IC ON THE RECORD

- CY2020 Transparency Report
- U.S. Person Unmasking Procedures
- 2019 National Intelligence Strategy
- IC TRANSPARENCY PLAN

SIGNALS INTELLIGENCE REFORM

2016 PROGRESS REPORT

- INTRODUCTION
- PRIVACY PROTECTIONS
- LIMITING SIGINT COLLECTION AND USE
- ENHANCING TRANSPARENCY

VIEW THE 2015 REPORT

INTRODUCTION

Last year, one year after the President signed **Presidential Policy Directive-28**, Signals Intelligence Activities (PPD-28), the Office of the Director of National Intelligence **issued a public report** on the Intelligence Community's changes to signals intelligence (SIGINT) activities.

The 2015 report detailed the significant progress the U.S. Government made in strengthening privacy and civil liberty protections, increasing transparency, and setting new limits on signals intelligence collection and use. That work has continued over the past year and the Office of the Director of National Intelligence is now reporting on the Intelligence Community's continued progress in implementing the requirements of PPD-28 as well as other transparency efforts discussed in the previous report.

This past year, the Intelligence Community continued to strengthen privacy protections of personal information, to enhance and institutionalize transparency, to declassify and release more information to the general public, to encourage dialogue with the American people and our foreign partners on our collection activities and transparency efforts, and to work with Congress to secure the passage of the USA FREEDOM Act. The impact and results of these efforts are described in this report.

Back to Top

PRIVACY PROTECTIONS

PPD-28 Policies and Procedures

In last year's report, we emphasized our commitment to strengthen privacy protections of personal information for all people, regardless of nationality. In the 2015 report, the Director of National Intelligence reported that, as required by PPD-28, all Intelligence Community elements reviewed and updated their existing policies and procedures, or issued new policies or procedures, to enhance safeguards for personal information collected through SIGINT, regardless of nationality and consistent with national security, technical capabilities, and operational needs. **These policies were released publicly.**

In addition to the policies and procedures, Intelligence Community elements have taken steps to sensitize their personnel to the requirements of PPD-28 by creating new or modifying existing training and, where appropriate, internal policies. For example, NSA created and implemented supplemental procedures, conducted a series of information sessions, promoted awareness to its workforce by including PPD-28 discussions in NSA events, and developed internal online training specifically related to PPD-28. By the end of 2015, all NSA analysts with access to unreviewed and unevaluated SIGINT were obligated to review and acknowledge the supplemental procedures incorporating PPD-28 into NSA policy or lose access to the data. Similarly, the FBI and CIA also developed internal guidelines and have taken steps to update various training mechanisms to incorporate PPD-28 principles and requirements. Further, the Deputy Directorate for Intelligence Integration in the Office of the Director of National Intelligence has established an Intelligence Community-wide training program that describes the governing principles for SIGINT activities as articulated in PPD-28.

Several agencies also created or modified existing oversight mechanisms to enable reporting incidents of non-compliance with PPD-28. PPD-28 requires that significant compliance incidents involving the personal information of any person collected from SIGINT be reported promptly to the Director of National Intelligence. To that end, the Office of the Director of National Intelligence is drafting and coordinating an Intelligence Community Standard (ICS) outlining the steps for agencies to report these matters in a timely and efficient manner.

Enhanced Protections Established by Legislation

In our 2015 report, the Intelligence Community encouraged Congress to pass legislation that would end bulk collection of telephone metadata under Title V of the Foreign Intelligence Surveillance Act (FISA) while ensuring that the Government has access to the information it needs to protect national security.

In June 2015, Congress passed the USA Freedom Act, which enhances privacy and civil liberty protections while ensuring the Intelligence Community has the necessary tools to protect both the homeland and U.S. interests abroad. Specifically, the USA FREEDOM Act:

- Prohibits the U.S. Government from collecting bulk information by using FISA business records authority, FISA pen register/trap and trace authority, and National Security Letters.

