Admiral ROGERS. So, we have taken a total-force approach to the force that we're building out. That includes both Guard and Reserve. Every service slightly different, not the least of which because different services have different Reserve and Guard structures. So, that is a part of it.

I'd say one of the challenges that we're still trying to work our way through is under the Title 32 piece, how we coordinate what Guard and Reserve are doing, how we generate capacity and bring it to bear with maximum efficiency. The one thing—the two things, in partnering with my Guard teammates and my Reserve teammates—because we're taking a total-force approach to this, we need one standard for this. We don't want a place where the Guard and Reserve are trained in one standard and the Active side is trained to a different. That gives us maximum flexibility in how we apply the capability across the force. And the Guard and Reserve has done great in that regard. And then, secondly, we need one common unit structure. We don't want to build unique, one-of-a-kind structures in the Guard or Reserves that don't match the Title 10 side. Again, we want to treat this as one integrated force. And again, I would give the Guard and the Reserves great kudos in that regard. We've got a common vision about the way we need to go, and we've got a great exercise series, CYBERGUARD, that we're using every year, where we bring together the Guard, the private sector, the Active component, and government, and work our way through the specifics about how we're going to make this work.

Senator DONNELLY. Thank you.

Director Clapper—and I apologize if you already answered this—what is the one cyber challenge you are most concerned about?

Director CLAPPER. Well, obviously, the one that I think about is—would be a massive Armageddon-like-scale attack against our infrastructure. That is not—we don't consider that the most likely probably right now, that the greater threat—or the low-to-moderate sort of threats that we're seeing. And what I have seen in the 5 years I've been in this job is a sort of progression, where these get more aggressive and more damaging. And, as I indicated in my oral statement at the outset, what I will see—I think what we can expect next are data manipulation, which then calls to question the integrity of the data, which, in many ways, is more insidious than the kinds of attacks that we've suffered thus far.

So, you know, the greater—the specter is this massive attack, although it's not likely.

Senator DONNELLY. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Lee.

Senator LEE. Thank you, Mr. Chairman.

Annex 3 of the recently signed Iran Nuclear Agreement calls for the participating countries to work with Iran to, quote, "strengthen Iran's ability to protect against and respond to nuclear security threats, including sabotage, as well as to enable effective and sus-

tainable nuclear security and physical protection systems," close quote.

Secretary Clapper, do you read this portion of the Iran Nuclear Agreement, the Annex, to include cyberthreats, meaning that the P5+1 countries, who are part of this agreement, will be expected—will be deemed to have an obligation under the agreement to assist Iran in developing systems to prevent other countries from using cyber capabilities to acquire information about, or to disrupt the operations of, Iran's nuclear capabilities—Iran's nuclear programs?

Director CLAPPER. Well, in this environs, I will say that I trust that this is not going to prevent us from gleaning intelligence from our traditional sources, in the interests of verifying the agreement, which will be principally monitored by international organization, IAEA. So, I'm not aware of any strictures on our ability to collect on their behavior and their components.

Senator LEE. But, why would we want to give Iran the ability to defend against cyberweapons that we, or perhaps some of our allies, might one day want to use against Iran?

Director CLAPPER. Well, sir, in this open environment, there are some aspects here that I can't discuss. I'm happy to talk with you privately or in a classified environment about that.

Senator LEE. Okay. Okay. But, you're not disputing the fact that the agreement says that, that we would have to——

Director CLAPPER. No.

Senator LEE. Okay.

Now, can you tell me, in this environment, what specific technical assistance we'll be offering Iran in this portion of the agreement?

Director CLAPPER. I honestly don't know the answer to that question. I've—have to have that researched. I don't know exactly what would—what's in mind there.

Senator LEE. Now, would any of these capabilities, once acquired by Iran, prevent or inhibit the United States or any of our allies, any other enemy of Iran, from using any cybermeasure against Iranian nuclear facilities?

Director CLAPPER. Again, I—I'm reluctant to discuss that in this setting.

Senator LEE. Were you consulted by U.S. negotiators during the nuclear negotiations in connection with this portion of the agreement, the agreement——

Director CLAPPER. Well, the intelligence community was deeply involved in—throughout the negotiations.

Senator LEE. Can you describe the nature of any consultation you had with them as to this portion of Annex 3?

Director CLAPPER. With the Iranians?

Senator LEE. Yes.

Director CLAPPER. I—no, I did not engage with the Iranians on——

Senator LEE. No, no, that's not what I'm asking. I'm asking if you can describe your discussions with U.S. negotiators as they came to you and consulted with you on the implications of this portion of Annex 3.

Director CLAPPER. I didn't actually—my lead for this was Norm Roule, who was the—known to many of you on this committee, the

National Intelligence Manager for Iran. And he was the direct participant. And I—I don't want to speak for him as—to the extent to which he was involved or consulted on that provision. I'd have to ask him.

Senator LEE. Okay. But, you would have been aware of consultation going on. I mean, I'm sure he came to you and said, "Look, this is going to impact our ability, the ability of the United States, to do what we need to do with respect to Iran." That—would that not have been something——

Director CLAPPER. Well, again, sir, I would rather discuss what the potential response of ours could be in a closed setting.

Senator LEE. Okay.

Secretary Work, how is the Department working to ensure that the hardware and software on some of these major programs that we're developing to future contingencies and technological advances so they can continue to address emerging cyberthreats well into the future without major overhauls of the entire system?

Mr. WORK. Senator, as I said, we are now putting into our KPPs, our key performance parameters, on any new systems, specific cyber-hardening requirements, much like during the Cold War, when we had EMP [Electromagnetic Pulse] requirements for many of our systems. The problem that we face is that many of the old systems that are still in service were not built to the—to respond to the cyberthreats that we see today. So, we're having to go back through all of those older systems, determine which ones are most vulnerable, prioritize them, and make fixes. So—and it also goes back to Senator Donnelly's question on the trusted foundry. We're trying to determine what is the best way to assure that we have reliable and trust microelectronics.

Senator LEE. Okay. Thank you.

I see my time's expired.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator King.

Senator KING. Thank you, Mr. Chairman.

Secretary Work, if there's a catastrophic attack tonight on the fiscal infrastructure or the financial infrastructure of this country, I do not want to go on cable news in the morning, if there is cable news in the morning, and say, "The administration told us that the policy is still in development." We've got to get on this. We've been talking about it for years. And, as the Chairman pointed out, this was an essential part of our National Defense Authorization Act, a year ago, And the idea that we can continue to simply defend and never have an offensive capability, I just think is ignoring this enormous threat, which we all agree——

So, let me ask a one-word-answer question to each of you. Do we need an offensive capability in the cyber realm in order to act as a deterrent?

Secretary Work.

Mr. WORK. We need a broad range of response options, to include——

Senator KING. Do we need a offensive cybercapability to act as a deterrent?

Mr. WORK. I would say yes, sir.

Senator KING. Secretary—Director, go ahead.

Director CLAPPER. Absolutely.
Senator KING. Admiral Rogers.
Admiral ROGERS. Yes.
Senator KING. Thank you.

The second part of that is that it can't be secret. Our instinct is to make everything secret. And the whole point of a deterrent capability is that it not be secret. So, I think we need to establish what we have—I suspect we do have some significant offensive capability, but part of a—making it a deterrent is that it has to be made—it has to be made public.

I think another question that needs to be addressed—and I don't necessarily think it—in this hearing this morning, but in this—terms of the policy—we need to define what an act of war is in the cyber area, whether hitting Sony pictures is an act of war, or the OPM. And how do you draw those lines? And I would suggest that that's got to be part of this policy definition.

And I don't mean to imply, Secretary Work, that this is easy. But, it's urgent. That's the—and we just simply can't defend ourselves by saying, "Well, it was complicated and we didn't get to it."

Changing the subject slightly. Admiral Rogers, do you believe that the dispersion of responsibility in the Federal Government for cyber is a potential problem? It strikes me we've got agencies and departments and bureaus—I suspect you could name 15 of them if you tried—that all have some responsibility here. Do we need to strengthen Cyber Command and make that the central repository of this policy?

Admiral ROGERS. I would not make Cyber Command or the Department of Defense the central repository. This is much broader than just the DOD perspective. But, I will say this. I have been very public in saying we have got to simplify this structure for the outside world, because if you're on the outside looking in—and I hear this from the private sector fairly regularly—″Who do you want me to go to? Is it—I should talk to the FBI [Federal Bureau of Investigation]. Should I talk to DHS? Why can't I deal with you? Do I need to talk to the″—if I'm a financial company, "Should I be talking to the sector construct that we've created?" We have got to try to simplify this for the private sector.

Director CLAPPER. If I might add to that, Senator King, it's one of the reasons why I had a very brief commercial for—just within the intelligence community—of integrating the cyber picture, the common operating picture simply from within intelligence, let alone, you know, what we do to react or protect. And that, to me, is one important thing that I have come to believe. We need along the lines of a mini-NCTC [National Counterterrorism Center] or NCPC [National Counterproliferation Center].

Senator KING. I would hope that that would also—and that—the leadership and decisionmaking on that has to start with the White House, it has to start with the administration, for an all-of-government approach to dealing with this dispersion-of-responsibility problem.

I would point out, parenthetically, that—you know, we're—there's been a lot of talk about China and our ability to interact with China and to respond and hold China responsible. And it's not the subject of this hearing, but the fact that we owe China trillions

of dollars compromises our ability to interact with China in a firm way. It's a complicated relationship, and that's one of the things that makes it difficult.

Director Clapper, do you have any idea what brought the Chinese to the table for this recent agreement with the President?

Director CLAPPER. Well, it appears that the threat of potential economic sanctions, particularly imposing them right before the visit of President Xi, I think, got their attention. And that's why they dispatched Minister Maung to try to come to some sort of agreement, which is what ensued subsequently.

Senator KING. And I agree that it's not a definitive agreement or a treaty, but I do agree, Secretary Work, that it's a step in the right direction. At least these issues are being discussed. But, countries, ultimately, only act in their own self-interest, and we have to convince the Chinese that it's in their interest to cut out this activity that's so detrimental to our country.

Thank you, gentlemen, for your——

Mr. WORK. Senator, could I just make——

Senator KING. Yes, sir.

Mr. WORK.—one real quick comment?

Just because we have not published our policy—it is so broad and encompassing, going over things like encryption—What are the types of authorities we need?—does not mean that, if we did have an attack tonight, we would not—we do not have the structure in place right now with the national security team to get together to try to understand who caused the attack, to understand what the implications of the attack were and what response we should take. Those are in place right now.

Senator KING. But, the whole point of being able to respond is deterrence so that the attack won't occur. Dr. Strangelove taught us that if you have a doomsday machine and no one knows about it, it's useless. So, having a secret plan as to how we'll respond isn't the point I'm trying to get at. The deal is, we have—they have to know how we will respond, and therefore, not attack in the first place.

Thank you.

Thank you all, gentlemen, for your testimony.

Senator REED [presiding]. On behalf of the Chairman, let me recognize Senator Fischer.

Senator FISCHER. Thank you, Senator Reed.

Following up a little bit where Senator King was going on this, many of you talked about establishing norms in cyberspace. Do you think it's possible to establish or maintain that norm without enforcement behaviors? When we look at publicly identifying those who are responsible for an activity or imposing costs on them, can we do that? I'll begin with you, Mr. Secretary.

Mr. WORK. Well, I believe that trying to establish these norms are very, very helpful. In the Cold War, for example, there was a tacit agreement that we would not attack each of our early-warning missile—I mean, warning satellites. And so, establishing these norms are very important. But, they will be extremely difficult, because the enforcement mechanisms in cyber are far more difficult than—because it's much more easy to attribute missile attacks, et cetera. So, I believe that this agreement with China is a good first

step, that we should strive to establish norms, especially between nation-states—and establish norms which we believe are beyond the bounds, and to try to establish mechanisms by which we can work these through. But, this will be very, very difficult, Senator, because it's—because of the—just the—it's much more difficult.

Director CLAPPER. And we have the added problem, of course, of—the norms are, as Secretary Work said, really applicable to nation-states. And, of course, you have a whole range of non-nation-state actors out there who wouldn't necessarily subscribe to these norms and would be a challenge to deal with even if we—if there were nation- state mutual agreement.

Senator FISCHER. Admiral?

Admiral ROGERS. I would echo the comments of my two teammates. I'm struck by—we're all captives of our own experience. In my early days as a sailor, well before I got into this business, at the height of the Cold War out there, we knew exactly how far we—between the Soviets and us—we knew exactly how far we could push each other. And we pushed each other, at times, right up to the edge. I mean, very aggressive behaviors. But, at the—we developed a set of norms. We had a series of deconfliction mechanisms in the maritime environment. We actually developed a set of signals over time so we could communicate with each other. But, the—so, I'm comfortable that we're going to be able to achieve this over time in the nation-state arena, but, as my teammates have said, it's the nonstate actor that really complicates this, to me. It's going to make this difficult.

Senator FISCHER. So, when we're attacked in cyberspace, how do we impose costs on those who are attacking us? Do we respond in cyberspace, or can we look at other ways to, I think, respond in an appropriate manner, say with sanctions? What would you look at, Admiral?

Admiral ROGERS. So, what we have talked about previously is, we want to make sure we don't look at this just from one narrow perspective, that we think more broadly, we look across the breadth of capabilities and advantages that we enjoy as a nation, and we bring all of that to bear as we're looking at options as to what we do, and that it's a case-by-case basis. There's no one single one-size-fits-all answers to this. But, fundamentally, think more broadly than just cyber. Not that cyber isn't potentially a part of this. I don't mean to imply that.

