

## IC ON THE RECORD



**Remarks as delivered by General Keith Alexander, Director of the National Security Agency**

*Open Hearing on Foreign Intelligence Surveillance Authorities, U. S. Senate Select Committee on Intelligence*

*Thursday, September 26, 2013*

*216 Hart Senate Office Building, Capitol, Washington DC*

Chairman Feinstein, Vice Chairman Chambliss, distinguished members of the committee, I am privileged today to represent the work of the dedicated professionals at the National Security Agency, who employ the authorities provided by Congress, the courts and the executive branch to help defend this nation. If we are to have a serious debate about how NSA conducts its business, we need to step away from sensational headlines and focus on the facts.

Today, I'd like to present facts about four key areas: who we are in terms of both our mission and our people; what we do — adapt to technology and the threat, take direction from political leadership, use lawful programs, tools, and ensure compliance; I'd like to cover what we have accomplished for our country with the tools we have been authorized; and where do we go from here.

First, who we are and our mission: NSA is a foreign intelligence agency with two missions. We collect foreign intelligence of national security interests and we protect certain sensitive information in U.S. networks. NSA contributes to the security of our nations, its armed forces and our allies. NSA accomplishes this mission while protecting civil liberties and privacy. NSA operates squarely within the authorities granted by the president, Congress and the courts.

Who we are, our people: I am proud of what NSA does and even more proud of these great Americans and what they do for this nation. The National Security Agency employees take an oath to protect and defend the Constitution of the United States against all enemies, foreign and domestic. They have devoted themselves to defending this nation. Just like you, they will never forget the moment terrorists killed 2,996 Americans in New York, Pennsylvania and the Pentagon. They witnessed the first responders, and I'll tell you, that's one of the things that has been in the front of the NSA lobby for the past 10 years, is a picture of those first responders holding the American flag and passing it off to our military, and the military and the intelligence community saying, we've got it; we'll take it from here. That's what we've done.

In fact, NSA employees deployed with our armed forces into areas of hostility. More than 6,000 NSA personnel have supported — have deployed in support of forces in Iraq and Afghanistan, and 22 cryptologists paid the ultimate sacrifice. Theirs is a noble cause; they are the true heroes.

NSA prides itself on its highly skilled workforce. We are the largest employer of mathematicians in the United States. We have 1,013 mathematicians, 966 Ph.Ds and 4,374 computer scientists. We have linguists in more than 120 languages. We have more patents than any other intelligence committee agency and most businesses. They are also Americans and they take their privacy and civil liberties seriously.

What we do; how we adapt to technology: Today's telecommunications system is literally one of the most complex systems ever devised by mankind.

Terrorists and other foreign adversaries hide in the global networks, use the same communications networks as everyone else and take advantage of familiar services — Gmail, Facebook, Twitter. Technology has made it easy for them. We must develop and apply the best analytic tools to succeed at our mission.

What we do — we take guidance from our political leadership, the National Intelligence Priorities Framework. NSA's direction comes from national security needs, as defined by the nation's senior leaders. NSA does not decide what topics to collect and analyze. NSA's collection and analysis is driven by the National Intelligence Priorities Framework and received in formal tasking. We do understand that electronic surveillance capabilities are powerful tools in the hands of the state. That's why we have extensive mandatory internal training, automated checks and an extensive regime of both internal and external oversight.

What we do — we use lawful programs and tools to do our mission. The authorities we have been granted and the capabilities we have developed help keep our nation safe. Since 9/11 we have disrupted terrorists attacks at home and abroad using capabilities informed by the lessons of 9/11.

The business record FISA program, NSA's implementation of Section 215 of the Patriot Act, focuses on defending the homeland by linking foreign and domestic threats. Section 702 of FISA focuses on acquiring foreign intelligence, including critical information concerning international terrorist organizations by targeting non-U.S. persons who are reasonably believed to be outside of the United States. NSA also operates under other sections of the FISA statute, in accordance with the law's provisions.

