Prepared Statement of GEN (Ret) Keith B. Alexander*
on Cyber Strategy and Policy before the
Senate Armed Services Committee

March 2, 2017

Chairman McCain, Ranking Member Reed, Members of the Committee: thank you for inviting me to discuss cyber strategy and policy with you today, and specifically for asking this panel to engage in a dialogue with this Committee about how we might provide for the common defense of the nation in cyberspace. I plan to speak candidly about these issues, including the current organizational construct for cybersecurity within the federal government, the need for joint cyber defense capabilities and operations between the public and private sector, and the insights and recommendations of the Commission for Enhancing National Cybersecurity, of which I was a member.

Before I begin my testimony, I want to note the leadership, Mr. Chairman, that you and the Ranking Member are demonstrating by taking the time to look at how we might architect the federal government to deal with the reality of the threats that our nation faces in this rapidly-evolving, technology-driven, highly-networked global environment. The series of hearings focused on the future of warfare, global cyber threats, and cyber strategy and policy that you and the Ranking Member continue to chair will help ensure the security of our nation and allies for many decades going forward.

Mr. Chairman, we must fundamentally rethink our nation's architecture for cyber defense. We must recast the way we think of the respective roles and responsibilities of the government and private entities, bringing a new jointness to our work in cyber defense. And we must develop a cadre of trained professionals that provides the public and private sectors a collective technical edge.

Overall, Mr. Chairman, I am concerned that as a nation, we have not made the key decisions necessary to put in place the foundational capabilities, provide the right authorities, and assign the critical responsibilities that are necessary to properly protect our nation in this new domain. I believe the cybersecurity Executive Order will be a key step in addressing some of these issues. In addition, I think it is critical that Congress, the White House, and the private sector work closely together to address the critical gaps that we face today.

* GEN (Ret) Keith Alexander is the former Commander, United States Cyber Command and Director, National Security Agency. Currently, he is the President and CEO of IronNet Cybersecurity and recently completed service as a member of the President's Commission on Enhancing National Cybersecurity.

For over 200 years, our Constitution has made clear that one of the core goals of the federal government is to provide "for the common defense."[1] Today, that common defense and the needed partnership between public and private sector is clearly lacking.

During my almost 40 years of service, it was an honor and privilege to work side-by-side with those who worked tirelessly to defend our nation. We worked hard to put in place the capabilities and to build the forces and structures needed to provide for the physical defense of our nation—both within our borders and abroad—and to do the same in cyberspace. Within the Department of Defense (DOD) alone, we fundamentally re-architected the way that the National Security Agency operated and created a key component of our nation's cyber defense, the U.S. Cyber Command.

In 2012, then-Secretary of Defense Leon Panetta made clear that the policy of the U.S. government was that "the Department [of Defense] has a responsibility not only to defend DOD's networks, but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace."[2] At that time, it was clear that in order to make our overall national cyber architecture truly defensible, we needed to establish a shared understanding of our respective roles and responsibilities, first within the government, then between the government and the private sector.

Initially, we worked closely with our colleagues in other agencies across the government to put in place a workable structure for sharing authorities and assigning responsibilities at the national level. Indeed, by one count, it took 75 drafts to obtain an agreement on a *single slide* regarding the national division of responsibilities for cybersecurity.[3]

At the end of that process, we assigned the responsibilities as follows: The Justice Department would, among other things, "[i]nvestigate, attribute, disrupt, and prosecute cyber crimes; [l]ead domestic national security operations; [and] [c]onduct domestic collection, analysis, and dissemination of cyber threat intelligence;" Department of Homeland Security (DHS) would, among other things "[c]oordinate the national protection, prevention, mitigation of, and recovery from cyber incidents; [d]isseminate domestic cyber threat and vulnerability analysis; [and] [p]rotect critical infrastructure;" and DOD would "[d]efend the nation from

---

[1] U.S. Const., preamble (emphasis added).

[2] *See* Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City* (Oct. 11, 2012), available online at <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> .

