



September 13, 2016

# Encryption and Cyber Matters

Committee on Armed Services, United States Senate, One Hundred  
Fourteenth Congress, Second Session

---

## HEARING CONTENTS:

### Witnesses

Marcell J. Lettre II  
Under Secretary of Defense for Intelligence  
[\[View Testimony\]](#)

Admiral Michael S. Rogers  
Commander, United States Cyber Command / Director, National Security  
Agency / Chief, Central Security Services  
United States Navy  
[\[View Testimony\]](#)

### Available Webcast(s)\*:

[\[Watch Full Hearing\]](#)

### Compiled From\*:

<https://www.armed-services.senate.gov/hearings/16-09-13-encryption-and-cyber-matters>

*\* Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

---

*This hearing compilation was prepared by the Homeland Security Digital Library,  
Naval Postgraduate School, Center for Homeland Defense and Security.*

---

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.

**Testimony of  
Admiral Michael S. Rogers, USN  
Commander, U.S. Cyber Command  
Director, National Security Agency  
before the  
Senate Armed Services Committee  
13 September 2016**

Chairman McCain, Ranking Member Reed, and Members of the Committee, thank you for inviting me. It is a distinct honor and privilege to appear before you today. I appreciate this opportunity to speak to you about the current communications environment, including the wide availability of strong encryption, and its impact on the National Security Agency as we conduct our foreign intelligence and information assurance missions. When we last met on 12 July, I outlined several of these challenges to the Committee, and today I look forward to discussing those challenges so that the American people are provided the greatest amount of information possible on this topic.

When I use the term encryption, I am referring to a means to protect data from any access except by those who are intended or authorized to have it. Encryption is usually accomplished by combining random data with the data you want to protect. The random data is generated by mathematical algorithm and uses secret information – called a key – in the generation. Without the key, you cannot unlock the encryption, and access the data.

First and foremost, you should know that NSA supports the use of encryption. Encryption is fundamental to the protection of everyone's data as it travels across the global network. NSA, through its Information Assurance mission, sets the standards for the use of encryption within the Department of Defense. We understand encryption, rely on it ourselves, and set the standards for others in the government to use it properly to protect national security systems. At the same time,

encryption presents an ever-increasing challenge to our foreign intelligence mission. The easy availability of strong encryption by those who wish to harm our citizens, our government, and our allies is a threat to national security.

As you well know, the threat environment – both in cyberspace and in the physical world – is constantly evolving, and we must keep pace in order to provide our policy makers and war fighters the foreign intelligence they need to keep us safe. Terrorists’ tactics, techniques, and procedures continue to evolve. Those who would seek to harm us use the same Internet, the same mobile communications devices, and the same social media platforms that law-abiding citizens around the world use. The trend is clear, terrorists are becoming more savvy about protecting their communications – including through the use of strong encryption.

NSA has not stood still in response to this changing landscape. We are making investments in technologies and capabilities designed to help us address this challenge and last year, we started a process to better position NSA to face these challenges. It’s premised on the idea – that as good as NSA is at its foreign intelligence and its information assurance missions, the world will continue to change. The goal is therefore to change as well in order to ensure we will be as effective tomorrow as we are today. The nation counts on NSA to generate insights into what is happening in the world around us, what should be of concern to our nation’s security, the safety and well-being of our citizens, and of our friends and allies. We asked ourselves: how do we continue to generate the same level of information assurance or foreign intelligence or computer network defense insight given these changes? We see technology fundamentally changing – the proliferation of strong encryption across the Internet and mobile devices is just one part of that change.

I told my team that I wanted us to think about what 2025 will look like and how we can better position NSA for that future. We call this effort NSA in the 21<sup>st</sup> Century, or NSA21. As we look out to 2025, we see technology fundamentally changing in a variety of ways. Encryption tends to be getting a lot of attention at the moment, but the nature of technology's change is so much broader than that. It's encryption. It's the Internet of Things. It's the increased interconnectivity that is being built into every facet of our lives.

We have a challenge before us. We're watching sophisticated adversaries change their communication profiles in ways that enable them to hide information relating to their involvement in things such as criminal behavior, terrorist planning, malicious cyber intrusions, and even cyber attacks. Right now technology enables them to communicate in a way that is increasingly problematic for NSA to acquire critical foreign intelligence needed to protect the nation or for law enforcement officers to defend our nation from criminal activity.

The question then becomes, so what's the best way to deal with that? Encryption is foundational to the future. And anyone who thinks we are just going to walk away from that, I think, is totally unrealistic. The challenge becomes, given the premise that encryption is foundational to the future, what's the best way for us to ensure the protection of information, the privacy and civil liberties of our citizens, and the production of the foreign intelligence necessary to ensure their protection and safety? All three are incredibly important to us as a nation.

Thank you. I look forward to your questions.