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 21st 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.