STATEMENT OF

LIEUTENANT GENERAL J. KEVIN MCLAUGHLIN

DEPUTY COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

EMERGING THREATS & CAPABILITIES SUBCOMMITTEE

19 APRIL 2016

Chairman Fischer, Ranking Member Nelson, and Members of the subcommittee, I am honored to appear before you today to discuss the activities of US Cyber Command (USCYBERCOM) in support of Department of Defense (DoD) efforts to enhance mission assurance, build resilience, and defend our critical infrastructure. It is my pleasure to do so alongside Assistant Secretary Thomas Atkin, who has told you about the Department's cooperative and extensive efforts in these areas. These efforts, and complementary work to mitigate risks that we incur due to our connections to civilian infrastructure, have been strengthened by DoD's collaboration with federal agencies and the private sector. Although such work remains on-going and will require sustained effort, DoD has a way forward. USCYBERCOM's role in this collective effort is what I hope to explain in more detail.

The Current Environment

Before I discuss matters specific to USCYBEROM, allow me to give you a clearer idea of why developments in cyberspace matter so much to our government and to the American people. Malicious cyber actors who gain access to the networks of our critical infrastructure could manipulate information or software, destroy data, harm the computers that host those data, and even impair the functioning of systems that those computers control. In short, cyberattacks could cause catastrophic damage to portions of our power grid, communications networks, and vital services. Destructive if not catastrophic strikes on infrastructure have already occurred in Europe. Just before Christmas last year, malicious actors launched coordinated cyberattacks on Ukraine's power grid, causing outages and damaging electrical control systems. If directed at the critical infrastructure that supports our nation's military, cyberattacks could hamper our

forces, interfere with deployments, command and control, and supply functions, and have broader impacts across our society.

Malicious cyber actors collectively launch a range of activities to support their interests in: a) fostering a nationalist vision of economic competition; b) intimidating émigré groups and neighbors whom they view as competitors; and c) deterring perceived threats from other states, including ours. They steal intellectual capital from our corporations and laboratories, and we learned last year that certain actors also stole the personal information of more than 21 million Americans that was stored in systems maintained by the Office of Personnel Management. Another group of hackers was responsible for an intrusion into an unclassified network maintained by our Joint Staff. Finally, we have seen cyber actors from more than one nation explore the networks of our nation's critical infrastructure (as the recent indictments of several Iranian hackers suggested). The largest threats to the Department and to the nation are those targeted against vulnerabilities in the networks supporting electric power, transportation, finance, and other sectors; these systems are designated critical because if they are not functioning then the United States will incur serious strategic risks.

Organizing to Provide Mission Assurance and Defend Critical Infrastructure

USCYBERCOM supports the Department's broader cyber strategy by planning and acting on a wide range of issues pertaining to the cyber field. Our mission set has us directing the operation and defense of the Department's networks and systems; assisting other U.S. government entities (as authorized and upon the request of the relevant department or agency) in the job of defending the United States and its interests against significant cyber incidents; and supporting the missions of the combatant commands by providing integrated cyber capabilities. Our experts are called upon, for instance, to help with the implementation of the new DoD Cyber Strategy, and

with the defense of sensitive databases containing DoD personnel or affiliates' personally identifying information. In addition, senior leaders at the Command are either leading or serving on all of the teams charged with implementing the DoD Cyber Strategy's many initiatives, particularly those tasked with integrating cyber effects in DoD and cross-agency planning efforts.

The work of improving our ability to operate in cyberspace begins in our own DoD information systems. Our top priority remains the defense of the Department's systems to assure the ability to conduct DoD missions; if these systems do not function, then our national military power is at risk in all of the domains in which it operates. The Department of Defense as a whole is working to harden and defend its networks, with USCYBERCOM providing the operational vision and directing the defense, and the DoD Chief Information Officer (CIO) providing the technical standards and implementation of policy. We work daily with the National Security Agency (NSA), the Defense Information Systems Agency (DISA), the Combatant Commands, and the military services to secure, operate, and defend DoD systems.

