DEPUTY SECRETARY OF DEFENSE ROBERT O. WORK
OPENING STATEMENT BEFORE THE SENATE ARMED SERVICES COMMITTEE
TUESDAY, SEPTEMBER 29, 2015

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.