[3] *See* Department of Defense Information Operations Center for Research and Army Reserve Cyber Operations Group, *Cyber Endeavor 2014: Final Report – When the Lights Go Out*, at 5 (June 26, 2014), available online at <https://my.nps.edu/documents/105372694/0/Cyber Endeavour 2014 - Final Report - 2014-08-13.pdf> ("The need to define these partnerships and relationships [] led the Government and U.S. Federal Cybersecurity Operations Team to define their national roles and relationships as highlighted in Figure 1, which is commonly referred to as the 'Bubble Chart.' There were seventy-five (75) versions made of this chart before all parties agreed on how this works, and it was powerful and important just to get an agreement.")

attack; [g]ather foreign threat intelligence and determine attribution; [and] [s]ecure national security and military systems."[4] Moreover, the "bubble chart," as this document was called, assigned the following lead roles: DOJ: investigation and enforcement; DHS: protection; and DOD: national defense.[5]

The position that DOD has the lead for national defense in cyberspace has been reiterated in both the 2014 Quadrennial Defense Review as well as the 2015 DoD Cyber Strategy, the latter of which also highlights the critical role that private sector entities must take in protecting themselves against threats in cyberspace.[6] While it may be clear that as a policy matter that DOD has the responsibility for defending the nation from nation-state attacks, the reality is that today U.S. Cyber Command lacks the clear authorities and rules of engagement to make this policy effective, even though it continues to build the forces and capabilities necessary to do so. It is critical that we work together, as a nation, to provide these authorities and rules of engagement now, when things are relatively calm, rather than seeking to identify and create them during a crisis. Mr. Chairman, I know that you and the Ranking Member have both taken the lead on working this effort, and I stand ready to assist you as needed.

While the primary responsibility of government is to defend the nation, the private sector also shares responsibility in creating the partnership necessary to make the defense of our nation possible. Neither the government nor the private sector can capably protect their systems and networks without extensive and close cooperation. The private sector controls most of the real estate in cyberspace, particularly when it comes to critical infrastructure and key resources,[7] and

---

[4] *See id.* at 6, Fig. 1.

[5] *See id*.

[6] *See* Department of Defense, *2014 Quadrennial Defense Review* at 14-15, available online at <http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf> ("The Department of Defense will deter, and when approved by the President and directed by the Secretary of Defense, will disrupt and deny adversary cyberspace operations that threaten U.S. interests. To do so, we must be able to defend the integrity of our own networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital U.S. interests."); Department of Defense, *2015 Department of Defense Cyber Strategy* at 5 (Apr. 15, 2015), available online at <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> ("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 purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life….As a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the U.S. homeland or U.S. interests before conducting a cyberspace operation. The United States government has a limited and specific role to play in defending the nation against cyberattacks of significant consequence. The private sector owns and operates over ninety percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense. One of the most important steps for improving the United States' overall cybersecurity posture is for companies to prioritize the networks and data that they must protect and to invest in improving their own cybersecurity. While the U.S. government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves.")

[7] *See, e.g.*, Office of the Director of National Intelligence, Office of the Program Manager-Information Sharing Environment, *Critical Infrastructure and Key Resources*, available online at <https://www.ise.gov/mission-

the notion that government might have control over, or even a constant, active defensive presence on these private systems and networks, is simply not something that our nation seeks today. Thus, given our current cyber architecture, if we are to create a truly defensible cyber environment, the government and the private sector must work closely together.

Consequently, the most important thing the government can do is to build connectivity and interoperability with the private sector. This is not simply connectivity and interoperability on a technology level, but on a policy and governance level. To that end, the Commission recommended the creation of a National Cybersecurity Public-Private Partnership (NCP^3).[8] This entity, as set forth in Commission's report, would serve the President directly, reporting through the National Security Advisor and would function as "a forum for addressing cybersecurity issues through a high-level, joint public–private collaboration."[9] Part of the NCP^3's key function would be to "identify clear roles and responsibilities for the private and public sectors in defending the nation in cyberspace," including addressing critical issues like "attribution, sharing of classified information…[and] an approach—including recommendations on the authorities and rules of engagement needed—to enable cooperative efforts between the government and private sector to protect the nation, including cooperative operations, training, and exercises."