Defending DoD's critical infrastructure in cyberspace is no easy task, and it requires a team effort. In a previous job in the Air Force, for instance, I found that I had a key partner in the Air Force Civil Engineering Center. I had not initially understood the importance of engaging our Air Force civil engineers unless I needed them to build a building or manage a construction project. In fact, they managed the deployment of much of the Air Force's critical infrastructure—important things like buildings and power generation on bases—all of which are now networked. I learned a lesson, and found another partner that we needed to work with early on to ensure the Air Force not only builds secure networked systems in the future but also helps us find ways to defend the infrastructure that we have already fielded.

A range of challenges loom before USCYBERCOM and every DoD component engaged in defending DoD information systems. Perhaps the greatest is the persistence of legacy systems, practices, and mindsets. In the United States military we have networked practically everything, and that networking of systems began in earnest decades ago with the growth of the Internet when the United States Government did not anticipate the sort of threats we see routinely today.

Fixing this requires changing a whole workforce culture. Last year the Department identified the need to transform DoD's cybersecurity culture by improving individual performance and accountability as called for in the DoD Cyber Strategy. As part of this broad effort, the Secretary and Chairman approved the DoD Cybersecurity Culture and Compliance Initiative (DC3I) to initiate a shift in the Department's cybersecurity culture and norms. This initiative seeks to instill principles of operational excellence, personal responsibility, and individual accountability into all who provide or use cyber capability to accomplish a mission. I would offer an example here. The Department already inculcates a culture of responsibility and accountability in every DoD affiliate, both uniformed and civilian, who is authorized to handle a firearm. Our reliance on networks and data systems to accomplish our missions likewise demands that all DoD personnel understand their individual responsibilities to protect the Department of Defense information systems and act with similar discipline and diligence every time they use a DoD system.

Instituting meaningful and lasting cultural change DoD-wide will require a long-term commitment by the Department. USCYBERCOM was identified as the mission lead for this initiative and is working with Joint Staff and the Office of the Secretary of Defense to build the

capacity and structure to increase cybersecurity and promote mission assurance through improved human performance in cyberspace.

Department of Defense networks are continually being probed, so we are learning to combine intelligence reporting, insights we gain from network events, and our knowledge of cybersecurity to achieve situational awareness and an intuitive feel for what is coming next. We are learning how to assess what we call "key terrain" in cyberspace, and even how to map our networks so we understand what is happening on them. As DoD expands the Joint Information Environment, moreover, we will gain confidence in the overall security and resiliency of our systems. How resilient can we make our own installations and even our weapons systems? Last year the director of Operational Test & Evaluation, Mr. Gilmore, stated publicly that each of our weapons systems has critical cyber vulnerabilities. This a complex issue, but I can assure you that USCYBERCOM is working with key stakeholders to identify solutions. We also need to understand how private-sector networks interact with DoD information systems.

Our operations to defend DoD systems and the nation's critical infrastructure proceed in conjunction with federal, industry, and international partners. Defending America in cyberspace is a whole-of-government, indeed a whole-of-nation, endeavor. It also requires close partnership with our allies. No single agency or department has the authority, information, or wisdom to accomplish this mission alone. USCYBERCOM has partners that possess very useful capabilities and skills, so we are constantly seeking to expand our knowledge of what is under development in the Services, national labs, and other departments and agencies. We consult our network of partners across the federal government so that we are ready, if called upon and when directed by the President or the Secretary, to support civil authorities in the context of a significant cyber incident. As an example, USCYBERCOM recently signed a cyber action plan

with the Department of Homeland Security (DHS) and the NSA to define the manner in which we would collaborate in this area. In the context of domestic incidents, we always expect to operate in support of another part of the federal government. DHS has the lead for cybersecurity, and the Department of Justice which has responsibility for Federal law enforcement matters, but other parts of the government have direct responsibilities as well. Our job is to have the capacity and capability ready to go when needed, and the procedures in place with our inter-agency partners, just as we have in other domains, so that we can operate alongside the appropriate U.S. government agencies. This area, I must add, is probably the least developed of our missions from a policy and legal perspective, but one we are actively developing and exercising to formalize.

