



9 August 2013

National Security Agency

The National Security Agency: Missions, Authorities, Oversight and Partnerships

“That’s why, in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communication, but also build in privacy protections to prevent abuse.”

--President Obama, May 23, 2013

In his May 2013 address at the National Defense University, the President made clear that we, as a Government, need to review the surveillance authorities used by our law enforcement and intelligence community professionals so that we can collect information needed to keep us safe and ensure that we are undertaking the right kinds of privacy protections to prevent abuse. In the wake of recent unauthorized disclosures about some of our key intelligence collection programs, President Obama has directed that as much information as possible be made public, while mindful of the need to protect sources, methods and national security. Acting under that guidance, the Administration has provided enhanced transparency on, and engaged in robust public discussion about, key intelligence collection programs undertaken by the National Security Agency (NSA). This is important not only to foster the kind of debate the President has called for, but to correct inaccuracies that have appeared in the media and elsewhere. This document is a step in that process, and is aimed at providing a succinct description of NSA’s mission, authorities, oversight and partnerships.

Prologue

After the al-Qa’ida attacks on the World Trade Center and the Pentagon, the 9/11 Commission found that the U.S. Government had failed to identify and connect the many “dots” of information that would have uncovered the planning and preparation for those attacks. We now know that 9/11 hijacker Khalid al-Midhar, who was on board American Airlines flight 77 that crashed into the Pentagon, resided in California for the first six months of 2000. While NSA had intercepted some of Midhar’s conversations with persons in an al-Qa’ida safe house in Yemen during that period, NSA did not have the U.S. phone number or any indication that the phone Midhar was using was located in San Diego. NSA did not have the tools or the database to search to identify these connections and share them with the FBI. Several programs were developed to address the U.S. Government’s need to connect the dots of information available to the intelligence community and to strengthen the coordination between foreign intelligence and domestic law enforcement agencies.

Background

NSA is an element of the U.S. intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes. NSA performs this mission by engaging in the collection of “signals intelligence,” which, quite literally, is the production of foreign intelligence through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire, or other electromagnetic means. Every intelligence activity NSA undertakes is necessarily constrained to these central foreign intelligence and counterintelligence purposes. NSA’s challenge in an increasingly interconnected world -- a world where our adversaries make use of the same communications systems and services as Americans and our allies -- is to find and report on the communications of foreign intelligence value while respecting privacy and civil liberties. We do not need to sacrifice civil liberties for the sake of national security – both are integral to who we are as Americans. NSA can and will continue to conduct its operations in a manner that respects both. We strive to achieve this through a system that is carefully designed to be consistent with *Authorities* and *Controls* and enabled by capabilities that allow us to *Collect, Analyze, and Report* intelligence needed to protect national security.

NSA Mission

NSA’s mission is to help protect national security by providing policy makers and military commanders with the intelligence information they need to do their jobs. NSA’s priorities are driven by externally developed and validated intelligence requirements, provided to NSA by the President, his national security team, and their staffs through the National Intelligence Priorities Framework.

NSA Collection Authorities

NSA’s collection authorities stem from two key sources: Executive Order 12333 and the Foreign Intelligence Surveillance Act of 1978 (FISA).

Executive Order 12333

Executive Order 12333 is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the United States. To the extent a person located outside the United States communicates with someone inside the United States or someone inside the United States communicates with a person located outside the United States those communications could also be collected. Collection pursuant to EO 12333 is conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA. Intelligence activities conducted under this authority are carried out in accordance with minimization procedures established by the Secretary of Defense and approved by the Attorney General.

To undertake collections authorized by EO 12333, NSA uses a variety of methodologies. Regardless of the specific authority or collection source, NSA applies the process described below.

1. NSA identifies foreign entities (persons or organizations) that have information responsive to an identified foreign intelligence requirement. For instance, NSA works to identify individuals who may belong to a terrorist network.
2. NSA develops the “network” with which that person or organization’s information is shared or the command and control structure through which it flows. In other words, if NSA is tracking a specific terrorist, NSA will endeavor to determine who that person is in contact with, and who he is taking direction from.
3. NSA identifies how the foreign entities communicate (radio, e-mail, telephony, etc.)
4. NSA then identifies the telecommunications infrastructure used to transmit those communications.
5. NSA identifies vulnerabilities in the methods of communication used to transmit them.
6. NSA matches its collection to those vulnerabilities, or develops new capabilities to acquire communications of interest if needed.

This process will often involve the collection of communications metadata – data that helps NSA understand where to find valid foreign intelligence information needed to protect U.S. national security interests in a large and complicated global network. For instance, the collection of overseas communications metadata associated with telephone calls – such as the telephone numbers, and time and duration of calls – allows NSA to map communications between terrorists and their associates. This strategy helps ensure that NSA’s collection of communications content is more precisely focused on only those targets necessary to respond to identified foreign intelligence requirements.