Senator FISCHER. Correct.

Mr. Secretary, would you agree with the Admiral on that? Do you see a variety of options out there? And wouldn't it be more beneficial to us as a country to be able to have a policy that is a public policy on what those options could be, and the consequences that would be felt when we are attacked?

Mr. WORK. Absolutely. And that is what I say about a broad policy, where we will respond in a time manner—time, place, and manner of our own choosing. In this case, there's an asymmetry with our nation-state potential adversaries. They are all authoritarian states. The attack surfaces that they have are far smaller than what we have as a free nation. And we value that. We do not want to close down the Internet. But, we are more vulnerable to a wide variety of attack surfaces than our adversaries. So, we may

sometimes have to respond proportionally, but in a different way than a simple cyber response. It might be sanctions. It might be a criminal indictment. It might be other reactions. So, we believe very strongly that this is something where it's an interagency process. The process is established where they are taken care of——

Senator FISCHER. And——

Mr. WORK.—handled on a case-by-case basis.

Senator FISCHER. And does the administration have a definition on what constitutes a cyberattack?

Mr. WORK. Well, any type of malicious activity which causes either damage or theft of information or IP [Internet Protocol], all of those are under either cyber—malicious cyberactivities. It might be espionage. In each case, there's no defined red line for what would constitute——

Senator FISCHER. What's——

Mr. WORK.—act of war.

Senator FISCHER. What would be the difference between a cyberattack and cybervandalism?

Director CLAPPER. Well, I would have to make a—again, a case-by-case determination. And, of course, important consideration here would—in terms of our reaction, would be attribution. And that—again, it would be case-by-case.

Mr. WORK. And cybervandalism, ma'am, do you—is that stealing information or IP or——

Senator FISCHER. The attack by North Korea on Sony was described by the President as cybervandalism. I was just wondering on how you distinguish that definition from a cyberattack.

Director CLAPPER. Well, it didn't affect a national security entity, but it certainly did cause damage to the company. And, in that case—and this is an important illustration of when we could attribute very clearly and there was uniform agreement across the intelligence community to attribute that attack to the North Koreans, and we did sanction them.

Senator FISCHER. Okay, thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN [presiding]. Senator Heinrich.

Senator HEINRICH. Thank you, Mr. Chair.

Gentlemen, thank you for your service and for joining us here today.

And, Director Clapper, before I start on—begin to focus on cyberpolicy, I think we're all very concerned about the allegations that leadership at Central Command deliberately distorted the assessments of intelligent officers related to the fight against ISIL. And I understand that there is an ongoing investigation, and I'm going to wait for the results of that investigation. But, I want to say that, as a member of both this committee and the Intelligence Committee, I want to, in the strongest terms possible, impress upon you the importance for all of us to receive absolutely objective and unbiased assessments. And I look forward to the results of the IG investigation, and I expect that you will hold accountable anyone who has failed in their duty in the intelligence community, no matter how high up the chain that may go.

Director CLAPPER. Well, Senator, I—you brought up a very important consideration here, which is a great concern to me. I'm a

son of an Army intelligence officer who served in World War II, Korea, and Vietnam. And I have served in various intelligence capacities for over 52 years, ranging from my first tour in Southeast Asia in the early '60s to my service now as the longest tenured DNI. And it is a almost sacred writ in intelligence—in the intelligence profession never to politicize intelligence. I don't engage in it. I never have. And I don't condone it when it—it's identified.

Having said that, I—and I completely agree with you—in spite of all the media hyperbole, I think it's best that we all await the outcome of the DOD IG investigation to determine whether and to what extent there was any politicization of intelligence at CENTCOM.

I will also say that the intelligence assessments from CENTCOM or any other combatant command come to the national level only through the Defense Intelligence Agency. That is the main conduit and, I will say, to the extent evaluater and filter for what flows into the national intelligence arena.

Senator HEINRICH. Thank you, Director.

Turning to you, Admiral Rogers. As the director of U.S. Cyber Command, your responsibilities include strengthening our cyberdefense and our cyberdeterrence posture. And I want to return to a line of questioning several of my colleagues have begun this morning.

As you know, the breach of OPM computers resulted in an enormous loss of sensitive personal information. Thus far, to my knowledge, the U.S. has not responded. And to put it in the words of Deputy Secretary Work's language this morning, we haven't imposed a cost, which raises questions about whether we truly have developed the mechanisms for proportionate response to cyberattacks against the U.S. Government, even after the April 2015 publication of the DOD cyber strategy. We know that if a foreign agent had been caught trying to steal U.S. personnel files in a less digital age, we would either kick them out of the country, if they were a diplomat, or we'd throw them in jail, if they weren't a diplomat. That would be considered a proportionate response. But, in the case of the OPM breach, the U.S. Government seems uncertain about what a proportionate response would look like.

So, I want to ask you three questions, and I'll let you take them as you may: What constitutes an act of war in cyberspace? Has the United States decided on a proportionate response in the case of the OPM cyber espionage case? And what types of information-gathering by nation-states, by governments, are legitimate, and what types are not?

Admiral ROGERS. Well, first, let me start out by saying, look, so I'm the operational commander here, and all three of the questions you've just asked me are much broader than that. I'm glad to give you an opinion, but I'm mindful of what my role is.

In terms of the three things—Have we defined what an active of war is? The bottom line is: clearly, we're still working our way through that. What are the parameters that we want to use to define what is an act of war? My going-in position is, we ought to build on a framework that we have developed over time in the more conventional domains. That's a good point of departure for it.

It's got a broad legal framework. It's something that people recognize. And it's where we ought to start as a point of departure.

The second question was about—just let me read my note to myself——

Senator HEINRICH. Proportional response to the OPM case.

Admiral ROGERS. Again, I think that what OPM represents is a good question about—so, what are the parameters we want to use? Is it—as the DNI has said, is it—the intent is within the acceptable realm? Is it scale? Is it—you can do espionage at some level, for example, but if you trip some magic threshold, hey, is 20 million records, is 10 million records—is there some scale component to this? I think we're clearly still trying to work our way through that issue. And there is no one- size-fits-all answer. I think there's recognition. I think that's clearly—is what has driven this broad discussion between the United States and China, for example. That's been a positive, I would argue.

And the third, type—what—could you repeat again—the types of information?

Senator HEINRICH. Just—you know, I'll—my time is expired, so I'll cut to the chase. I think what you're hearing from all of us——

Chairman MCCAIN. No, go ahead, Senator. This is an important——

Senator HEINRICH.—is——

Chairman MCCAIN.—line of questioning.

Senator HEINRICH. We would like to see more transparency in being able to telegraph our deterrent, because we all know that—looking back into the Cold War, that our deterrent was very important. But, the other side knowing what that deterrent was, was absolutely critical for it to be effective. And so, we need to be clear about what types of information-gathering by governments are considered legitimate and acceptable, and where those red lines are going to be.

Admiral ROGERS. I agree. I think that's the important part of the whole deterrence idea. It has to be something that's communicated, that generates understanding and expectation, and then a sense of consequence.

Director CLAPPER. I think the contrast with the Cold War is a good one to think about, in that—well, I think what you're—what—the concern that people are raising is, Should there be red lines on spying? That's really what this gets down to. We didn't have red lines during the Cold War. It was freewheeling as far as us collecting intelligence against the Soviet Union, and vice versa. There were no limits on that. It was very difficult, for both—well, more so for us.

And, of course, underlying—the backdrop to all that was the deterrent, the nuclear deterrent, which, of course, restrained behavior even though it got rough at times, as the example that Admiral Rogers cited, in a—just in a maritime context. But, there were ground rules that governed that.

We're sort of in the Wild West here with cyber, where there are no limits that we've agreed on, no red lines, certainly on collecting information, and—which is what the OPM breach represented.

Chairman MCCAIN. Director and Admiral, I would like to thank you for your forthright and candid assessment. And also, I think,

the lesson that all of us are getting is that we really have to have some policy decisions. And you've been very helpful in fleshing that out for us.

Senator Cotton.

Senator COTTON. Secretary Work, I'd like to return to an exchange you had with Senator Ayotte about the Intermediate-Range Nuclear Forces Treaty, also known as the INF Treaty. Is Russia in violation of their obligations under the INF Treaty?

Mr. WORK. We believe that a system that they have in development would violate the treaty.

Senator COTTON. And you said, just now, "in development." I thought I heard you say, with Senator Ayotte, that it's not deployed, or it's not yet operationally capable. Is that correct?

Mr. WORK. That's my understanding. I can have—I can get back to you with a question for the record. But, it is in development, and we have indicated our concern with the Russians that, if they did deploy it, we believe it would violate the INF.

Senator COTTON. Thank you. Could you please do that in writing. And, if it's appropriate, in a classified writing, that's fine, as well.

[The information referred to follows:]

The Department finds that Russia is in violation of its obligations under the Intermediate-range Nuclear Forces (INF) Treaty not to possess, produce, or flight-test a ground-launched cruise missile with a range capability of 500 to 5,500 kilometers, or to possess or produce launchers of such missiles. Russia has built and tested a ground-launched cruise missile system that violates the Treaty.

Senator COTTON. I'd now like to move to the Cyber Mission Force. At the Air Force Association Conference a couple of weeks ago, Major General Ed Wilson, the commander of the 24th Air Force, stated that DOD's Cyber Mission Force was halfway through its buildup. How difficult is it to establish the needed infrastructure and manning across the services to create the capability that we need to defend and deter cyberthreats?

Mr. WORK. Well, I'd like to start, and then I'll turn it over to Admiral Rogers.

We're building to 133 total teams—68 are cyber protection teams that are focused on our number-one mission: defense of our networks. We have 13 national mission teams that we are building to help defend our Nations' critical infrastructure. And we have 27 combat mission teams that are aligned with the combatant commanders and assist them in their planning. To support those, we have 25 support teams which they can call upon, for a total of 133. We're building to 6200 military personnel, civilians, and some specialized contractors, and another 2,000 in the Reserves, so about 8400.

We expect to reach that in 2018, provided there is not another government shutdown. The last time, we had a government shutdown and sequestration, it put us behind by 6 months in building this. So, as of right now, we are—I think we're on track.

And I'd turn it over to Admiral Rogers to explain the—how well we're doing in attracting talent.

Admiral ROGERS. And, if I could, first let me accent, if you will, one particular portion of DEPSECDEF [Deputy Secretary of Defense] Work's comments, in terms of impact of a government shutdown or sequestration for us. The last time we went through this

and we shut it down, we assessed that we probably lost 6 months' worth of progress, because we had to shut down the school system, we went to all stop, in terms of generation of capability in the—like a domino, the layover effect of all of that, we think, cost us about 6 months of time. If we go to a BCA or sequestration level, that puts us even further behind in an environment in which we have all uniformly come to the conclusion we're not where we need to be and we've got to be more aggressive in getting there. And you can't do that if—when you're shutting down your efforts, when you're cutting money.

To go specifically, Senator, to the question you asked, I would tell you the generation of the teams, in terms of the manpower and their capability—knock on wood—is exceeding my expectations. The bigger challenge, to me, has been less—not that it's not an insignificant challenge, but the bigger challenge has been less the teams and more some of the enabling capabilities that really power them, the tools, if you will, the platform that we operate from, the training environment that we take for granted in every other mission set. The idea that we would take a brigade combat team—before it went to Iraq, before it went to Afghanistan, we'd put it out in the National Training Center, and we'd put it through the spectrum of scenarios we think they're likely to encounter in their deployment. We don't have that capability right now in cyber. We have got to create that capability. It's those enablers, to me, and the intelligence piece, let—just like any other mission set, everything we do is predicated on knowledge and insights. No different for the CENTCOM Commander than it is for me. Those are the areas, to me, where the challenges are greater, if you will, than just the manpower. I'm not trying to minimize the——

Senator COTTON. Yeah.

Admiral ROGERS.—manpower——

Senator COTTON. And how important is it that we take advantage of the existing infrastructure and capabilities that we have as you're building out the entire mission force?

Admiral ROGERS. I mean, that's what we're doing right now. But, I will say, one of our experiences—Cyber Command has now been in place for approximately 5 years—one of our insights that we've gained with practical experience and as we're looking at both defensive response as well as potential offensive options, we need to create infrastructure that is slightly separate from the infrastructure we use at NSA. It's—so, a unified platform, you've heard us talk about. It's supported in the funding. That's an important part of this. Experience has taught us this in a way that 5–6 years ago, we didn't fully understand.

Senator COTTON. Well, I'd like—my time is up for questioning, but I'd just like to bring to your attention that Arkansas Attorney General Mark Barry has requested a cyber protection team at Little Rock Air Force Base. There is an 11,000-square-foot facility there. It has a SCIF of 8500 square feet. It's already had $3.5 million invested in it. One of these facilities, I understand, would cost about $4 million. It's a request that I support. I think it's harnessed resources that we've already invested, and it also—it's a capability that they are ready to support, in addition to the profes-

sional educational center that does a lot of cybertraining for the National Guard, which is less than 30 minutes away.

Thank you.

Director CLAPPER. Mr. Chairman, I have to comment. I'm rather struck by the irony, here, of—before I left my office to come for this hearing, I was reviewing the directions that we're putting out to our people for shutting down and furloughing people. What better time for a cyberattack by an adversary when much of our expertise might be furloughed.