It is important to remember that in order to target a U.S. person anywhere in the world, under the FISA statute, we are required to obtain a court order based on a probable cause showing that the prospective target of the surveillance is a foreign power or agent of a foreign power.

NSA conducts the majority of its SIGINT authorities — activities solely pursuant to the authority provided by Executive Order 12333. As I have said before, these authorities and capabilities are powerful. We take our responsibility seriously.

What we do: We ensure compliance. We stood up a directorate of compliance in 2009 and repeatedly trained our entire workforce and privacy protections and the proper use of capabilities. We do make mistakes. The vast majority of incidents reflect the challenge, very specific rules in the context of ever-changing technology. Compliance incidents, with very rare exception, are unintentional and reflect the sorts of errors that will occur in any complex system of technical activity.

The press claimed evidence of thousands of privacy violations. This is false and misleading. According to NSA's independent inspector general, there have been only 12 substantiated cases of willful violation over 10 years — essentially one per year. Several of these cases were referred to the Department of Justice for potential prosecution, appropriate discipline action in other cases. We hold ourselves accountable very day.

Most of these cases involved improper tasking or querying regarding foreign persons in foreign places. To repeat, I am not aware of any intentional or willful violations of the FISA statute, which is designed to be most protective of the privacy interests of U.S. persons.

Of the 2,776 violations noted in the press, about 75 percent are not violations of court-approved procedures at all but rather NSA's detection of valid foreign targets to travel to the United States and a record that NSA stopped collecting in accordance with the rules. We call those roamers. I do mention them, chairman. Yes, I pronounced that — I had dental surgery; I pronounced that "roamers"; it came out "rumors." It's "roamers" — R-O-A-M-E-R.

And those are just as you stated. These are not compliance incidents.

The court asked us to track those and report those so that we can show when they do come in the country that we shut down the collection exactly as we're supposed to, right away. Two thousand sixty five of those 2,776 were, in fact, roamers.

Let me also start to clear to air on actual compliance incidents. The vast majority of the actual compliance incidents involve foreign locations and foreign activities as our activities are regulated by specific rules wherever they occur. And I think that's important to note, just as a sidebar, that we hold ourselves to the same standard overseas in terms of compliance.

This system can't be used willfully or incorrectly by anyone. We hold them accountable. So where it says we're sweeping up the communications of civilians overseas that aren't targets of collection systems, it is wrong. If our folks do that, we hold them accountable. NSA detects and corrects and, in many cases, does so before any information is even obtained, used or shared outside the United States.

And I want to go back and just hit a key point. For the small number that does include a U.S. person, a typical incident involves a person overseas involved with a foreign organization who is subsequently determined to be a U.S. person. The majority of our incidents that we report are U.S. persons that were overseas that we didn't know was a U.S. person. We still call that a compliance incident. We correct it. We delete the data.

Despite the difference between willful and not, we treat incidents the same. We detect, we address, we remediate, include removing information from our databases in accordance with the rules, and finally we report to Congress, to the courts and to the administration. We hold ourselves accountable and keep others informed so they can do the same.

Today NSA has a privacy compliance program any leader of a large, complex organization would be proud of. We welcome an ongoing discussion about how the public can, going forward, have increased information about NSA's compliance program and its compliance posture, much the same way all three branches of the government have today.

What we have accomplished in our country: NSA's existing authorities and programs have helped connect the dots, working with the broader intelligence community and homeland and domestic security organizations for the good of the nation and our people. NSA's programs have contributed to understanding and disrupting 54 terror-related events — 25 in Europe, 11 in Asia and five in Africa and 13 in the United States.

This was no accident. This was not coincidence. These are the direct results of a dedicated workforce, appropriate policy and well-sculpted authorities created in the wake of 9/11 to make sure 9/11 never happens again. In the week ending 23 September, there were 972 terror-related deaths in Kenya, Pakistan, Afghanistan, Syria, Yemen and Iraq. Another 1,030 people were injured in the same countries.

The programs that I've been talking about, we need these programs to protect this nation to ensure we don't have those same statistics here. NSA's global system is optimized for today's technology on a global network. Our analytic tools are effective at finding terrorist communication in time to make a difference. This global system and analytic tools are also what we need for cybersecurity. This is how we see in cyberspace, identify threats there and defend networks.

With respect to reforms, on 9 August the president laid out some specific steps to increase the confidence of the American people in our foreign intelligence collection programs. We are always looking for ways to better protect privacy and security. We have improved over time our ability to reconcile our technology with our operations and with the rules and authorities. We will continue to do so as we go forward and strive to improve how we protect the American people, their privacy and their security.

Regarding NSA's telephone metadata program, policymakers across the executive and legislative branches will ultimately decide whether we want to sustain or dispense with a tool designed to detect terrorist plots (across the scene ?) before foreign and domestic domains. Different implementations of the program can address the need, but each should be scored against several key attributes.

Privacy: Privacy and civil liberties much be protected. Agility: Queries can be made in a timely manner so that in the most urgent cases, results can support disruption of imminent terrorist attacks. Duration: Terrorist planning can extend for years, so the metadata repository must extend back for some period of time in order to discover terrorist plots and their plans. The breadth: The repository of metadata is comprehensive enough to ensure query responses can indicate with high confidence any connections a terrorist-associated number may have to other persons who are engaged in terrorist activities.

As you consider changes in metadata storage location, length of storage, who approves the query terms and the number of hops, we must preserve these foundational attributes of the BR FISA program. Similarly, as you entertain reforms to the FISA Court, operational and practical considerations must be weighed so that there are no inherent delays, emergency provisions are maintained, and any reform to the FISA structure is respectful to the nature of classified information.

In conclusion, NSA looks forward to supporting the discussion of reforms. Whatever changes are made, we will exercise our authorities dutifully, just as we have always done. The leaks of classified NSA and partner information will change how we operate and what people know about us; however, the leaks will not change the ethos of the NSA workforce, which is dedicated to finding and reporting the vital intelligence our customers need to keep the nation safe in a manner that is fully compliant with the laws and rules that authorize and limit NSA's activities and vindicate the privacy protections that we as a nation enjoy.

I look forward to answering your questions.

- [#Testimony](#)
- [#Keith Alexander](#)
- [#NSA](#)
- [#Section 702](#)
- [#Section 215](#)
- [#FISA](#)
- [#FISC](#)
- [15 hours ago](#)
- [4](#)
- [Permalink](#)

Share

Short URL

<http://tumblr.co/ZZQjsqw>

[Twitter](#)[Facebook](#)[Pinterest](#)[Google+](#)

**4 Notes/** [Show](#)

[← Previous](#) • [Next →](#)

**About**

Created at the direction of the President of the United States, [IC ON THE RECORD](#) provides immediate, ongoing and direct access to factual information related to the lawful foreign surveillance activities carried out by the U.S. Intelligence Community.

Follow [@IConTheRecord](#)

---

#### CONTENT CATEGORIES:

- - [Official Statements](#)
- - [Declassified Documents](#)
- - [Testimony](#)
- - [Speeches & Interviews](#)
- - [Fact Sheets](#)
- - [Oversight & Compliance](#)
- - [Video](#)

---

#### HOT TOPICS:

- - [Civil Liberties](#)
- - [FISA](#)
- - [FISC](#)
- - [Section 215](#)
- - [Section 702](#)

---

#### IN THEIR OWN WORDS:

- - [James Clapper, DNI](#)
- - [Keith Alexander, Dir. NSA](#)
- - [Robert Litt, GC, ODNI](#)
- - [John Inglis, Dep. Dir., NSA](#)
- - [Alex Joel, CLPO, ODNI](#)

Search this site



This website is maintained by the [Office of the Director of National Intelligence](#).