In line with this recommendation, the Commission also recommended that "[t]he private sector and Administration [] launch a joint cybersecurity operation program for the public and private sectors to collaborate on cybersecurity activities in order to identify, protect from, detect, respond to, and recover from cyber incidents affecting critical infrastructure."[10] Empowering such joint efforts is critical to ensuring our long-term national security in cyberspace. As the Commission indicated, "[k]ey aspects of any collaborative defensive effort between the government and private sector [will] include coordinated protection and detection approaches to ensure resilience; fully integrated response, recovery, and plans; a series of annual cooperative training programs and exercises coordinated with key agencies and industry; and the development of interoperable systems."[11] Having such mechanisms in place well ahead of crisis is critical so that public and private sector entities can jointly train and exercise these rules of engagement and mitigate any potential spillover effects on ongoing business or government activities. Implementing these two Commission recommendations are amongst the most important things we might do as a nation in the near-term.

Finally, it is critical that the collaboration between the government and private sector is a two-way partnership. The government can and must do more when it comes to partnering with

---

partners/critical-infrastructure-and-key-resources> ("The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation's physical and economic security.").

[8] *Id*. at 14 (action item 1.2.1)

[9] *Id*. at 14-15.

[10] *Id*. at 15 (action item 1.2.2.)

[11] *Id*.

the private sector, building trust, and sharing threat information—yes, even highly classified threat information—at network speed and in a form that can be actioned rapidly. Building out a cross-cutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to the air traffic control picture. As the air traffic control picture ensures our aviation safety and synchronizes government and civil aviation, the cyber common operational picture can be used to synchronize a common cyber defense for our nation, drive decision-making, and enable rapid response across our entire national cyber infrastructure. This would provide a critical defensive capability for the nation.

The cyber legislation enacted by Congress last year is a step in the right direction; however, it lacks key features to truly encourage robust sharing, including placing overbearing requirements on the private sector, overly limiting liability protections, restricting how information might effectively be shared with the government, and keeping the specter of potential government regulation looming in the background.[12] Moreover, while the government has placed this responsibility with DHS today,[13] it is important to recognize the perception in industry is that DHS faces significant challenges in this area, in particular that it simply lacks the technical capabilities necessary to succeed.[14] More can be done here, and I stand ready to work with this Committee and others in Congress and the Administration as we seek a path forward on this important issue. As with the recommendations of the Commission above, I believe that implementing robust, real-time threat information sharing across the private sector and with the government would be a game-changer when it comes to cyber defense.

In sum, Mr. Chairman, I think much remains to be done to fully put our nation on a path to real security in cyberspace, and I am strongly hopeful for our future. With your leadership and that of the Ranking Member, working together collaboratively across the aisle and with the White House and key players in the private sector, we can achieve real successes in securing our nation in cyberspace.

Thank you for the opportunity to appear before this committee.

---

[12] *See, e.g.*, Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, __ S. Car. L. Rev. __ (forthcoming 2017).

[13] *See, e.g.*, Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (Feb. 13, 2015), available online at <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari> ("The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002…shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents.").

[14] *See* Commission on Enhancing National Cybersecurity, *Testimony of Greg Rattray*, Director of Global Cyber Partnerships & Government Strategy, J.P. Morgan Chase (May 16, 2016) (describing DHS's six information sharing initiatives, as "too broad and [simply] not meet[ing] the need[] to enhance cyber defense"); *Testimony of Mark Gordon*, n. 13 *supra* (arguing that while tactically accelerating automating and systemizing threat indicator content with the government is a big vision, it is not a reality today); *see also* Jaffer, n. 14 *supra*, at __ ("DHS is generally seen as facing major challenges in capability in the cyber area and a number of other agencies, from DOD/NSA to FBI, are seen by industry as more capable, reliable, or secure.").