Chairman MCCAIN. I think that's a very important comment, Director, and thank you for saying it. There are some of us who feel it's urgent that we inform the American people of the threats to our national security of another government shutdown. I believe that it was an Arkansas philosopher that said there is no education in the second kick of a mule. So, I thank you for your comment.

Senator McCaskill.

Senator MCCASKILL. It was probably a Missouri mule.

Director Clapper, earlier this year I introduced a bill that would give intelligence community contractors whistleblower protections as long as those complaints were made within the chain or to the Inspector General or the GAO. So, disclosures made to the press would not be protected. I—as you probably know, Defense Department—I know that Secretary Work knows this—that we've already put into the law, in recent years, whistleblower protections for the contractors at the Department of Defense. And, to my knowledge—and certainly correct me if I'm wrong, any of you—I'm not aware of any classified or sensitive information that has made its way to a damaging place as a result of these protections.

The 2014 intel authorization gave these protections to the government employees within intelligence. And one of the challenges we have in government is this divide between the contractors and government employees. And, frankly, whistleblower protections—I can't think of a good policy reason that we would give whistleblower protections to employees and not give them to contractors. And so, I am hopeful today that you would indicate that you believe this is an important principle and that we should move forward with this legislation.

Director CLAPPER. Absolutely, Senator. And we have published, internal to the intelligence community, an intelligence community directive that includes whistleblowing protections for contractors. After all, that was the source of our big problem, here, with Mr. Snowden, who was a contractor. And so, our challenge—you know, the additional burden we have, of course, is trying to prevent the exposure of classified information outside channels. So, that's why whistleblowers absolutely must be protected, so that they are induced or motivated to go within the channels, knowing that they will be protected. This is a program that is managed by the intelligence community Inspector General, who is, of course, independent as a Senate-confirmed official.

Senator MCCASKILL. Thank you. And I'm pleased to see that you would be supportive of that.

And, Secretary Work and Admiral Rogers, I assume that you would be supportive of giving whistleblower protections to intelligence community contractors?

Mr. WORK. Absolutely. I agree totally with what Director Clapper said.

Admiral ROGERS. Yes, ma'am, and I say this as the head of an intelligence agency.

Senator MCCASKILL. Thank you.

I want to follow up a little bit, Director Clapper, with your comment about a shutdown. Could you tell us what impact another government shutdown would have on your progress of getting the cyber mission force fully operational? Excuse me—Admiral Rogers. I think that, in political isolation, shutdown appeals to a certain swath of Americans, and I understand why. Because sometimes it just feels good to say, "Well, let's just shut it down," because, obviously, government is never going to win popularity contests, certainly not in my State. On the other hand, there's a difference between responsible, in terms of public policy, and being irresponsible, in terms of recognizing—I love it when some of my friends wave the Constitution in my face and then fail to read the part that we have a divided checks and balances in this country, unlike other countries. The American people sent a party—a President of one party to the White House and elected a Congress of a different party. And that means we have to figure out how to get along. So, could you talk a moment about what the impact would be to this important mission if once again we went down the rabbit hole of deciding the best thing to do is just to shut down government?

Admiral ROGERS. So, if we use our experience the last time, first thing I had to do was shut down the school system. And training and education is a core component of our ability to create this workforce. Just shut it all down, because it was only mission essential.

The second thing I was struck for, all travel that was associated with training, all—we had to shut all that down, so I couldn't send people to generate more insights, to gain more knowledge.

We had to shut down some of our technical development efforts because of the closure—again, put that all on hold. At a time where we have talked about the need to develop more capability, the need to develop more tools, I had to shut that all down during the period of the last shutdown. We were forced to focus our efforts on the continued day-to-day defense, which is critical—don't get me wrong. As Secretary Work has indicated, it is priority number one for us.

The other concern I have is—and I have watched this play out now just in the last 10 days—I've been in command 18 months, and I will tell you, the biggest thing I get from my workforce, prior to the last 10 days, "Sir, this happened to us once in 2013. Is this going to happen again? If it is, why should I stay here, working for the government? I can make a whole lot more money in the cyber arena on the outside." So, in addition to the threat piece that the DNI has highlighted, my other concern is—if we do this again, is the amount of our workforce that says, "You know, twice in the course of 2 years? I've got a family, I've got mortgages, I've got to take care of myself. As much as I love the mission, as much as I believe in defending the Nation, I can't put myself or my family through this. I've got to go work in the commercial sector." That would be terrible for us. Because people—despite all our tech-

nology, never forget, it is men and women who power this enterprise. That's our advantage.

Senator MCCASKILL. At the risk of sounding like a smart aleck, which I do from time to time, I would say maybe we need to open some of those schools so some of my colleagues could do some math and realize the votes are not there to overcome a presidential veto. And this is a recipe for dysfunction that does not help anyone in this country, and particularly our national security.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Tillis.

Senator TILLIS. Thank you, Mr. Chairman.

I want to just echo the comments of my colleague Senator McCaskill. I think it's irresponsible. We've had this—the Secretary come before this committee and say that the number and severity of threats have not been greater since 9/11. That should be enough said, in terms of what we need to do to keep continuity in funding the government. All the other things that I may have a problem with have to be second to that priority. I thank you all for your work. And, Director Clapper, I thank you for your comment.

Admiral Rogers, we've had briefings from you since you've taken the command. And one of the briefings I'm reminded of is the trend that you see, in terms of the gap between what tends to be still an American advantage, overall, narrowing, particularly with nations like China and Russia, and I think you may have even mentioned Iran being an emerging threat. Can you tell me, really in the context of maybe another 6 months reset on your training, but, more importantly, based on your current funding streams and your current plan, Are we going to be able to widen that gap again, or is this just a matter of staying slightly ahead of our adversaries?

Admiral ROGERS. For right now, I think the most likely scenario is, we're staying slightly ahead of our adversaries, because we're trying to do so much foundational work, if you will, as I said previously, trying to overcome a very different approach over the previous decades. It's not a criticism of that approach. It was a totally different world. It led to a different prioritization. It led to a different level of effort and a different investment strategy. Clearly, we're going to have to change that. And we're changing that at a time when budgets are going down and threats—not just in cyber, but more broadly—are proliferating. I don't envy the choices that Secretary Carter and the leadership has to make. There's nothing easy here.

So, I think, in the near term, the most likely scenario for us is, How can we focus on the best investments that maximize your defensive capability while continuing to help us retain the advantage we do right now against most?

Senator TILLIS. Thank you.

And this question may be for Secretary Work. The announcement about the agreement with China, that we're not going to, basically, attack each other, in the face of the compelling evidence that we have that China's done it in the past and they've denied it, why is this agreement a positive thing if, with the smoking-gun information we have right now on prior attacks, theft of intellectual property, commercial data, that we have a pretty strong base of

evidence to say that they're guilty of it, if they deny it, why does this agreement mean anything?

Mr. WORK. On the buildup to this visit, we made it very clear, through a wide variety of efforts, that this was going to be something that was foremost in the discussions when President Xi came. We have made it as clear as we possibly can in every single level, from the President on down, that the Chinese cyberactivities are unacceptable. And we believe that this is a good first step as a confidence-building measure, where China can either demonstrate that they are serious about establishing some norms, and going after crimes, et cetera. But, the proof will be in the pudding. I agree with Director Clapper and Admiral Rogers, it's going to be up to the Chinese to demonstrate that they're serious about this.

Senator TILLIS. Would the manipulation of commercial data fall within the definition of theft under this agreement?

Mr. WORK. Well, specifically, one part of it is the theft of IP—intellectual property—for commercial advantage in, say, for example, a Chinese state enterprise. And we have agreed, at least at—we have made a tentative agreement that we will not do those type of activities. China has done those activities in the past. It will be up to them to prove that they won't do it in the future.

Senator TILLIS. And then, the—for anyone, and then I'll yield. I know the committee's gone on a while. But, at what point—I think Senator Heinrich made some very important points about drawing red lines. But, at what point are we going to have clear definitions about malign activities in cyberspace being acts of war or acts of terrorism, and then have appropriate responses, whether they be through cyber, through sanctions, or other? When are we going to get that clarity? Because we don't have it today.

Mr. WORK. Senator, I don't believe that we will ever have a definitive one-size-fits-all definition for these type things. Every single attack will be—have to—handled on a case-by-case basis, and you will have to judge the damage that was caused, who made the attack, was it just a nonstate actor or just a malicious hacker—we'd have to go after that person, in terms of criminal activity. So, I don't believe we're ever going to have a specific definition that says, "If this happens, we will trigger this response." Each one will be handled in a case-by-case basis and be proportional.

Senator TILLIS. Well, thank you. Mr. Chair, the——

I think the lack of clarity, though, the only concern that I have is, you're not establishing some level of known deterrent. And that's why—I understand the complexities of it. I've worked in the field. But, I think that, without that clarity, you're more likely to have more things that you're going to have to look at and figure out how to do a situational response.

Thank you, Mr. Chair.

Chairman MCCAIN. Senator Sullivan.

Senator SULLIVAN. Thank you, Mr. Chairman.

And thank you, gentlemen, for your testimony today on a really important topic.

You know, I believe and I'm—I was looking for the transcript, but—at the joint press conference between President Xi and President Obama that—President of China, I think, publicly stated that they don't engage in these kind of cyberactivities. Was that an ac-

curate statement, if that was, indeed, what he said, in terms of cyberwarfare? It's pretty remarkable, if you're in a press conference with another head of state, and you just say something that seems to be pretty blatantly false.

Director CLAPPER. Well, it is. And I think, apart from the statements, at least for our part, it will be: What happens now, what is—will there be a change in their behavior? And as I said earlier, well, hope springs eternal, but—I personally am somewhat of a skeptic, but it will be our responsibility to look for the presence or absence of the—of their purloining of intellectual property and other information.

Senator SULLIVAN. And were any of you gentlemen, or all of you gentlemen, consulted on the terms of the agreement?

Director CLAPPER. We were aware of the negotiations, but, at least from—normally, intelligence wouldn't be a voice or shaper of a policy agreement like this between two heads of state. It will—I think our responsibility is to report what they do.

Mr. WORK. We participated in the buildup of the visit, in terms of policy development, et cetera. But, in terms of what went on between the two leaders of the nations, we were not directly consulted.

Senator SULLIVAN. Admiral?

Admiral ROGERS. And I was aware of the ongoing process, and, like Secretary Work, same thing, part of the broad effort in preparation for the visit.

Senator SULLIVAN. But, you weren't—you didn't see the terms of this agreement before the——

Admiral ROGERS. No.

Senator SULLIVAN. Did you, Mr. Secretary?

Mr. WORK. No.

Senator SULLIVAN. Let's assume that, you know, kind of pass this prologue, here, and, you know, we were talking about intellectual property. As you know, our country has been trying to get the Chinese from—to stop stealing United States intellectual property for decades, really. And it hasn't really worked out very well. If—let's assume that this agreement—that there is some additional cybertheft that we can attribute to China. What would you recommend the actions of the United States should be, particularly in light of this agreement?

Mr. WORK. I wouldn't be able to answer that, as I would have to know what the degree of the activity would be.

Senator SULLIVAN. Let's say another OPM kind of activity.

Mr. WORK. I think we—the Department of Defense would recommend a very vigorous response.

Senator SULLIVAN. And, Mr. Secretary, what would you—I mean, just give me a sense of what that would be. Sanctions, retaliation——

Mr. WORK. Could be any of those, Senator. Maybe all of the above. It will depend upon the severity of the activity. But, again, I know this is—I know this is a big point of contention with the committee. It is—we are serious about cost imposition, and our statement is, "If you participate in that—this activity, we will seek some type of measure which imposes costs upon you." And we just do not think it's a proportional cyberattack for a cyberattack. It

might be something entirely different, like a criminal indictment or sanctions or some other thing.

Senator SULLIVAN. Let me ask kind of a related question for all three of you. How—and I know you've been discussing this, and I'm sorry if I'm kind of going over areas that we've already discussed, but—help us think through the issue of rules of engagement here. I mean, we have rules of engagement in so many other spheres of the military that are well established. How do we think through these issues, which I think in some ways are the fundamental aspects of what we do in response to cyberattacks?

Admiral, do you want to take a stab at that?

Admiral ROGERS. So, if you look at the defensive side, I'm pretty comfortable that we've got a good, broad recognition of what is permissible within a rules-of- engagement framework.

Senator SULLIVAN. Do we? I mean, between us and other nations?

Admiral ROGERS. I'm—I wouldn't—if you define it between us and other nations, I would—no, I apologize. I thought your question was in a DOD kind of responsive framework.

If you want to expand it to a broader set of nations, then it's probably fair to say no.

Director CLAPPER. I would agree. I think, when it comes to offensive—if you're thinking about offensive cyberwarfare, we probably don't—do not have rules—defined rules of engagement.

Mr. WORK. I agree with what Director Clapper said earlier, Senator, that this really is the Wild West right now. There's a lot of activity going on, both from nation- state actors all the way down to criminals. And so, sorting through each of the different attacks and trying to attribute what happened and who it came from and who was responsible for it all demand specific responses on these attacks.

But, I agree totally with the committee that we need to strengthen our deterrence posture, and the best way to do that is continue to work through these things and make sure that everyone knows that there will be some type of cost.

Senator SULLIVAN. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. The committee would also like to know when there's going to be a policy that would fit into these attacks and would then be much more easily responded to if we had a policy, as mandated by the 2014 defense authorization bill.