NSA uses EO 12333 authority to collect foreign intelligence from communications systems around the world. Due to the fragility of these sources, providing any significant detail outside of classified channels is damaging to national security. Nonetheless, every type of collection undergoes a strict oversight and compliance process internal to NSA that is conducted by entities within NSA other than those responsible for the actual collection.

FISA Collection

FISA regulates certain types of foreign intelligence collection including certain collection that occurs with compelled assistance from U.S. telecommunications companies. Given the techniques that NSA must employ when conducting NSA’s foreign intelligence mission, NSA quite properly relies on FISA authorizations to acquire significant foreign intelligence information and will work with the FBI and other agencies to connect the dots between foreign-based actors and their activities in the U.S. The FISA Court plays an important role in helping to ensure that signals intelligence collection governed by FISA is conducted in conformity with the requirements of the statute. All three branches of the U.S. Government have responsibilities for programs conducted under FISA, and a key role of the FISA Court is to ensure that activities conducted pursuant to FISA authorizations are consistent with the statute, as well as the U.S. Constitution, including the Fourth Amendment.

FISA Section 702

Under Section 702 of the FISA, NSA is authorized to target non-U.S. persons who are reasonably believed to be located outside the United States. The principal application of this

authority is in the collection of communications by foreign persons that utilize U.S. communications service providers. The United States is a principal hub in the world's telecommunications system and FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans. In general, Section 702 authorizes the Attorney General and Director of National Intelligence to make and submit to the FISA Court written certifications for the purpose of acquiring foreign intelligence information. Upon the issuance of an order by the FISA Court approving such a certification and the use of targeting and minimization procedures, the Attorney General and Director of National Intelligence may jointly authorize for up to one year the targeting of non-United States persons reasonably believed to be located overseas to acquire foreign intelligence information. The collection is acquired through compelled assistance from relevant electronic communications service providers.

NSA provides specific identifiers (for example, e-mail addresses, telephone numbers) used by non-U.S. persons overseas who the government believes possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification. Once approved, those identifiers are used to select communications for acquisition. Service providers are compelled to assist NSA in acquiring the communications associated with those identifiers.

For a variety of reasons, including technical ones, the communications of U.S. persons are sometimes incidentally acquired in targeting the foreign entities. For example, a U.S. person might be courtesy copied on an e-mail to or from a legitimate foreign target, or a person in the U.S. might be in contact with a known terrorist target. In those cases, minimization procedures adopted by the Attorney General in consultation with the Director of National Intelligence and approved by the Foreign Intelligence Surveillance Court are used to protect the privacy of the U.S. person. These minimization procedures control the acquisition, retention, and dissemination of any U.S. person information incidentally acquired during operations conducted pursuant to Section 702.

The collection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world. One notable example is the Najibullah Zazi case. In early September 2009, while monitoring the activities of al Qaeda terrorists in Pakistan, NSA noted contact from an individual in the U.S. that the FBI subsequently identified as Colorado-based Najibullah Zazi. The U.S. Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with al Qaeda, as well as identify any foreign or domestic terrorist links. The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi pled guilty to conspiring to bomb the New York City subway system. The FAA Section 702 collection against foreign terrorists was critical to the discovery and disruption of this threat to the U.S.

FISA (Title I)

NSA relies on Title I of FISA to conduct electronic surveillance of foreign powers or their agents, to include members of international terrorist organizations. Except for certain narrow

exceptions specified in FISA, a specific court order from the Foreign Intelligence Surveillance Court based on a showing of probable cause is required for this type of collection.

Collection of U.S. Person Data

There are three additional FISA authorities that NSA relies on, after gaining court approval, that involve the acquisition of communications, or information about communications, of U.S. persons for foreign intelligence purposes on which additional focus is appropriate. These are the Business Records FISA provision in Section 501 (also known by its section numbering within the PATRIOT Act as Section 215) and Sections 704 and 705(b) of the FISA.

Business Records FISA, Section 215

Under NSA's Business Records FISA program (or BR FISA), first approved by the Foreign Intelligence Surveillance Court (FISC) in 2006 and subsequently reauthorized during two different Administrations, four different Congresses, and by 14 federal judges, specified U.S. telecommunications providers are compelled by court order to provide NSA with information about telephone calls to, from, or within the U.S. The information is known as metadata, and consists of information such as the called and calling telephone numbers and the date, time, and duration of the call – but no user identification, content, or cell site locational data. The purpose of this particular collection is to identify the U.S. nexus of a foreign terrorist threat to the homeland

The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism. Under the FISC orders authorizing the collection, authorized queries may only begin with an “identifier,” such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court. An identifier used to commence a query of the data is referred to as a “seed.” Specifically, under Court-approved rules applicable to the program, there must be a “reasonable, articulable suspicion” that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization. When the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment. The “reasonable, articulable suspicion” requirement protects against the indiscriminate querying of the collected data. Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.

