STATEMENT FOR THE RECORD OF

THE HONORABLE MARCEL LETTRE

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

OFFICE OF THE SECRETARY OF DEFENSE

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

13 SEPTEMBER 2016

INTRODUCTION

Chairman McCain, Ranking Member Reed, and Members of the Committee, thank you for inviting us to discuss the importance of strong encryption, trends on its use, and its effects on the Department of Defense (DoD). It is an honor to appear before you today and we appreciate the opportunity to explain both the importance of encryption to secure data and to protect systems vital to our national defense, as well as the impact that the continuing adoption of strong encryption has on the execution of our national security missions. The use of strong encryption is a vital component to protect our warfighting capabilities and ensures our national security interests remain secure.

IMPORTANCE OF STRONG ENCRYPTION

The Department supports the use of strong encryption. Commercial encryption technology is vital to U.S. competitiveness and economic security and the Department depends upon secure data and strong encryption technology to carry out our national security mission. DoD depends upon our commercial-sector partners to help protect national security systems, research and development data related to our weapons systems, classified and sensitive information, service members' personally identifiable information and health records, just to name a few examples. The National Security Agency (NSA), which is responsible for setting encryption standards within the Department of Defense, depends upon strong and voluntary commercial industry partnerships to protect these systems and to develop best practices on the implementation and integration of encryption.

If our adversaries are able to gain access to our networks, weapons systems, and other critical infrastructure, they could manipulate information, destroy data, and harm our national

security systems. We must stay ahead of our adversaries' capabilities to ensure that our systems remain protected. Strong encryption remains a vital element to do so.

ENCRYPTION CHALLENGES

The threat landscape continues to change. The widespread availability of strong encryption has also allowed terrorist groups, such as the Islamic State of Iraq and the Levant (ISIL), to leverage such technology for its operations. ISIL uses the internet and mobile applications to securely communicate and recruit fighters, further incite violence, and inspire, plan, and conduct attacks against its enemies, including our forces. As terrorist groups become more sophisticated and technologically savvy, encryption presents a challenge for the Department, especially NSA, to acquire needed intelligence if communications cannot be decrypted. This challenge will compound as industry moves towards implementation of encryption that they are incapable of unencrypting as they will no longer hold the decryption keys enabling them to provide access to the content of communications.

While the Department benefits from strong encryption, malicious actors use the accessibility of strong encryption and other technologies to thwart DoD efforts in a variety of areas. This presents a unique challenge for government, one that requires the nation to determine how to balance individual privacy, a fundamental tenet in our democracy, with the need to protect our citizens from those who would do harm. As we have seen with ISIL, terrorists are increasingly using strong encryption to hide the content of their communications. This challenges the ability of the Department to understand our adversaries' intent, terrorist networks, financing streams, tactics, attack planning and execution, in the United States and abroad.

ENCRYPTION WAY AHEAD

We need to strengthen our partnership with industry to find ways to protect against the national security threats to the United States. We will continue to work closely with our industry partners to find innovative ways to outmaneuver malicious actors' adoption of strong encryption, while ensuring that individual privacy interests are protected. I believe any steps we take as a government must be carefully considered to avoid introducing unintentional weaknesses in the protection of our commercial networks and national security systems. We should also be careful not to negatively affect our economic competitiveness as a world leader in technology, which could unintentionally drive technology innovation outside the United States.

CONCLUSION

The Department is committed to the security and resiliency of our data and networks and for defending the U.S. interests at home and abroad. Our relationship with Congress as well as other Departments, Agencies, and industry is absolutely critical as we work together to navigate the encryption challenge. I am grateful for the committee's interest in these issues, and I look forward to your questions.