I thank the witnesses for a very helpful hearing. I know that they're very busy, and we—the committee appreciates your appearance here today.

Thank you.

[Whereupon, at 11:38 a.m., the hearing was adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR JAMES INHOFE

1. Senator INHOFE. Has the DOD established a pipeline for the development of a future cyber force?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. Each of the Military Departments has established recruiting and retention goals to establish the pipeline for all cyber officer, enlisted, and civilian specialties. This pipeline supports both fielding the Cyber Mission Force and the Military Departments core missions. The Military Departments are projecting an overall increase in their officer and enlisted cyber specialists over the next few years. In order to meet a new cyber force sustainment rate, the increase will be required in order to meet anticipated separations and retirements from the Services.

On April 17, 2015, the Secretary of Defense signed "The Department of Defense Cyber Strategy." The first strategic goal in the strategy is "Build and Maintain Ready Forces and Capabilities to Conduct Cyberspace Operations." An entire line of effort is dedicated to fostering a viable career path for military personnel and improving recruitment and retention processes for the most highly skilled military cyber personnel. This effort will focus on validating current career paths, determining future military cyber billet structure and, within military manpower plans, evaluation of areas where specialized skills and assignments fit within the overall career progression structure.

Similar to the military workforce, the "Cyber Strategy" requires the Department to improve civilian recruitment and retention for cyber-related personnel by the end of 2016. This effort is on track to deliver the needed governance structure, policies and implementation plan to meet the 2016 target.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

2. Senator INHOFE. Are universities and technology institutions graduating both the numbers needed to fill force requirements and personnel with the right skill sets to ensure we maintain a dominant offensive and defensive capable cyber force?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. I have noted that academic universities and technology institutions are focusing on digital communications, forensics, and cybersecurity. Many university programs are nascent and remain focused on computer science. There is also an important element of cyber operations which involves sociology and ethnography. These degrees have direct relationship to the Military Department Cyber workforce and contribute to building a professional and well-trained team. I have noted many institutions are reluctant to include curricula on offensive capabilities. In order to understand the cyber domain, graduates from universities and institutions must be exposed to offensive, defensive, and sociocultural capabilities during their course of instruction.

Additionally, the Department supports the National Initiative for Cyberspace Education (NICE). In the Department of Defense Cyber Strategy, the Department is tasked to develop policies to support NICE, and working with interagency partners and educational institutions, the Department will provide input to NICE, thereby announcing the Department's requirements to universities and technology institutions.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

3. Senator INHOFE. How are we addressing the recruiting and sustainment of personnel to eliminate critical cyber expert shortages?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. The DOD Cyber Strategy, published in April 2015, challenged the Department to improve recruiting and sustainment under the heading of Cyber Workforce Development. The subsequent implementation plan included well-defined objectives and timelines. The Department's first priority is to develop a ready Cyber Mission Force and associated cyber workforce to make good on the significant investment in cyber personnel, and to help achieve many of the objectives in the DOD Cyber Strategy. This workforce will be built on three foundational pillars: enhanced training; improved military and civilian recruitment and retention; and stronger private sector support.

The Department requires an individual and collective training capability to achieve the goals outlined in the DOD Cyber Strategy and to meet future oper-

ational requirements. This training capability, identified as the Persistent Training Environment, is a cornerstone objective highlighted in the strategy and will contribute to both recruiting and sustainment of cyber experts. US Cyber Command will work with other components, agencies, and military departments to define the requirements and create a training environment that will enable the total cyber force to conduct joint training (including exercises and mission rehearsals), experimentation, certification, as well as the assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks.

The second objective addresses military personnel recruitment and retention. In terms of recruiting, DOD has an operational mission in cyber that is unavailable in the private sector, a unique mission focus should be used to motivate people to serve in the DOD. Solving the Department's shortages for cyber experts is a supply and demand problem; as such, we must right size our training pipelines to accommodate those we retain as well as those that will leave for the private sector.

We have completed recruitment research determining personality and technical attributes needed for successful cyber operators. Based on that research, the Department is exploring instruments to identify those individuals. These instruments are being evaluated in a second pilot of the Cyber Operators Course which demonstrates a new learning practice approach for cyber.

To aid retention, DOD must demonstrate commitment via additional training and development for our cyber workforce. Throughout the course of this strategy, and following the Cyber Mission Force decisions of 2013, the Department will continue to foster viable career paths for all military personnel performing and supporting cyber operations.

Another objective of Cyber Workforce Development is to improve civilian recruitment and retention. In addition to developing highly-skilled military personnel, the Department must recruit and retain highly-skilled civilian personnel, including technical personnel for its total cyber workforce. Civilians must follow a well-developed career path. The cyber career path will include an advancement track and best-in-class opportunities to develop and succeed within the workforce. A related effort is support of exchanges between DOD and industry.

In January 2016, Congress provided the Department the ability to adopt Title V Exempted Service hiring authorities for US Cyber Command and the Service Cyber Headquarters civilian employees. Exempted Service hiring authorities will help motivate key civilians to serve in the Department of Defense, and will assist in retaining them for career service.

The DOD should also leverage public and private partnership to identify promising candidates within the academic pipeline. To supplement the civilian cyber workforce, for example, the Department must employ technical subject matter experts from the best cybersecurity and information technology companies in the country to perform unique engineering and analytic roles.

Many of the best practices, both in recruiting and retention, have already been identified by the National Security Agency (NSA)—who we are actively working with, to scale those initiatives to support DOD. We are also looking at more diverse training pathways, including leveraging universities and their Reserve Officer Training Corps programs. The Department is working with all appropriate organizations in pursuit of innovative and effective solutions to recruitment and sustainment needs of the cyber workforce.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

WEAPONS SECURITY

4. Senator INHOFE. How concerned are each of you with cyber vulnerabilities in our existing weapons systems?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. I am very concerned about cyber vulnerabilities in Department of Defense weapons systems. My concern stems from the lack of efficient opportunities to modernize and update the underlying electronic infrastructure and operating systems of those weapon systems. New vulnerabilities are routinely discovered, but the existing list of known vulnerabilities is both lengthy and costly to mitigate.

Admiral ROGERS. Mr. Work will address cyber resilience in weapons systems development and expanding mission assurance activities at the Department level.

5. Senator INHOFE. Are we incorporating cyber security into the development of all our new weapons systems during the acquisition process?

Secretary WORK. Yes. The Department is incorporating cybersecurity into the development of all new weapons systems during the acquisition process. DOD Instruction (DODI) 5000.02, "Operation of the Defense Acquisition System," dated January 7, 2015, contains requirements for acquisition programs to address cybersecurity countermeasures. Program Managers, as an element of the Systems Engineering process, have the responsibility in their Program Protection Plan (PPP) to describe the program's critical program information and mission-critical functions and components; the threats to and vulnerabilities of these items; and the plan to apply countermeasures to mitigate associated risks. Countermeasures include cybersecurity, secure system design, supply chain risk management, software assurance, anti-counterfeit practices, and other mitigations. Program Managers will submit the program's Cybersecurity Strategy as part of every PPP. In addition, during the Test and Evaluation phase, Program Managers are responsible for developing a strategy and budget resources for cybersecurity testing to support design, development, and deployment decisions.

In addition, the Department is developing a cybersecurity in acquisition enclosure to DODI 5000.02 in order to more strategically align cybersecurity activities across the acquisition and operational communities. This update is intended to synchronize efforts that are underway to strengthen our cybersecurity posture and enable systems to maintain critical mission capabilities in a cyber-contested operational environment. The enclosure, along with the existing PPP for acquisition programs, further defines DODI 8500.01, "Cybersecurity," and DODI 8510.01, "Risk Management Framework for DOD Information Technology," for defense weapon systems and acquisition programs.

DOD ROLES & RESPONSIBILITIES

6. Senator INHOFE. How does the U.S. deter cyber-attacks?

Secretary WORK. The Department of Defense (DOD) seeks to deter adversaries from conducting malicious cyber activities of significant consequence; this effort focuses on denying the adversary the ability to achieve the objectives of a cyber-attack, being able to impose costs on the adversary, and ensuring that our computer systems and networks are resilient.

Key elements of a deterrence approach include declaratory policy, indications and warning, defensive posture, response procedures, and network resilience. DOD has a number of specific roles to play in this approach, which are nested within DOD's core cyberspace missions and the new DOD Cyber Strategy.

Deterrence is a function of perception and convincing a potential adversary that the costs of conducting an attack outweigh any potential benefits. The Department must also demonstrate the futility of such attacks through network defense and resilience and by showing that DOD will be able to continue its mission even while under attack. DOD must maintain capabilities to affect an adversary's behavior by shaping the environment, controlling escalation, and, when necessary, imposing costs.

7. Senator INHOFE. Do you consider all cyber-attacks against the U.S. a national security threat? If no, how do you determine what constitutes a national security threat?

Secretary WORK. Not all malicious cyber activities directed towards the United States constitute a national security threat, but some may rise to that level. The determination of what constitutes a national security threat, in or out of cyberspace, would be made on a case-by-case and fact-specific basis by the President. There would likely be an accompanying assessment of the seriousness of a particular act. Cyber activities that cause death, injury, or significant destruction would be carefully assessed to determine if they should be considered unlawful attacks or "acts of war." The context for these events would also be important to consider, and cyber activities should not be viewed in isolation.

8. Senator INHOFE. What triggers DOD involvement in a cyber-attack against the U.S.?

Secretary WORK. The Department of Defense (DOD) is involved on a daily basis in countering cyber-attacks against the United States through the defense of its own networks, which are constantly under attack.

In addition to defending its own networks, one of DOD's three missions in cyberspace is to be prepared to defend the United States and its interests against cyber-attacks of significant consequence. If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. homeland or U.S. interests in cyberspace. The pur-

pose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life.

In the event of an attack on domestic interests that are not of national security consequence, DOD may respond in a supporting capacity to requests for assistance from the Department of Homeland Security, the Federal Bureau of Investigation, as well as other departments and agencies.

9. Senator INHOFE. Do you have the rules of engagement you need or do they need to be modified?

Secretary WORK. Rules of engagement are one of the many factors we consider when planning cyber operations. The current rules of engagement do not unduly restrict our ability to carry out current operations. The Department continually reassesses the rules of engagement required to complete its assigned missions.

QUESTIONS SUBMITTED BY SENATOR KELLY AYOTTE

DETENTION FACILITY AT GTMO

10. Senator AYOTTE. Secretary Work, why does it make sense to this administration to provide weapons to moderate Syrian fighters but not to Ukraine—a legitimately elected democracy simply seeking to maintain their territorial integrity, protect their sovereignty, and choose their own future?

Secretary WORK. Our different approaches towards resolving the conflicts in Syria and Ukraine reflect our assessment of the most effective ways for countering threats emanating from each country. In Syria, countering the Islamic State of Iraq and the Levant (ISIL) threat requires sustained kinetic strikes against the group and enabling local forces that defend against and eventually go on the offense against the group. For this reason, the Department is committed to its objective of providing support—including weapons and ammunition—to moderate Syrians fighting ISIL and will focus on finding ways to enable already successful counter-ISIL operations by groups on the ground.

As the President has said, the provision of defensive lethal assistance to Ukraine remains an option; however, assistance to date has been calibrated towards supporting a diplomatic solution to the crisis. Since the first of September, a ceasefire has held and the parties are now moving toward elections and greater implementation of the Minsk Agreements. While not providing lethal assistance, we have committed substantial resources to help Ukraine, with more than $266 million in equipment and training committed since the beginning of the crisis.

VULNERABILITY OF DOD'S WEAPONS TO CYBER ATTACK

11. Senator AYOTTE. As you noted in your prepared statement, Secretary Work, "Without secure systems, we cannot do any of our missions." Admiral Rogers and Secretary Work, can we be confident that America's military systems (IT systems, as well as strategic and conventional weapons) will function properly if we are forced to engage in a full spectrum conflict against a near pear competitor employing sophisticated cyber attacks?

Secretary WORK. I cannot say that I am one hundred percent confident that our military systems will be able to withstand a sophisticated cyber-attack. That said, we are doing what we can, through three mission areas, to mitigate this risk and to raise our level of confidence.

The first mission area is focused on defending our own networks and weapons because they are critical to what we do every day. We consider this form of mission assurance to be our top priority, and we have put in place mechanisms to reduce risk, enhance resilience, and increase accountability for mitigation of vulnerabilities. Second, we help defend the nation against cyber threats—especially if they would cause loss of life, property destruction, or significant foreign policy and economic consequences. Our third mission is to provide integrated cyber capabilities to support military operations and contingency plans, if directed by the President or the Secretary of Defense.

Admiral ROGERS. [Deleted.]

12. Senator AYOTTE. DOD's Defense Science Board produced a January 2013 Task Force Report entitled "Resilient Military Systems and the Advanced Cyber Threat". Secretary Work, what steps to improve this situation has DOD undertaken since this January 2013 report?

Secretary WORK. Since the study, there have been significant leadership initiatives to address cyber, as evidenced by Department policy, investment, and boards.

With the participation of the United States Strategic Command and the Department of Defense (DOD) Chief Information Officer, the Department has conducted a series of cyber risk assessments, and we are now proceeding to identify and prioritize elements of conventional force structure, platforms, and weapon systems for cyber resilience. In accordance with the DOD Cyber Strategy, the Department has refocused intelligence to be able to understand, predict, and attribute cyber capabilities, plans, and intentions of adversaries. The Department has also established and are manning, training, and equipping the Cyber Mission Forces (CMF). The Department is also building both offensive capabilities and capabilities to respond to cyber-attacks.