Even the federal government, however, cannot do this job without the active cooperation of the private sector. DHS brings together private companies, state, local and federal actors, as well as commercial infrastructure providers, with U.S. Cyber Command and the Department of Defense to understand mutual problems. That should help both sides view this as a broader partnership.

We know there are various legal and policy questions that have to be answered with regard to how we can allocate DoD resources inside the United States. Cyberspace, of course, is no exception, but that in itself is encouraging. Years ago we figured out how the nation's military can work with federal, state, and local authorities and the private sector in many other areas. In a natural disaster, for instance, we in DoD know how to shift federal and military resources to assist municipalities and their citizens so they can do the hard jobs of responding, recovering, and rebuilding. It works, and so I am confident that we can figure out how to render similar rapid responses in cyberspace, add value to state, local, and private efforts, and apply

insights from our other operations combined with innovative solutions that will keep our nation safer.

Maturing the Cyber Mission Force

The Cyber Mission Force (CMF) gives USCYBERCOM and the Department a means to apply military capability at scale in cyberspace. USCYBERCOM manpower reflects a true total force effort encompassing a robust active component along with both Guard and Reserve forces being fully integrated at all echelons from the highest levels of our USCYBERCOM headquarters to our Cyber Mission Force teams. Our Combat Mission Teams (CMTs) operate with the combatant commands to support their missions, while National Mission Teams (NMTs)–when directed, and in support civil authorities—help defend the nation's critical infrastructure from malicious cyber activity of significant consequence. We have Cyber Protection Teams (CPTs) to defend DoD Information Networks alongside local Cybersecurity Service Providers. At USCYBERCOM, we also have several CPTs with unique capabilities that could provide assistance to DHS in responding to domestic incidents. Finally, last year we established the Joint Force Headquarters-Department of Defense Information Network (JFHQ-DoDIN) and dual-hatted the Director of DISA as the Commander. JFHQ-DoDIN is a functional component command of USCYBERCOM located at DISA that directs an aggressive and agile network defense.

Each of these elements complements the efforts of the others. USCYBERCOM has recently employed CMF teams in real-world operations responding to intrusions in DoD systems and the networks of other federal entities. Cyber Protection Teams, for instance, played an important role in defending the Joint Staff's unclassified systems after an intrusion last summer, and in remediating the vulnerabilities that the intruders had utilized.

Training the force for such missions is imperative. Teams must learn to operate against live opposition, even on degraded networks. Our commanders and seniors must develop an understanding of how cyber operations unfold so they know what to expect and what can be achieved. USCYBERCOM's annual CYBER GUARD exercise provides a realistic training environment in which federal, state, industry, and international partners can use their skills against a wily opposition force. Each June CYBER GUARD has become bigger, more comprehensive, and more complex. Last year USCYBERCOM supported the planning and execution with co-sponsorship from DHS and FBI. We create a notional network for each CYBER GUARD to allow our teams to respond to an attack against the power grid in partnership with the power companies; indeed, we even developed a simulated internal network like that in a large utility. The response to CYBER GUARD from our public and private partners has been tremendous. Dozens of critical infrastructure companies have expressed interest in participating in CYBER GUARD exercises; indeed, we might even have more interest than we have room to include all the companies that want to participate. Exercises like CYBER GUARD allow senior policymakers to observe the types of issues seen in real cyberattacks, and helps us generate a "playbook" that should save the federal government precious time and stress in crafting its response.

Conclusion

Chairman Fischer, Ranking Member Nelson, and Members of the subcommittee, thank you again for inviting me to appear before you today. USCYBERCOM supports the implementation of the DoD Cyber Strategy in a "total force" manner and is devoting particular efforts to the security of DoD's information systems, beginning with directing the defense of the

DoDIN but extending, as appropriate, to the protection of industrial control systems and networks for U.S. military forces and installations, and when directed, to support civil authorities in defense of the nation's critical infrastructure. The growing Cyber Mission Force is adding to our capacity to perform this mission, and we are taking advantage of the increasing opportunities to pursue this goal by partnering with federal, state, local, industry, academic, and foreign partners in an expanding range of training and operational contexts. I now look forward to your questions.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu