

THE WHITE HOUSE  
Office of the Press Secretary

FOR IMMEDIATE RELEASE  
January 17, 2014

**FACT SHEET: Review of U.S. Signals Intelligence**

In the latter half of 2013 and early 2014, the United States Government undertook a broad-ranging and unprecedented review of our signals intelligence programs, led by the White House with relevant Departments and Agencies across the Government. In addition to our own intensive work, the review process drew on input from key stakeholders, including Congress, the tech community, civil society, foreign partners, the [Review Group on Intelligence and Communication Technologies](#), the Privacy and Civil Liberties Oversight Board, and others. The Administration's review examined how, in light of new and changing technologies, we can use our intelligence capabilities in a way that optimally protects our national security while supporting our foreign policy, respecting privacy and civil liberties, maintaining the public trust, and reducing the risk of unauthorized disclosures. On January 17, 2014, the President delivered a speech at the Department of Justice to announce the outcomes of this review process.

In that speech, the President made clear that the men and women of the U.S. intelligence community, including the NSA, consistently follow those protocols designed to protect the privacy of ordinary people and are not abusing authorities. When mistakes have been made, they have corrected those mistakes. But for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world. To that end, the Administration has developed a path forward that we believe should give the American people greater confidence that their rights are being protected, while preserving important tools that keep us safe, and that addresses significant questions that have been raised overseas. Today the President announced the Administration's adoption of a series of concrete and substantial reforms that the Administration will adopt administratively or seek to codify with Congress, to include a majority of the [recommendations made by the Review Group](#).

**New Presidential Policy Directive**

Today, President Obama issued [a new presidential policy directive](#) for our signals intelligence activities, at home and abroad. This directive lays out new principles that govern how we conduct signals intelligence collection, and strengthen how we provide executive branch oversight of our signals intelligence activities. It will ensure that we take into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of our companies; and our commitment to privacy and basic liberties. And we will review decisions about

intelligence priorities and sensitive targets on an annual basis, so that our actions are regularly scrutinized by the President's senior national security team.

### **The Foreign Intelligence Surveillance Court (FISC)**

Since the review began, we've declassified over 40 opinions and orders of the Foreign Intelligence Surveillance Court, which provides judicial review of some of our most sensitive intelligence activities – including the Section 702 program targeting foreign individuals overseas and the Section 215 telephone metadata program. Going forward, the President directed the Director of National Intelligence, in consultation with the Attorney General, to annually review – for the purpose of declassification – any future opinions of the Court with broad privacy implications, and to report to the President and Congress on these efforts. To ensure that the Court hears a broader range of privacy perspectives, the President called on Congress to authorize the establishment of a panel of advocates from outside the government to provide an independent voice in significant cases before the Court.

### **Section 702 of Foreign Intelligence Surveillance Act**

Section 702 is a valuable program that allows the government to intercept the communications of foreign targets overseas who have information that's important to our national security. The President believes that we can do more to ensure that the civil liberties of U.S. persons are not compromised in this program. To address incidental collection of communications between Americans and foreign citizens, the President has asked the Attorney General and DNI to initiate reforms that place additional restrictions on the government's ability to retain, search, and use in criminal cases, communications between Americans and foreign citizens incidentally collected under Section 702.

### **Section 215 of the PATRIOT Act**

Under Section 215 of the PATRIOT Act the government collects meta-data related to telephone calls in bulk. We believe this is a capability that we must preserve, and would note that the Review Group turned up no indication that the program had been intentionally abused. But, we believe we must do more to give people confidence. For this reason, the President ordered a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a program that preserves the capabilities we need without the government holding the data.

This transition has two steps. Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of three. The President has directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding, or in a true emergency. On the broader question, the President has instructed the intelligence community and the Attorney General to use this transition period to develop options for a new program

that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this meta-data, and report back to him with options for alternative approaches before the program comes up for reauthorization on March 28. At the same time, the President will consult with the relevant committees in Congress to seek their views, and then seek congressional authorization for the new program as needed.

### **National Security Letters**

In investigating threats, the FBI relies on the use of National Security Letters (NSLs), which can be used to require companies to provide certain types of information to the government without disclosing the orders to the subject of the investigation. In order to be more transparent in how the government uses this authority, the President directed the Attorney General to amend how we use NSLs to ensure that non-disclosure is not indefinite, and will terminate within a fixed time unless the government demonstrates a need for further secrecy.

We will also enable communications providers to make public more information than ever before about the orders they have received to provide data to the government. These companies have made clear that they want to be more transparent about the FISA, NSL and law enforcement requests that they receive from the government. The Administration agrees that these concerns are important, and is in discussions with the providers about ways in which additional information could be made public.