To combat mid-tier threats, the Department maintains defense of information environments as a top priority, and evaluating key cyber terrain using CMF Cyber protection teams. To change the DOD culture regarding cyber and cyberspace security, the Department has initiated accountability scorecards and expanded workforce training. The Department is equipping program managers, updating policy, and expanding the capability and use of red teams to evaluate and adjust designs, acquisition, and operations. In addition, the Department is continuing to leverage the Defense Science Board's wise counsel through a number of studies currently underway on the subjects of cyber defense, supply chain, and deterrence.

13. Senator AYOTTE. Secretary Work, how are we incorporating lessons learned regarding cyber resilience into programs for new DOD IT systems and weapons systems?

Secretary WORK. The Department of Defense (DOD) is implementing risk-based approaches to manage evolving cybersecurity threats, achieve mission objectives, and develop resilient weapon systems and information systems by better integrating cybersecurity activities during system development. DOD cybersecurity policy [1] requires that robust cybersecurity processes be applicable to all systems containing information technology, including weapons systems. DOD is developing guidance for a new cyber survivability element of the System Survivability key performance parameter.

To achieve stringent DOD mission assurance goals, we are enhancing system security engineering, expanding early testing to include cyber resiliency, updating requirements for survivability, and updating how program protection planning is executed in the defense acquisition system. In addition, DOD continues to mitigate cyber vulnerabilities in systems and conducts operational tests assuming a cyber-contested environment.

14. Senator AYOTTE. Secretary Work, is there a systematic process that requires program managers to incorporate cyber resilience into DOD programs from the beginning rather than as an afterthought?

Secretary WORK. Resiliency is an essential element of an overall Department cyber defensive strategy. While traditional strategies have focused on keeping cyber adversaries "out," more effective new strategies, combined with a resiliency focus, ensure that critical capabilities continue despite successful attacks. Program managers address cyber resilience requirements in their system technical requirements, which are included in technology and product development solicitations and inform system definition and design. The cybersecurity risk management guidebook for program managers and the new cybersecurity enclosure to the Department's acquisition system policy reinforce incorporation of cyber resilience and cybersecurity requirements starting from the beginning of the system life cycle. Program protection plans, supply chain risk management analysis, test planning, and life cycle management processes are being adjusted and improved to enhance our systems' ability to operate in a cyber-contested environment and maintain robustness.

These efforts to place requirements, develop cyber resilient systems, expand the Department's testing regime, and equip program managers to work effectively with industry will enhance the Department's ability to deliver cyber resilient systems through acquisition by considering integrated cyber risk management and early development of plans to proactively ensure that cyber resilience is maintained throughout the life cycle.

RUSSIAN INF VIOLATIONS AND DOD RESPONSE

15. Senator AYOTTE. Secretary Work, you agreed in the hearing that Russia has violated the INF. Why is DOD waiting for Russia to field the system in question

[1] Including DODI 8500.01, "Cybersecurity," dated March 14, 2014, and DODI 8510.01, "Risk Management Framework for DOD Information Technology," dated March 12, 2014.

to respond if Russia has already violated the INF by flight testing the respective system? Is violation of the treaty not enough to respond?

Secretary WORK. The Administration is not waiting on Russia to field this system and is examining options to respond to the Russian violation. The Intermediate-range Nuclear Forces (INF) Treaty has served the strategic interests of the United States, North Atlantic Treaty Organization Allies, and Russia since it entered into force. The Administration is seeking to convince Russia that it is in its interest to return to compliance. However, American patience is not without limits; accordingly, the Department is considering an array of responses to the Russian violation that will ensure Russia gains no significant military advantage from its violation.

BETTER USE OF GUARD AND RESERVE TO IMPROVE OUR CYBER READINESS

16. Senator AYOTTE. Secretary Work, in your prepared statement you note that "Successfully executing our missions in cyberspace requires a whole-of-government and whole-of-nation approach." Admiral Rogers and Secretary Work, in light of this growing cyber threat and the need to respond with a "whole-of-government and whole-of-nation approach", how can we better utilize our nation's Reserve and National Guard forces to 1) defend DOD systems; 2) defend the nation against major cyber-attacks; and 3) provide cyber support to operational commanders?

Secretary WORK. The Army will implement one full-time Army National Guard Cyber Protection Team (CPT), and ten part-time Army National Guard CPTs. The Air Force will leverage 12 Air National Guard Cyber Operations Squadrons to develop two full-time CPTs, three Air National Guard squadrons to develop the cyber operations component of one National Mission Team, and will create one Air Force Reserve unit in a classic associate unit construct to comprise three cyber mission force required CPTs. The Navy and Marine Corps will continue to augment vacancies in their Cyber Mission Force (CMF) teams by leveraging their Reserve Forces as individual mobilization augmentees.

Continuing to rotate National Guard forces through the CMF and improving synchronization of federal interagency and the state response (including State use of National Guard cyber capabilities) provides the Department a method to better utilize National Guard capabilities. Integration of the National Guard into the CMF provides surge capability to the Department. This capability also makes experienced units available to the Governors for State use when not in federal service. Continuing to improve synchronization of Federal and State responses will allow for more effective use of the National Guard as a state response resource and foster better information sharing across whole-of-government and whole-of-nation in defense of the nation.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

NSA-LIKE AUTHORITIES FOR DHS

17. Senator AYOTTE. Director Clapper and Admiral Rogers, the Federal Information Security Management Reform Act of 2015 (FISMA Reform) was introduced in July and it would benefit immensely our federal civilian network security from streamlined and clear authorities for DHS, which has the lead for safeguarding the cyber domain for federal civilian agencies (.gov), yet has limited authority to do so. How important is it to be able to move quickly, decisively, and with legal authority when an intrusion is detected?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

18. Senator AYOTTE. Admiral Rogers, how important is it to have a clear delineation of responsibilities to act?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

19. Senator AYOTTE. Director Clapper and Admiral Rogers, based on your experience, what are the most important aspects of robust detection and mitigation of cyber intrusions?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Admiral ROGERS. Ideally, cyber intrusions are detected and mitigated at machine speed using automation. End point protection capabilities, such as Host Based Security System (HBSS), along with additional layers of defense at various tiers

throughout the Department of Defense Information Network (DODIN) provide a wide breadth of protection. These multiple layers of protection (i.e. HBSS, Web Content Filtering (WCF), Demilitarized Zone (DMZ), etc.) provide sensing and blocking of threats at all tiers within the DODIN architecture along with the associated command and control (C2) to drive response actions should automated mitigation fail. In addition to these efforts, the commercial sector, mission partners, DOD Components, and the Intelligence Community (IC) all play a crucial role regarding information sharing and strengthening the security posture of the DODIN. The other most important aspect of robust detection and mitigation of cyber intrusions is trained personnel at the network operations centers, at the Computer Network Defense Service Providers, and throughout the Cyber Mission Force. If the end point protection system does not catch the initial download of malicious software, it takes the operators' keen observation of network activity or the analysts' scrutiny of security logs to detect adversary activity and take action to eradicate adversary presence on the network. In addition, current and effective policy and processes improve our ability to block potential threats to the DODIN.

GENOCIDE IN IRAQ AND SYRIA?

20. Senator AYOTTE. Director Clapper, according to the United States Commission on International Religious Freedom's annual report for 2015, Yazidis and Christians in Iraq and Syria have endured a "systematic campaign" of persecution which has included summary executions, forced conversions, rape, sexual enslavement, child abduction, and destruction of houses of worship. Do you assess that ISIS has undertaken a "systematic campaign" of persecution against religious and ethnic minorities?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

21. Senator AYOTTE. Director Clapper, article II of the 1948 United Nations Convention on the Prevention and Punishment of the Crime of Genocide defines genocide as any act committed with the intent to destroy all or part of a national, ethnic, racial, or religious group. Based on your knowledge of the situation in Iraq and Syria, do you assess that ISIS's actions in Iraq and Syria against religious and ethnic minorities amounts to genocide?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

U.S. MILITARY SUPERIORITY AND CHINESE CYBER THEFT

22. Senator AYOTTE. All witnesses, how would you characterize the scale and severity of the cyber theft that China is committing against U.S. defense companies?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. That is a difficult question to answer. The full extent or pervasiveness of China's infiltration and persistence within the Defense Industrial Base, or other commercial entities is unknown.

There are several objectives listed within the Department of Defense (DOD) Cyber Strategy (objectives 2(m), 2(o), 2(p), and 2(q)) that specifically focus on the problem related to the theft of intellectual property. Accordingly, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics is well on its way toward establishing a Joint Acquisition Protection and Exploitation Cell to link intelligence, counterintelligence, law enforcement, and acquisition communities to enable Controlled Technology Information protection efforts across the DOD enterprise. Such a cell would allow DOD, by the end of 2016, to mitigate future losses proactively and to exploit opportunities to deter, deny, and disrupt adversaries that may threaten the U.S. military advantage.

Finally, DOD is not addressing this problem alone. For example, objectives 2(o) and 2(q) of the DOD Cyber Strategy call for further voluntary and cooperative engagement between the Defense Industrial Base and DOD. Through these objectives, the Department is promoting cyber threat awareness, information sharing, and collaboration on technical innovations geared toward disrupting and denying the theft of intellectual property.

Admiral ROGERS. [Deleted.]

23. Senator AYOTTE. All witnesses, how has this theft impacted U.S. military superiority relative to China?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. China's cyber-enabled theft of intellectual property from U.S. defense companies has likely eroded, though not negated, U.S. military superiority relative to China. As Secretary Carter has emphasized, it would take years for any country to build the military capability the United States has today. Nevertheless, the Department will continue to make the investments necessary to maintain military dominance, while continuing to take all lawful measures to stop the theft of information.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

POLICY CHANGES

24. Senator AYOTTE. Admiral Rogers, what specific policy/statutory changes are needed to help CYBERCOM?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

CYBER AND THE RESERVE COMPONENT

25. Senator AYOTTE. Secretary Work and Admiral Rogers, Secretary Carter outlined a program to engage with the civilian sector in Silicon Valley. In terms of cyber, what other efforts are ongoing to capitalize on the technology center of excellence? How might you use the Reserve Component to do the same thing?

Secretary WORK. The Defense Innovation Unit Experimental (DIUx) has engaged deeply with the cyber-related companies in Silicon Valley. As an example, on October 20, 2015, DIUx hosted a Cyber Showcase for ADM Rogers, where seven newly formed companies presented their technologies to an audience that included government experts, cyber-related companies, and Silicon Valley venture capitalists. As a result of this showcase, the Department is exploring pilot projects with several of these companies. This is just one aspect of the DIUx mission to engage with the Silicon Valley innovation ecosystem.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

26. Senator AYOTTE. Secretary Work and Admiral Rogers, to protect our country against cyber theft and attack requires coordination with many civilian agencies and state governments. How is the Reserve Component being leveraged to do this?

Secretary WORK. The Reserve Component is already engaged in associate unit roles, training functions, and fully integrated into Cyber Command and Control and operational units. A key reason these units are successful is many of the Reserve members are also full time industry experts in areas such as cybersecurity, digital forensics, and many other relevant networking essentials. Their commercial experience and certifications are directly brought to bear when in their Reserve role supporting States and the interagency. Capitalizing on commercial best practices is a common thread the Reserve teams bring to the cyber workforce. Exercises such as US Cyber Command's CYBER GUARD provide an opportunity for Guard, Reserve, and Active Duty to focus on the cyber aspect and work with critical infrastructure providers. States and federal agencies, including the Department of Homeland Security, determine procedures, requirements, and authorities required for our national security.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

27. Senator AYOTTE. Secretary Work and Admiral Rogers, what has been done—and what still needs to be done—to assure National Guard cyber mission forces receive the required number of military school-house seats, training days and other resources needed to leverage their civilian-acquired cyber skills for protection of our national security interests?

Secretary WORK. National Guard and Reserve forces are part of the overall total force's training requirements. Each of the Services prioritizes its training capacity to ensure cyber mission forces are brought on-line as quickly as possible. In collaboration with US Cyber Command, the National Security Agency's Associate Director for Education and Training (ADET) has increased training capacity, providing seats for both the Active and Reserve Components. Additionally, ADET has offered guidance and assistance to the National Guard's Professional Education Center and to the US Cyber Command Reserve Force Advisor on how to meet the Reserve Component demand for general cyber training. This effort continues. Early on in the fielding of the Cyber Mission Force, the Department recognized the need for a mechanism to evaluate Services members' skills and experience and provide credit where

appropriate. US Cyber Command's Individual Training Equivalency Board was created to provide members of the Active and Reserve Components equivalency based on their civilian acquired skills. This board minimizes the overall training demand and more quickly provides the nation with a cyber capability.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

IRAN

28. Senator AYOTTE. Director Clapper, does Iran continue to develop capabilities useful for an ICBM program? When do you estimate that Iran will attain an ICBM capability?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

QUESTIONS SUBMITTED BY SENATOR MIKE ROUNDS

CHINA

29. Senator ROUNDS. Director Clapper, Secretary Work and Admiral Rogers, last week, the President announced that the United States and China have agreed not to conduct or knowingly support cyber enabled theft of intellectual property including trace secrets or other confidential business information for commercial advantage. Isn't this agreement made meaningless by the fact that China has repeatedly denied that it engages in the activities this agreement purports to stop?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. The United States has been clear with the Chinese Government that the United States is watching to ensure that the Chinese follow through on their commitment. Should China continue to engage in cyber-enabled economic theft, the United States can now hold China accountable for adhering to its own promise, rather than arguing over China's previous claims that economic theft is no different than traditional intelligence collection. It is important to note that these commitments do not take off the table any options that we might use to defend our companies from malicious cyber threats. As President Obama stated in September 2015, if China's aggressive cyber actions do not stop, the United States is prepared to take countervailing actions at the time and place of our choosing.