The BR FISA program is used in cases where there is believed to be a threat to the homeland. Of the 54 terrorism events recently discussed in public, 13 of them had a homeland nexus, and in 12 of those cases, BR FISA played a role. Every search into the BR FISA database is auditable and all three branches of our government exercise oversight over NSA's use of this authority.

FISA Sections 704 and 705(b)

FISA Section 704 authorizes the targeting of a U.S. person outside the U.S. for foreign intelligence purposes if there is probable cause to believe the U.S. person is a foreign power or is an officer, employee, or agent of a foreign power. This requires a specific, individual court order

by the Foreign Intelligence Surveillance Court. The collection must be conducted using techniques not otherwise regulated by FISA.

Section 705(b) permits the Attorney General to approve similar collection against a U.S. person who is already the subject of a FISA court order obtained pursuant to Section 105 or 304 of FISA. The probable cause standard has, in these cases, already been met through the FISA court order process.

Scope and Scale of NSA Collection

According to figures published by a major tech provider, the Internet carries 1,826 Petabytes of information per day. In its foreign intelligence mission, NSA touches about 1.6% of that. However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission – that's less than one part in a million. Put another way, if a standard basketball court represented the global communications environment, NSA's total collection would be represented by an area smaller than a dime on that basketball court.

The Essential Role of Corporate Communications Providers

Under all FISA and FAA programs, the government compels one or more providers to assist NSA with the collection of information responsive to the foreign intelligence need. The government employs covernames to describe its collection by source. Some that have been revealed in the press recently include FAIRVIEW, BLARNEY, OAKSTAR, and LITHIUM. While some have tried to characterize the involvement of such providers as separate programs, that is not accurate. The role of providers compelled to provide assistance by the FISC is identified separately by the Government as a specific facet of the lawful collection activity.

The Essential Role of Foreign Partners

NSA partners with well over 30 different nations in order to conduct its foreign intelligence mission. In every case, NSA does not and will not use a relationship with a foreign intelligence service to ask that service to do what NSA is itself prohibited by law from doing. These partnerships are an important part of the U.S. and allied defense against terrorists, cyber threat actors, and others who threaten our individual and collective security. Both parties to these relationships benefit.

One of the most successful sets of international partnerships for signals intelligence is the coalition that NSA developed to support U.S. and allied troops in Iraq and Afghanistan. The combined efforts of as many as 14 nations provided signals intelligence support that saved U.S. and allied lives by helping to identify and neutralize extremist threats across the breadth of both battlefields. The senior U.S. commander in Iraq credited signals intelligence with being a prime reason for the significant progress made by U.S. troops in the 2008 surge, directly enabling the removal of almost 4,000 insurgents from the battlefield.

The Oversight and Compliance Framework

NSA has an internal oversight and compliance framework to provide assurance that NSA's activities – its people, its technology, and its operations – act consistently with the law and with NSA and U.S. intelligence community policies and procedures. This framework is overseen by multiple organizations external to NSA, including the Director of National Intelligence, the Attorney General, the Congress, and for activities regulated by FISA, the Foreign Intelligence Surveillance Court.

NSA has had different minimization procedures for different types of collection for decades. Among other things, NSA's minimization procedures, to include procedures implemented by United States Signals Intelligence Directive No. SP0018 (USSID 18), provide detailed instructions to NSA personnel on how to handle incidentally acquired U.S. person information. The minimization procedures reflect the reality that U.S. communications flow over the same communications channels that foreign intelligence targets use, and that foreign intelligence targets often discuss information concerning U.S. persons, such as U.S. persons who may be the intended victims of a planned terrorist attack. Minimization procedures direct NSA on the proper way to treat information at all stages of the foreign intelligence process in order to protect U.S. persons' privacy interests.

In 2009 NSA stood up a formal Director of Compliance position, affirmed by Congress in the FY2010 Intelligence Authorization Bill, which monitors verifiable consistency with laws and policies designed to protect U.S. person information during the conduct of NSA's mission. The program managed by the Director of Compliance builds on a number of previous efforts at NSA, and leverages best practices from the professional compliance community in industry and elsewhere in the government. Compliance at NSA is overseen internally by the NSA Inspector General and is also overseen by a number of organizations external to NSA, including the Department of Justice, the Office of the Director of National Intelligence, and the Assistant Secretary of Defense for Intelligence Oversight, the Congress, and the Foreign Intelligence Surveillance Court.

In addition to NSA's compliance safeguards, NSA personnel are obligated to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure. This self-reporting is part of the culture and fabric of NSA. If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to constantly improve.