FACT SHEET: THE DEPARTMENT OF DEFENSE (DOD) CYBER STRATEGY

APRIL 2015

An engine of innovation and communication, the Internet connects billions of people, helps deliver goods and services globally, and brings ideas and knowledge to those who would otherwise lack access. The United States relies on the Internet and the systems and data of cyberspace for a wide range of critical services. This reliance leaves us vulnerable in the face of a real and dangerous cyber threat, as state and non-state actors plan to conduct disruptive and destructive cyberattacks on the networks of our critical infrastructure and steal U.S. intellectual property to undercut our technological and military advantage.

The purpose of the new *Department of Defense Cyber Strategy*, the Department's second, is to guide the development of DoD's cyber forces and strengthen its cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DoD's **three cyber missions: defend DoD networks, systems, and information; defend the United States and its interests against cyberattacks of significant consequence; and provide integrated cyber capabilities to support military operations and contingency plans.** The strategy sets five strategic goals and establishes specific objectives for DoD to achieve over the next five years and beyond.

What drove DoD to develop a new cyber strategy? Three major drivers required that DoD develop a new cyber strategy. First is the increasing severity and sophistication of the cyber threat to U.S. interests, to include DoD networks, information, and systems. The Department of Defense has the largest network in the world and DoD must take aggressive steps to defend its networks, secure its data, and mitigate risks to DoD missions. Second, in 2012 President Obama directed DoD to organize and plan to defend the nation against cyberattacks of significant consequence, in concert with other U.S. government agencies. This new mission required new strategic thinking. Finally, in response to the threat, in 2012 DoD began to build a Cyber Mission Force (CMF) to carry out DoD's cyber missions. The CMF will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components. The strategy provides clear guidance for the CMF's development.

Building bridges to the private sector and beyond. To build the force of the future, DoD must attract the best talent, the best ideas, and the best technology to public service. To do so, DoD must build strong bridges to the private sector as well as the research institutions that make the United States such an innovative nation. The private sector and America's research institutions design and build the networks of cyberspace, provide cybersecurity services, and research and develop advanced capabilities. The Department of Defense has had a strong partnership with the private sector and these research institutions historically, and DoD will strengthen those historic ties to discover and validate new ideas for cybersecurity for DoD and for the country as a whole.

Deterrence is a key part of DoD's new cyber strategy. This strategy describes the Department of Defense contributions to a broader national set of capabilities to deter adversaries from conducting cyberattacks. The Department of Defense assumes that the deterrence of cyberattacks on U.S. interests will be achieved through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. DoD has a number of specific roles to play in this equation; this strategy describes how DoD will fulfill its deterrence responsibilities effectively.

STRATEGIC GOALS AND KEY IMPLEMENTATION OBJECTIVES:

I. BUILD AND MAINTAIN READY FORCES AND CAPABILITIES TO CONDUCT CYBERSPACE OPERATIONS. In 2013, DoD initiated a major investment in its cyber personnel and technologies for the Cyber Mission Force. The Department of Defense must train its people, build effective organizations and command and control

systems, and fully develop the capabilities that DoD requires to operate in cyberspace. Key objectives of this goal include:

- Build technical capabilities for operations, to include a unified and integrated operational platform.
- Accelerate research and development to provide DoD with a significant advantage in developing leap-ahead technologies to defend U.S. interests in cyberspace.
- Assess CMF capacity to achieve mission objectives when confronted with multiple contingencies.

II. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions. DoD must identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively. DoD must also plan and exercise to operate within a degraded and disrupted cyber environment in the event that an attack on DoD's networks and data succeeds, or if aspects of the critical infrastructure on which DoD relies for its operational and contingency plans are disrupted. Key objectives of this goal include:

- Build the Joint Information Environment single security architecture to shift the focus from protecting service-specific networks and systems to securing the DoD enterprise.
- Implement a capability to mitigate all known vulnerabilities that present a high risk to DoD.
- Identify, plan, and defend the networks that support key DoD missions.
- Build a layered defense around the Defense Industrial Base through improved accountability, cybersecurity standards, counterintelligence, and whole of government efforts to counter IP theft.

III. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence. The Department of Defense must work with its interagency partners, the private sector, and allied and partner nations to deter and if necessary defeat cyberattacks of significant consequence on the U.S. homeland and U.S. interests. The Department of Defense must develop its intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyberattacks. Key objectives of this goal include:

- Develop intelligence and warning capabilities to anticipate threats.
- Partner with key interagency organizations to prepare to defend the nation in cyberspace.
- Work with DHS to develop continuous and automated mechanisms for sharing information.
- Assess DoD's cyber deterrence posture and provide recommendations for improving it.

IV. 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. During heightened tensions or outright hostilities, DoD must be able to provide the President with a wide range of options for managing conflict escalation. As a part of the range of tools available to the United States, DoD must develop viable cyber options and integrate those options into Departmental plans. DoD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property.

V. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability. All three of DoD's cyber missions require close collaboration with foreign allies and partners. In its international cyber engagement, DoD seeks to build partnership capacity in cybersecurity and cyber defense.

- Partner capacity building will focus on priority regions, to include the Middle East, Asia-Pacific, and Europe. DoD will remain adaptive and flexible to build new alliances and partnerships as required.