Admiral ROGERS. The United States and China have reached a common understanding on the way forward, which is what matters. We have agreed that neither the United States nor the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. We are watching carefully to make an assessment as to whether progress has been made in this area. The Department is focused on working with Congress, other U.S. departments and agencies, and the private sector to strengthen our ability to detect, attribute, and respond to future cyber intrusions.

30. Senator ROUNDS. Have you assessed whether you would be able to adequately verify such an agreement?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. Yes, the Department and Intelligence Community will work to verify the cyber agreement reached during President Xi Jinping's 24–25 September 2015 state visit. The agreement consisted of four key commitments focused on the provision of assistance and information on, and investigation of, malicious cyber activities; that either state would not conduct or knowingly support theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors; to identify and promote norms of behavior in cyberspace within the international community; and establish a high level joint dialogue mechanism on fighting cybercrime or related issues. The "trust, but verify" whole-of-government approach will be implemented through traditional intelligence methods and enhanced with engagement via open dialogue to ensure transparency.

The United States will have to watch China's behavior, and it will be incumbent on the Intelligence Community to depict and help portray to policymakers what behavioral changes, if any, may result from confronting the Chinese with evidence of any transgression or violation of this agreement. In addition, the United States will need to continue to use all instruments of national power to deter this kind of behavior and work closely with interagency and international partners to explore addi-

tional whole-of-government approaches to impose costs on China in order to deter unacceptable behavior.

Admiral ROGERS. The DOD, in coordination with other Departments and Agencies, as well as the private sector, continues to improve our capacity to detect, attribute, and respond to cyber intrusions.

31. Senator ROUNDS. Are you aware of any commitments by China to stop stealing personally identifiable information such as the hack against Anthem that included the information of nearly 80 million Americans? What about OPM?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. No. The cyber agreement and associated commitments reached during President Xi Jinping's 24–25 September 2015 state visit did not address personally identifiable information (PII). As for the specific hacking examples given in this question, it should be acknowledged that these unattributed activities have been characterized by the Intelligence Community as a form of "cyber espionage." As illustrated so dramatically by the OPM breaches, counterintelligence risks are inherent when foreign intelligence agencies obtain access to an individual's PII and virtual identifiable information. Hence we can expect foreign intelligence agencies and non-state entities to continue to target PII using a variety of physical and electronic methods for espionage purposes.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

RESPONSE TO CYBER ATTACKS ON U.S. FORCES

32. Senator ROUNDS. Admiral Rogers, you have advocated that cyber could be treated like any other military domain: air, land, sea, and space. In that context, do you believe the response to a cyber-attack on the U.S. or our forces overseas should be based upon the same policies governing response to a kinetic attack?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

33. Senator ROUNDS. If not, how should our responses differ for a kinetic attack versus a cyber-attack?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

34. Senator ROUNDS. How might our response vary depending upon which nation conducted the cyberattack, specifically Russia, China, North Korea, or Iran?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

35. Senator ROUNDS. If yes, why have we taken no action against the Chinese after the devastating cyber-attacks they have conducted against us?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

36. Senator ROUNDS. If yes, how can we attribute the attack? How do we detect the 'fingerprints' of an attacker?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

QUESTIONS SUBMITTED BY SENATOR TED CRUZ

CYBER ATTACKS COMBINED WITH CONVENTIONAL OR NUCLEAR ATTACKS

37. Senator CRUZ. Director Clapper, would you rank and characterize the threat level of the cyber capabilities demonstrated by Russia, China, Iran, and North Korea?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

38. Senator CRUZ. Is there a particular signature or methodology to the cyber capabilities we see each of these countries developing?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

39. Senator CRUZ. Admiral Rogers, how robust are the efforts of Russia, China, Iran, and North Korea to integrate cyber operations into their conventional or nuclear warfare strategies?

Admiral ROGERS. [Deleted.]

40. Senator CRUZ. How capable are they of sowing confusion or casting doubt on the reliability or effectiveness of the radars, space based systems, and other early warning systems that we or our allies use?

Admiral ROGERS. [Deleted.]

CYBERESPIONAGE, CYBERCRIME, AND CYBERWARFARE

41. Senator CRUZ. Director Clapper, Secretary Work, and Admiral Rogers, how do you distinguish the difference between cybercrime, cyber espionage, and cyber warfare?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. The Department of Defense approaches cyberspace as a domain, alongside air, maritime, ground, and space. The distinctions between crime, espionage, and warfare in cyberspace are made similarly to how they would be made in any other context; taking into account the nature and effects of an action and the actor initiating it.

Cybercrime refers to any illegal activity that uses a computer as its primary means of commission. It can take a variety of forms, from online fraud, to cyberstalking, to data theft.

Cyberespionage is the use of computer systems and/or networks in order to obtain, deliver, transmit, communicate, or receive information about national defense with an intent, or reason to believe that the injury may be used to injure the United States or the advantage of a foreign nation. Espionage is a violation of Title 18 of the United States Code and would also be considered a cybercrime.

Warfare in and through cyberspace is typically conceptualized as state-on-state or state-on-nonstate action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional use of force.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

42. Senator CRUZ. Do you believe that gaining access or infiltrating critical infrastructure is an act of espionage, or an act of warfare?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. Critical infrastructure—the physical and virtual assets, systems, and networks vital to national and economic security, health, and safety—is vulnerable to cyberattacks by foreign governments, criminal entities, and lone actors. In cases involving cyberespionage, the attacker establishes access, periodically revisits the victim's network, and steals their intellectual property. By contrast, in cases of cyber warfare, if an adversarial nation launches a sophisticated, targeted cyber-attack that takes down significant parts of our critical infrastructure, the consequences could be significantly disruptive or potentially devastating. Determining whether such an incident would constitute cyberespionage or an act of warfare would depend upon the facts of the case.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

43. Senator CRUZ. Do you believe that damaging or destroying those systems constitutes an act of cyber warfare?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. The United States is vulnerable to cyber intrusions and potential cyberattack against our critical infrastructure. Cyberattacks can affect our critical infrastructure, the national economy, and military operations. Determination of whether an incident is an act of war should follow the same practice as in other domains, because it is the severity, not the means of an attack, which matters most. Whether a particular attack is considered an "act of war," in or out of cyberspace, requires determination on a case-by-case and fact-specific basis. Malicious cyber activities could result in death, injury, or significant destruction. Any such activities

would be regarded with the utmost concern. The Department is pursuing several initiatives to reduce our vulnerabilities and works in close collaboration with Department of Homeland Security on protecting critical infrastructure.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

44. Senator CRUZ. How would you classify theft or alteration of personnel information in a database? How would you classify disruption, degradation, or destruction of sensors and early warning systems?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. The Department takes these kinds of actions very seriously and classification of specific actions such as these must be made on a case-by-case basis, according to the facts. In the case of theft or alteration of personnel information in a database, we would assess the action, the actor, the effects and the possible intent. Depending on the assessment, such actions would be considered acts of espionage or criminal acts. We would make a similar assessment for disruption, degradation, or destruction of sensors and early warning systems. Such actions could be considered a use of force depending on the specific circumstances.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

45. Senator CRUZ. In instances where these activities might cross lines or lie across multiple definitions, how will the scope and scale of the instance be considered?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. Malicious cyber activity could potentially cross categories or definitional lines depending on the specific facts of each case. The scope and scale of a particular act will be an important consideration for policymakers, for example, the scope/scale of any impacts on services being provided to citizens or scope/scale of damage to property.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

46. Senator CRUZ. Is there a timeframe or window for that consideration?

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Secretary WORK. There is no specific timeframe for determining how a cyberattack should be categorized or defined. While the Department must be prepared to respond very quickly to blunt or respond to a cyberattack, the United States reserves the right to respond to malicious cyber activity at a time, place, and manner of its choosing. These determinations must be made on a case-by-case and fact-specific basis, with due consideration for the seriousness of a particular act. Based on the specifics of the situation, departments and agencies work as quickly as possible to provide their assessments of a particular situation to the President and his national security team.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

NORMS IN CYBERSPACE AND DETERRENCE

47. Senator CRUZ. Director Clapper stated that the absence of universally accepted and enforceable norms has contributed to cyber threats we face. However, I would argue that it isn't just an absence of norms. The Ayatollah in Iran cares nothing for international norms; neither does ISIS. Similarly, Putin cares little about the international community and will act if he believes he can get away with it. We talk of norms, but the Chinese have a long track record of flouting the legal guidelines for intellectual property. Despite China's membership in the World Trade Organization, they consistently fail to fulfill WTO obligations. The glaring reality is that we must have a means to visibly deter our adversaries and holding them accountable if they choose to conduct offensive operations against our national security interests. Admiral Rogers, what do you require in the form of policy or guidance in order to improve our deterrence capabilities?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

48. Senator CRUZ. Admiral Rogers, if tasked to do so, do you possess the capabilities to effectively retaliate against any adversary in the cyber domain?
Admiral ROGERS. {Deleted.]

49. Senator CRUZ. Admiral Rogers, if so ordered, could you destroy networks and devices, or harm physical infrastructure in the states or regions that choose not to follow norms of behavior? If not, what would it take to develop those capabilities?
Admiral ROGERS. [Deleted.]

50. Senator CRUZ. Admiral Rogers, if the Chinese continue to violate norms of behavior surrounding intellectual property and defense information, do you possess the capability to tear down the Great Firewall and reveal to the citizens of China the extent of censorship the Communist Party imposes on them?
Admiral ROGERS. [Deleted.]

51. Senator CRUZ. Secretary Work, how do you plan to engage the other pillars of influence in response to a cyberattack?
Secretary WORK. The Administration is pursuing a comprehensive strategy to confront malicious cyber actors. That strategy includes diplomacy, law enforcement, and other measures such as sanctions on individuals or entities that engage in certain significant, malicious cyber-enabled activities. The Department is fully integrated in the Administration's efforts to ensure a cyberattack is met with a whole-of-government response. The Department coordinates closely with the Department of Homeland Security, the Federal Bureau of Investigation, and other departments and agencies across the government, as well as key stakeholders outside of government. The intent of this approach is to ensure the United States can respond in any manner appropriate at the time, manner, and place of our choosing as the President has previously stated.

52. Senator CRUZ. Secretary Work, do you have the necessary tools to isolate and retaliate against the aggressor, particularly if that aggressor is a non-state actor?
Secretary WORK. The Department of Defense has demonstrated its ability to isolate and remove malicious actors from our networks effectively, regardless of whether they are a State or non-State actor. The Department continues to develop tools and capabilities to improve the timeliness of responses, to harden defenses, and to mitigate any malicious activity.
The Department continues to develop our cybersecurity response capabilities, but any response to malicious cyber activity will be at a time, manner, and place of the President's choosing. Potential aggressors must know that we will be able to hold them accountable, using appropriate instruments of U.S. power and in accordance with applicable law.

ADEQUATE RESOURCES FOR CYBERSECURITY

53. Senator CRUZ. Admiral Rogers, you coordinate the efforts of the National Mission Teams responsible for defending the nation's critical infrastructure. Toward that end, how many state backed adversaries or groups are you currently monitoring and countering, how many non-state actors or groups are you currently monitoring and countering, and how many National Mission Teams currently work full time to counter these groups?
Admiral ROGERS. [Deleted.]

54. Senator CRUZ. Admiral Rogers, do you believe that you have adequate resources to offset the number and volume of threats, and defend the critical infrastructure and defense networks of this nation?
Admiral ROGERS. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR JACK REED

AUTHORITY FOR IMPOSING SANCTIONS ON CHINA FOR INDUSTRIAL ESPIONAGE

55. Senator REED. Secretary Work, President Obama in April 2015 signed an executive order establishing a process to impose sanctions for industrial espionage through cyberspace under the International Emergency Economic Powers Act (IEEPA) and other authorities and statutes. Prior to this action, Senator Levin and Senator McCain, with co-sponsors, included a provision (section 1637) in the Fiscal Year 2015 NDAA granting the President under IEEPA to impose such sanctions. Yet, to my knowledge, the President and his staff have not referenced this congres-

sional grant of authority that buttresses the order he imposed. Since the President's power is at its strongest when he acts with congressional concurrence, and since doing so would help to persuade China of our seriousness, the President's omission is more than curious. Do you have an explanation for why the President has not cited this explicit congressional support for threatening and imposing sanctions in response to industrial espionage through cyberspace

Secretary WORK. My understanding is that the Administration supports and welcomes section 1637 of the National Defense Authorization Act for Fiscal Year 2015 and views it as a valuable tool for compelling foreign countries, including China, to refrain from economic or industrial espionage in cyberspace.

ENCRYPTION

56. Senator REED. Admiral Rogers, twice in the 1990s NSA rang alarm bells over encryption, predicting that strong encryption would become ubiquitous. The first time was in the early-to-mid 90s, when NSA proposed the adoption of the so-called "Clipper Chip" that would enable the government to access unenciphered content through legal processes. The second time was in the late 90s when companies overseas began selling strong commercial encryption and U.S. companies demanded easing of export controls to enable them to compete globally. In both cases, the dire predictions of NSA and law enforcement officials did not materialize. What makes this situation different?