### **Increasing Confidence Overseas**

U.S. global leadership demands that we balance our security requirements against our need to maintain trust and cooperation among people and leaders around the world. For that reason, the new presidential guidance lays out principles that govern what we do abroad, and clarifies what we don't do. The United States only uses signals intelligence for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the e-mails or phone calls of ordinary people.

*What we don't do:* The United States does not collect intelligence to suppress criticism or dissent. We do not collect intelligence to disadvantage people based on their ethnicity, race, gender, sexual orientation, or religion. And we do not collect intelligence to provide a competitive advantage to U.S. companies, or U.S. commercial sectors.

*What we will do:* In terms of our bulk collection, we will only use data to meet specific security requirements: counter-intelligence; counter-terrorism; counter-proliferation; cyber-security; force protection for our troops and allies; and combating transnational crime, including sanctions evasion.

The President has also decided that we will take the unprecedented step of extending certain protections that we have for the American people to people overseas. He has directed the Attorney General and DNI to develop these safeguards, which will limit the duration that we can hold personal information, while also restricting the dissemination of this information.

People around the world – regardless of their nationality – should know that the United States is not spying on ordinary people who don't threaten our national security and takes their privacy concerns into account.

This applies to foreign leaders as well. Given the understandable attention that this issue has received, the President has made clear to the intelligence community that – unless there is a compelling national security purpose – we will not monitor the communications of heads of state and government of our close friends and allies. And he has instructed his national security team, as well as the intelligence community, to work with foreign counterparts to deepen our coordination and cooperation in ways that rebuild trust going forward.

While our intelligence agencies will continue to gather information about the intentions of governments – as opposed to ordinary citizens – around the world, in the same way that the intelligence services of every other nation do, we will not apologize because our services may be more effective. But heads of state and government with whom we work closely, on whose cooperation we depend, should feel confident that we are treating them as real partners. The changes the President ordered do just that.

### **International Engagement**

To support our work, the President has directed changes to how our government is organized. The State Department will designate a senior officer to coordinate our diplomacy on issues related to technology and signals intelligence. The Administration will appoint a senior official at the White House to implement the new privacy safeguards that we have announced today. And the President has also asked his Counselor, John Podesta, to lead a review of big data and privacy. This group will consist of government officials who – along with the President's Council of Advisors on Science and Technology – will reach out to privacy experts, technologists and business leaders, and look at how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security.

The President also announced that we will devote resources to centralize and improve the process we use to handle foreign requests for legal assistance, called the Mutual Legal Assistance Treaty (MLAT) process. Under MLAT, foreign partners can request access to information stored in the United States pursuant to U.S. law. As the

concentration of U.S.-based cloud storage providers has increased, so has the number of MLAT requests. To address this increase, we will speed up and centralize MLAT processing; we will implement new technology to increase the efficiency and transparency of the process; and we will increase our international outreach and training to help ensure that requests meet U.S. legal standards. We will put the necessary resources in place to reduce our response time by half by the end of 2015, and we will work aggressively to respond to legally sufficient requests in a matter of weeks. This change will ensure that our foreign partners can more effectively use information held in the U.S. to prosecute terrorists and other criminals, while still meeting the strict privacy protections put in place by U.S. law.

\*\*\*

In addition to the initiatives that were announced by the President, the Administration's review affirmed our commitment to ongoing initiatives:

### **Consumer Privacy Codes of Conduct**

Two years ago, the President released a Blueprint for Consumer Privacy in the Digital Age as a "dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies." Following the release of the Blueprint, the Administration has convened the private sector, privacy experts, and consumer advocates to develop voluntary codes of conduct to safeguard sensitive consumer data. Last summer a multi-stakeholder group completed the first such code on how mobile apps should access private information. The Department of Commerce is continuing this multi-stakeholder process, aiming to launch the development of new codes of conduct in 2014.

### **Commitment to an Open Internet**

Maintaining an open, accessible Internet, including the ability to transmit data across borders freely is essential for global growth and development. We will redouble our commitment to promote the free-flow of information around the world through an inclusive approach to Internet governance and policymaking. Individuals in the 21st century depend on free and unfettered access to data flows without arbitrary government regulation. Businesses depend increasingly on agreed data-sharing regimes that allow information to move seamlessly across borders in support of global business operations. Developing countries and small businesses around the world in particular have a lot at stake, and much to lose from limitations restricting the Internet as an engine of prosperity and expression. Requirements to store data or locate hardware in a given location hurt competition, stifle innovation, and diminish economic growth. And they undermine the DNA of the Internet, which by design is a globally-distributed network of networks. We will continue to support the multi-stakeholder, inclusive approach to the Internet and work to strengthen and make more inclusive its policy-making, standards-setting, and governance organizations.

###