Admiral ROGERS. Since the mid-90's, encryption has grown in complexity and difficulty, and it is now used to protect millions of daily communications across the global network. It is used by friend and foe alike. However, the National Security Agency (NSA) would not describe the situation as "dire." The prevalence of encryption across the global network is good for the nation. It protects our daily commerce, and is an important element of cyber defense for individuals, corporations, and government.

At the same time, the prevalence of encryption has provided adversaries of the United States the ability to communicate in a way that impairs the Intelligence Community's ability to gather information and understand their actions and motives. There is no one-size-fits all approach to dealing with the challenge of encryption. NSA continues to explore new techniques and methods to counter adversary use of encryption. Continued support of NSA's investment in world class technical talent, as well as the technology and tools needed to counter encryption is vital to give us the best chance of success.

ELEVATING CYBER COMMAND TO A UNIFIED COMMAND AND SUSTAINING THE "DUAL HATTING" OF THE COMMANDER OF CYBER COMMAND AS THE DIRECTOR OF NSA

57. Senator REED. Secretary Work and Admiral Rogers: The Committee understands that the Chairman of the Joint Chiefs is considering recommending to the President that the next Unified Command Plan elevate Cyber Command from a sub-unified command under U.S. Strategic Command to a full unified command. It is rumored that the Department is not considering alteration of the current arrangement under which the Commander of Cyber Command also serves as the Director of NSA. The Armed Services Committee has for several years expressed concern about this dual-hat arrangement in the context of a decision to make Cyber Command a new unified command. There are reports that the Department fears that ending the dual-hat arrangement would result in NSA not sustaining the necessary level of support for the Command, despite NSA's designation under the Goldwater-Nichols Act as a combat support defense agency. Is this a genuine fear? It would be disturbing if NSA could not be counted upon to faithfully execute orders.

Secretary WORK. The National Security Agency (NSA) provides robust and excellent support to the Department and U.S. Cyber Command (USCYBERCOM), and I have the fullest confidence in NSA's willingness and ability to execute its mission. The dual-hat arrangement provides necessary support to USCYBERCOM as it continues to grow and mature in its mission execution, and the Cyber Mission Force benefits greatly from the experience of its NSA partner. The relationship between the two organizations demonstrates a unity of effort and close collaboration in a field of growing importance.

The decision to decouple the organizations must rely upon a conditions-based approach that considers several criteria, including ensuring that USCYBERCOM is manned, trained, and equipped to fulfill its missions. One of the key considerations in prolonging the dual-hat arrangement is the efficiency created when allocating workforce resources, which are often common for both NSA's and USCYBERCOM's respective missions. In light of the current fiscal climate, as well as efforts to develop the DOD cyber workforce, we believe the dual-hat arrangement remains the

prudent course of action at this time. However, I am grateful to Congress for the budgetary assistance in helping the Department and USCYBERCOM take on its new mission.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

58. Senator REED. We have also heard the argument that Cyber Command is so dependent on NSA that separating these positions would put Cyber Command's effectiveness at risk. If this reflects the views of DOD's leadership, what does it say about the maturity of Cyber Command and its readiness to be a unified command?

Secretary WORK. I support the President's decision in December 2013 to maintain the dual-hat arrangement for Cyber Command and NSA. The dual-hat arrangement has allowed for the unification of leadership for the organizations responsible for defending the nation in cyberspace and for signals intelligence. By virtue of their relationship, Cyber Command is able to fully leverage NSA's resources, enabling a more coordinated and rapid response to threats in cyberspace. The Department of Defense is in the third year of an ambitious plan to develop the Cyber Mission Force and develop additional capabilities as a sub-unified command. As Cyber Command continues to mature, the Department will analyze and assess the merits of whether it should be elevated to a full unified combatant command.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

59. Senator REED. The Services are just now reaching IOC for the bulk of the newly created cyber mission force units. Until we began fielding these units, Cyber Command had very few forces with which to execute its missions. Moreover, we are a number of years away from equipping these forces with the tools, weapons systems, infrastructure, and command and control capabilities they need to operate effectively. What does the lack of such capabilities say about the maturity of the Command?

Secretary WORK. The Department of Defense (DOD) is in the third year of an ambitious plan to build the Cyber Mission Force, which envisions 133 teams as fully manned, trained, and equipped by the end of Fiscal Year 2018. As part of this plan, DOD closely evaluates Cyber Command's maturation and its ability to execute its missions. This includes regularly assessing the resources, tools, infrastructure, and facilities needed to train, equip, and enable Cyber Mission Force team personnel to operate effectively. The Department also assesses the resources required to build and develop cyberspace operations, intelligence, and planning staffs that support operational and strategic level headquarters.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

60. Senator REED. When Cyber Command was established, NSA leaders asserted that military and intelligence operations in cyberspace overlapped almost entirely, and argued that Cyber Command for efficiency and effectiveness should make use of the infrastructure, planning systems, and tools that NSA had already developed. NSA expected that a military command would operate much the same way that a signals intelligence agency would in cyberspace. Five years later, we know that these assumptions were incorrect. Cyber Command needs separate and different tools, infrastructure, training ranges, planning systems, TTPs, and command and control capabilities from those that NSA has developed for its own use. Cyber Command has surely benefited substantially from having a uniquely close relationship with NSA, but it also seems possible that NSA's views and assumptions could have held back the proper development of Cyber Command. What are your views on this possibility?

Secretary WORK. I do not believe that National Security Agency's (NSA) views and assumptions held back the development of Cyber Command. In fact, NSA played a direct role in supporting Cyber Command's development, providing critical expertise in training, education, certification, techniques, mission sharing, and capability development. In addition, by virtue of their relationship, Cyber Command leveraged NSA's cryptologic enterprise to enable a more coordinated and rapid response to countering threats in cyberspace. Cyber Command does need separate tools, infrastructure, and capabilities to conduct certain missions, but the arrangement between Cyber Command and NSA enabled Cyber Command to learn key lessons and mature as an enterprise.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

61. Senator REED. Combatant commanders by design have broad and extensive command experience and education in combined arms and joint warfare. Traditionally, combatant commanders have been drawn from the ranks of combat arms officers or, in Navy parlance, "officers of the line." NSA Directors, in contrast, are typically selected from the Service Cryptologic Elements, or at least from the ranks of intelligence specialists. Maintaining the dual-hat arrangement into the future will mean that either cyber combatant commanders are going to be intelligence specialists, or NSA will not be led by career intelligence officers, which may be a disservice to both organizations. What are your views on this dilemma?

Secretary WORK. The dual-hat remains important to the success of the Department's mission in cyberspace and thus far the arrangement has not created any sort of dilemma. I have full trust and confidence in the capabilities of past, present, and any future National Security Agency (NSA) Director/Commander, U.S. Cyber Command (USCYBERCOM), and their ability to fully support and command both organizations. NSA plays a unique role in supporting USCYBERCOM's mission and helps integrate capabilities and infrastructure and enable operational effectiveness while USCYBERCOM continues to build its capabilities and infrastructure.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

62. Senator REED. When the CIA Director was also the Director of Central Intelligence—the head of the Intelligence Community—the intelligence agencies other than the CIA did not believe that the DCI was an honest broker. They believed that the DCI favored the CIA, and resisted centralized control and appeals to jointness. Dual-hatting the Commander as NSA Director would appear to present the same drawback: the military service cyber components would likely always see NSA as privileged and more powerful. Do you think that the dual-hat arrangement has potentially some unhealthy side effects?

Secretary WORK. The comparison between the previous situation when the Central Intelligence Agency director was also the Director of Central Intelligence and the current Director, National Security Agency (NSA)/Commander, U.S. Cyber Command (USCYBERCOM) dual-hatting can appear to be similar. However, in this case, the authorities, budgetary lines, and overall missions of USCYBERCOM and NSA are different, which alleviates risk of preferential treatment. Additionally, USCYBERCOM follows the same processes for requesting intelligence from the national intelligence system as other commands and agencies.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

63. Senator REED. Have you considered the idea of keeping the dual-hat arrangement only for a certain period of time, perhaps selecting a "sunset" date when it would be ended, and Cyber Command would be expected to be self-sufficient except for those specialized needs that could and should be met by NSA as a combat support agency?

Secretary WORK. The dual-hat remains important to the success of the Department's mission in cyberspace. The National Security Agency plays a unique role in supporting U.S. Cyber Command's mission, providing critical support, including linguists, analysts, cryptanalytic capabilities, and sophisticated technological infrastructure. The dual-hat helps integrate capabilities and infrastructure and enable operational effectiveness while U.S. Cyber Command continues to build its capabilities and infrastructure. Building U.S. Cyber Command's capabilities is a top priority of the cyber strategy. If a decision is made to end the dual-hat arrangement it will be based on the capabilities and needs of the command rather than being tied to a set date.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

QUESTIONS SUBMITTED BY SENATOR KRISTEN GILLIBRAND

DYNAMIC THREAT RESPONSE

64. Senator GILLIBRAND. Admiral Rogers, in March you told us that one of the issues you have raised internally in the Department is "that in creating the force, we've allocated all very specifically across the board. And so one of the implications . . . [is] we perhaps didn't build in as much flexibility as our experience now is telling us perhaps we need. So, that's something, to be honest, within the Department,

we're going to be looking at." Can you give us an update on any work you have done to create more flexibility?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

65. Senator GILLIBRAND. As we have seen in the past year, many cyber incidents have come to light that are not necessarily directed at the military, but at U.S. institutions, including other government agencies and private businesses. How do you see CYBERCOM supporting a whole of government approach to these major domestic cyber incidents?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

66. Senator GILLIBRAND. What do you need to better support a whole-of-nation approach to a cyber incident?

Secretary WORK. Answer is for official use only and will be retained in committee files.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

67. Senator GILLIBRAND. After FY16, how will the people assigned to CYBERCOM receive the necessary training?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

68. Senator GILLIBRAND. How do we ensure that the reserve component gets equivalent and timely training?

Secretary WORK. The Department ensures the Reserve Component gets equivalent training by continued adherence to the Services' policies that stipulate that there is to be no differentiation in training requirements and standards between the Reserve and Active Components. Additionally, reliance on the Services' force generation models ensures that Reserve Component forces receive any additional equivalent training in accordance with timelines established by the Secretary of Defense (in response to Presidential/ National Security Council guidance).

69. Senator GILLIBRAND. Please provide your thoughts on the relationship between the Department of Homeland Security (DHS) and DOD in terms of global cyber security roles and responsibilities.

Secretary WORK. The Department of Defense (DOD) works very closely with its interagency partners to ensure that it is building and implementing a whole-of-government approach to cybersecurity. DOD's relationships with the Department of Homeland Security (DHS) and the Department of Justice (DOJ) are and must remain strong, given that DHS and DOJ have the lead for domestic response to cyber threats. In this context, DOD has a support role.

DOD and DHS regularly collaborate and share information through a variety of channels, ranging from daily communication between operational centers to interagency forums. The two organizations also exercise together to ensure unity of effort across the departments and determine what assets and resources DOD may be able to provide to support DHS and DOJ in an emergency.

We continue to develop ways to improve collaboration and information sharing to protect and defend U.S. critical infrastructure, to create consistent approaches to cybersecurity across both national security and non-national security systems, and to enhance our ability to prevent, mitigate, respond to, and recover from domestic cyber incidents.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

70. Senator GILLIBRAND. What specifically do you see as the Department of Defense's role in support of the states, DHS and FBI?

Secretary WORK. Ensuring the nation's cybersecurity is a shared responsibility. The Department of Homeland Security (DHS) is the lead federal department responsible for national protection against, mitigation of, and recovery from domestic cybersecurity incidents. The Department of Justice (DOJ) is responsible for the investigation, attribution, disruption, and prosecution of cybercrimes outside of military jurisdiction.

As in other domains, the Department of Defense (DOD) supports DHS and DOJ when necessary and through those agencies, can support the private sector and state/local governments. For example, DOD is developing capabilities to respond and

defend its own network that could provide support to DHS and the Federal Bureau of Investigation during an emergency through the Defense Support of Civil Authorities process.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

71. Senator GILLIBRAND. What changes to legislation do you need to provide a better response to a domestic cyber incident and complement the efforts of DHS and FBI?

Secretary WORK. The Department supports legislation to increase information sharing between government and industry that will improve the Nation's cybersecurity posture. While many companies currently share cybersecurity threat information under existing laws, there is a growing need to increase the volume and speed of information shared without sacrificing the protection of privacy, confidentiality, civil rights, or civil liberties. It is essential to ensure that cyber threat information can be shared quickly between trusted partners so that network owners and operators can take the necessary steps to block threats and avoid damage. The Department also supports other key provisions, such as data breach and cybercriminal provisions, included in the President's legislative proposal submitted earlier this year.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

RESERVES AND THE NATIONAL GUARD/HOMELAND SECURITY

72. Senator GILLIBRAND. DOD put out its report about the role of the reserve component in cyber last year. Can you please tell us what capabilities have already been set up?

Secretary WORK. As the Department continues to strengthen the Cyber Mission Force, we recognize the need to incorporate the strengths and skills inherent within the Reserve and National Guard forces. Each Service developed Reserve Component integration strategies that embrace Active Component capabilities in the cyberspace domain and leverage the Reserve and National Guard strengths from the private sector. Up to 2,000 Reserve and National Guard personnel support the Cyber Mission Force and allow the Department to surge cyber forces in a crisis.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

73. Senator GILLIBRAND. When will the reserve component teams be trained to NSA standards and what are the impediments to getting them on board?

Secretary WORK. Reserve Component teams are already trained to the National Security Agency's (NSA) standards, the training courses they receive depend on their individual role within the Cyber Mission Teams. The Air Force, Navy and Army undergraduate cyber training course, which the Reserve Component attends, has been accredited by the NSA and meets all NSA requirements for Cyber Protection Teams mission roles. For other roles and missions, Cyber Mission Teams and National Mission Teams, additional training may be required and is conducted by the NSA. I see no impediments at this time

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

74. Senator GILLIBRAND. What missions will the reserve component teams have both at CYBERCOM and at the service level?

Secretary WORK. As stated in the Department of Defense Cyber Strategy, the Department draws on the National Guard and Reserve Components as a resource for expertise and to foster creative solutions to cybersecurity problems. The Reserve Component (RC) offers unique capabilities for supporting each of the Department's missions, including engaging the defense industrial base and the commercial sector. It represents a critical surge capacity for cyber responders.

Specific to USCYBERCOM and the Services, the Department is integrating approximately 2,000 Reserve Component personnel into the Cyber Mission Force to contribute Cyber Protection Teams (CPT) as well as to provide surge support. While there are RC personnel qualified to perform National Mission Team and Combat Mission Team tasks to defend the Nation and support combatant commander tasks, most RC personnel and units align most closely with the CPT mission, which is the most similar to their professional civilian roles. These CPT units are aligned to the Services to protect Service networks.

Admiral ROGERS. The reserve component personnel assigned to U.S. Cyber Command (USCYBERCOM), while in active duty status, will continue to play vital roles

on the Cyber Mission Force (CMF) teams and in other areas. Currently, several Air National Guard squadrons are training to support key Cyber National Mission Force, Service, and Combatant Command aligned CMF teams. The Army National Guard currently supplements USCYBERCOM's staff in specialized areas and performs critical missions. The Army National Guard is currently developing a method to source cyber professionals nationwide to aid USCYBERCOM in these roles. Army, Navy, Marines and Air Force reservists have supported USCYBERCOM from its conception with military and civilian cyber skills and training. At Camp Parks, California we have maintained a group of expert reserve intelligence personnel producing high quality cyber intelligence products for over six years. Our use and planned use of reserve personnel provide an instant force multiplier for the Command, DOD and the United States.

75. Senator GILLIBRAND. Admiral Rogers, you also told us that "Because we're still really focused on the initial cadre [of cyber warriors], the challenge is going to be, 'So, how do you sustain it as people come and go? That's something we're going to be in the—in the next year or two, in particular, spending a lot of time on.' Can you please explain how you are planning to develop that next cadre?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

76. Senator GILLIBRAND. What might be the role of the reserve component in this next stage of cadre development?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

77. Senator GILLIBRAND. As members transition to other positions both in the military and in the civilian sector, how do you think the reserve components can help retain the talent of the individuals already trained?

Secretary WORK. This is a key focus area for the Department. Cyber talent, whether serving in the Active Duty or Reserve Component, is the same. Ensuring the highest return on investment for our cyber training is necessary. The "DOD Cyber Strategy" challenges the Department to use the National Guard and Reserves as a resource for expertise and to foster creative solutions to cybersecurity problems. Retaining that talent is a focus point for my attention.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

RECRUITMENT

78. Senator GILLIBRAND. It is my understanding that the training necessary to build a cyber-warrior can take up to 2 years. How do you envision the development not only of separate specialties for cyber but also career tracks for these cyber warriors?

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

79. Senator GILLIBRAND. What direction has been given to the services regarding recruiting goals and priorities for individuals with skills and aptitudes relevant to the needs of CYBERCOM?

Secretary WORK. The Department of Defense Cyber Strategy Strategic Goal #1 is to "Build and Maintain Ready Forces and Capabilities to Conduct Cyberspace Operations." The Office of the Undersecretary of Defense for Personnel and Readiness and the Office of the Department of Defense Chief Information Officer, in coordination with the Military Departments, USCYBERCOM, and the Joint Staff, are leading this line of effort, which is specifically focused on recruiting, retention, training and other developmental needs for building viable career paths for these recruits. We recognize that the talent pool is highly competitive for each of the Services and U.S. Cyber Command, which continue to mature their cyber aptitude assessments to better identify talent with the potential to succeed in the cyber workforce. Recruiting goals are important, but just as important are viable career paths for cyber recruits; such career paths are a critical piece of the solution. Our objective is to create a career path model with established standards to meet mission requirements and career progression. To that end, the Department is focused not only on recruiting the appropriate talent to meet mission requirements at more senior levels, we are also focused on growing cyber talent at the entry level through a more robust on-campus recruiting effort targeting students and recent graduates, which is one of the highest priority civilian workforce Force of the Future initiatives.

Admiral ROGERS.

80. Senator GILLIBRAND. In your opinion, what can Congress do to assist DOD in this effort of recruitment and retention?

Secretary WORK. The improving economy and scaled-back advertising campaigns over the past decade have reduced both the number of young Americans considering military service and their understanding of military service. Evidence of this trend is the fact that the most recent survey by the Joint Advertising, Market Research and Studies (JAMRS) office indicated that only one in four young Americans can name all the military services. Given this trend, we anticipate that meeting recruiting goals with high-quality and diverse candidates will become increasingly more difficult, particularly if the projected budget constraints persist. As the realities of sequestration and shrinking defense budgets continue, the impact to force readiness will remain a significant and constant concern; lost messaging and reduced recruiting presence further compounds this issue. Absent near-term relief, the Military Departments will have to choose between maintaining critical infrastructure and sustaining the All-Volunteer Force.

We have committed to investing in our recruiting data analytics in JAMRS as part of our force of the future initiatives to help us better target the qualified candidates in the youth population. Continued congressional support is essential to maintaining adequate investments in recruiting resources, which will generate the future force upon which the nation will depend. Mass marketing in traditional media, as well as more tailored social media campaigns will provide increased opportunities to afford both young Americans and their influencers (e.g., parents, teachers and coaches, clergy) access to accurate information about military service.

The Department is also looking for greater flexibilities, as specified in the Defense Officer Personnel Management Act related legislative proposals submitted to Congress, to assist the Military Services in attracting, recruiting, and retaining highly skilled individuals and high performers. Today, we can access exceptionally skilled and experienced doctors and dentists into the Services and award constructive service credit up to the grade of colonel in the Army, Air Force, or Marine Corps, or captain in the Navy. However, as we look at emerging requirements, we see that this authority may be equally useful in attracting highly skilled personnel in a wide array of technical or scientific fields, to include cyberspace, that are difficult to fill and require extensive training, education, or experience not widely available within the Military departments.

81. Senator GILLIBRAND. As we start planning for the FY17 NDAA, are there any issues with regards to recruitment and retention, the role of DOD in a whole-of-nation approach, or the role of the reserve component that you would like to see addressed?

Secretary WORK. While the American public clearly has faith in the efficacy of our military, a disconnect, defined by lack of knowledge, misperceptions, and an inability to identify with those who choose to serve, has emerged in today's society. This disconnect threatens our ability to recruit quality youth with needed skill sets to maintain our military force. A variety of circumstances have contributed to the disconnect, such as a shrinking/disappearing military footprint in parts of our country, declining veteran presence, a perception that military service will result in disability or Post-Traumatic Stress Disorder, and reduced recruiting advertising due to budget reductions. This disconnect is compounded by the number of youth not qualified for military service (about 71 percent), and the relatively low propensity for youth to serve (12 percent). Given appropriate resources, the Department will be proactive and ensure the appropriate recruiting tools are available to address these changes in the recruiting environment. Additionally, while the Military Departments have been successful in achieving their retention goals in recent years, the improving economy and job market, compounded by tightening budgets, will make it more difficult to retain many of the most experienced service members with high-demand skills.

QUESTIONS SUBMITTED BY SENATOR JOE DONNELLY

HARDWARE ASSURANCE

82. Senator DONNELLY. Secretary Work, I have been to NSWC Crane in Indiana on several occasions and have witnessed the efforts on trusted electronics/high reliability hardware being accomplished there. The work at NSWC Crane supports our nation's nuclear deterrence programs such as the Navy's Strategic Systems Program

and recently they have begun collaborating with the Air Force to support that service's strategic capabilities. What are your thoughts on how this emerging collaboration within DOD can be extended to a collaborative effort with DoE to address the emerging threats to our nation's trusted defense systems?

Secretary WORK. The Department is already working in cooperation with the Department of Energy (DOE) to mitigate supply chain vulnerabilities. DOE is updating their nuclear security policies to incorporate a Weapon Trust Assurance program and a Supply Chain Risk Management program to ensure malicious hardware or software does not enter the Nuclear Security Enterprise supply chain. DOE recently became a participant in the Joint Federated Assurance Center (JFAC), which was established to improve collaboration among hardware and software assurance capabilities like those that Naval Surface Warfare Center (NSWC) Crane possesses and to make these capabilities visible to defense system programs. The JFAC considers Sandia National Laboratory and other DOE laboratories to be potential service providers. DOE participation in the JFAC resulted from collaboration between DOD and DOE leadership on microelectronics assurance activities via the Mission Executive Council, which is an interagency body chartered to promote common interests.

83. Senator DONNELLY. Secretary Work, Section 937 of the National Defense Authorization Act for Fiscal Year 2014 established a Joint Federated Assurance Center (JFAC) "to serve as a joint, Department-wide federation of capabilities to support the trusted defense system needs of the Department to ensure security in the software and hardware developed, acquired, maintained and used by the Department, pursuant to the trusted defense systems strategy and the Department and supporting policies related to software assurance and supply chain risk management." NSWC Crane in Indiana has become one of our nation's thought leaders on this topic and holds a "hardware" leadership role within JFAC. In general, how is JFAC addressing the critical requirements of combating threats to the strategic electronics supply chain and providing assurance to our strategic deterrence?

Secretary WORK. NSWC Crane leads the Joint Federated Assurance Center (JFAC) Hardware Assurance (HwA) Technical Working Group, which includes representation from the Military Departments, the National Security Agency, and the Defense Microelectronics Activity. The JFAC HwA efforts promote coordination, collaboration, and communication in order to spread best practices in mitigating or countering threats to the strategic electronics supply chain and to foster sharing of assurance resources in support of program needs. We have established a JFAC operational concept and piloted several cases where critical needs for software assurance (SwA) and HwA have been met. In FY 2016, pilots will include JFAC efforts within the strategic deterrence enterprise, promote Department SwA and HwA capabilities, and provide guidance on how to request and integrate these technical assessments into acquisition programs. The JFAC will monitor demand for SwA and HwA support and identify future capability and capacity needs.

84. Senator DONNELLY. Secretary Work, more specifically, in light of the IBM Foundry sale, what is the role of JFAC in assuring the integrity of integrated circuits not manufactured in a trusted foundry?

Secretary WORK. For critical parts not manufactured in a trusted foundry, the Joint Federated Assurance Center (JFAC) will enable acquisition programs to evaluate trustworthiness of microelectronics software and hardware. In light of the IBM Foundry sale, the JFAC plays an important role in maintaining a library of techniques used to determine the integrity and authenticity of application-specific integrated circuits that may now be produced in other foundries. The JFAC will help acquisition programs plan and implement assurance activities including vulnerability assessment, detection, analysis, and mitigation. Through the JFAC, participating organizations will share information about emerging threats and capabilities, software and hardware assessment tools and services, and best practices. Assurance services include inspection, functional verification, physical verification, vulnerability detection, detailed analysis, assessment, and, in a growing number of instances, recommendations for remediation.

QUESTIONS SUBMITTED BY SENATOR TIM KAINE

U.S. CYBER COMMAND WORKFORCE

85. Senator KAINE. Secretary Work and Admiral Rogers, U.S. Cyber Command's current manning goals have been reported as 133 cyber mission teams, requiring approximately 6200 trained personnel by the close of 2016. Does DOD still antici-

pate reaching this goal by the end of next year? Please elaborate on challenges experienced hiring sufficiently skilled operators and whether or not there are unique challenges to the Armed Services compared to the cyber industry overall. Most importantly, explain how the full staffing of U.S. Cyber Command will be affected—numbers and timeline—if a budget agreement is delayed or not reached by the end of CY15.

Secretary WORK. Answer is for official use only and will be retained in committee files.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

NON-DEFENSE AGENCIES

86. Senator KAINE. Director Clapper and Admiral Rogers, despite attempts to use OCO funding to mitigate BCA funding for defense, sequestration level funding will severely decrease budgets at federal agencies that closely coordinate with DOD on cyber activities. With DHS designated as the lead agency for cyber protection of non-defense domains, it is presumed that any funding loss will hamper cyber operations at all our government agencies, particularly for non-DOD efforts related to law enforcement and cyber-related investigations. Please elaborate on any national security concerns if funding is not provided for a comprehensive interagency cyber effort for contingency operations abroad and for ongoing cyber surveillance and protection programs that rely on both DOD and non-defense agencies to work effectively.

Director Clapper did not respond in time for printing. When received, answer will be retained in committee files.

Admiral ROGERS. Answer is for official use only and will be retained in committee files.

○