- Creates a new framework for the NSA to seek the ongoing production of call detail records associated with international terrorism by sending query requests directly to telecommunications service providers. The bill ensures that bulk collection of call detail records cannot occur under FISA business records authority by requiring that each FISA application and order include a "specific selection term." Before specific selection terms are submitted as query requests for the production of call detail records, the FISA Court (or the Attorney General in an emergency) must find both that the records are relevant to an authorized investigation and that there is a reasonable, articulable suspicion that the information sought is associated with a foreign power or agent of a foreign power engaged in international terrorism. NSA's Civil Liberties and Privacy report on this new process, as well as its minimization procedures for this collection, **can be found here**.

- Strengthens the FISA Court process by requiring the FISA Court to appoint a panel of experts who can serve as amicus curiae should the FISA Court confront significant or novel interpretations of the law. The Court has selected five lawyers for the panel and has already appointed amicus curiae when it has deemed it appropriate to do so.

- Requires the U.S. Government to declassify or summarize for public release, FISA Court opinions that involve significant interpretations of the law. Between June 2015 and December 2015, the Intelligence Community, in coordination with the Department of Justice, reviewed FISA Court documents for public release, consistent with national security. The FISA Court has posted these documents on its **publicly available website.**

- Requires the U.S. Government to publish and make publicly available its annual transparency report containing statistics of its surveillance activities. **Read last year's report.**

- Allows companies who receive legal process from the U.S. Government to periodically report the number, in banded ranges, of national security orders received.

Engagement with the Privacy and Civil Liberties Oversight Board

The Intelligence Community continues to engage with the **Privacy and Civil Liberties Oversight Board** on ways to ensure that our collection activities contain adequate safeguards while meeting operational needs. Specifically, the Intelligence Community has focused on implementing the recommendations made by the Board in its 2014 reports on sections 215 and 702. While the enactment of USA FREEDOM Act addressed many of the Board's section 215 report recommendations, the U.S. Government has worked diligently, often seeking additional Board feedback, to implement its section 702 report recommendations. For example, the Board's recommendations dealing with changes to section 702 minimization and targeting procedures have been successfully implemented by the Intelligence Community and approved by the FISA Court when it approved renewed certifications under Section 702.

Additionally, following the Board's July 2014 announcement that it planned to examine Executive Order (EO) 12333's implications for privacy and civil liberties, the Intelligence Community began providing relevant briefings to the Board. The Board determined in April 2015, that it will conduct in-depth reviews of specific counterterrorism activities of the NSA and CIA undertaken pursuant to EO 12333. The Intelligence Community continues to assist the Board in its ongoing review of these activities.

More recently, the Board began to review the Intelligence Community's implementation of PPD-28. The Board will review and assess the Intelligence Community's implementation of matters contained within PPD-28 that fall within the Board's mandate. Several agencies, including NSA, CIA and FBI, have already begun to brief the Board on PPD-28's applicability to their collection activities as well as their implementation of its requirements.

Back to Top

LIMITING SIGINT COLLECTION AND USE

The National Intelligence Priorities Framework

This year, in response to PPD-28, the Office of the Director of National Intelligence led a comprehensive review with senior policymakers of the intelligence priorities captured in the **National Intelligence Priorities Framework**, or "NIPF." The NIPF is the primary mechanism by which the Director of National Intelligence manages and communicates national intelligence priorities to Intelligence Community agencies to enable them to prioritize collection and analytic activities, including the use of SIGINT. The NIPF establishes priorities over the upcoming 12-18 months, and includes warning issues that have the potential to catch the U.S. Government by surprise. These priorities address a diverse range of threats, and a description of these threats is published by the Director of National Intelligence in the annual release of the Worldwide Threat Assessment.

Policymakers from the departments and agencies designated in PPD-28 examined the content of the national intelligence priorities that guide the Intelligence Community's collection and analytic activities. Policymakers validated each priority with respect to the anticipated intelligence value from SIGINT coverage. This process ensures that SIGINT is used in support of valid national security objectives.

Refined Process on SIGINT Targeting

PPD-28 directed changes to the process for selecting targets for SIGINT collection in response to intelligence priorities, to ensure that special concerns unique to SIGINT collection were considered alongside other risks and benefits. The heads of policy departments and agencies must now approve SIGINT collection consistent with the requirements of PPD-28. This ensures those who are best positioned to identify the requirements for intelligence collection – senior policymakers – provide comprehensive oversight of SIGINT collection. The decisions to initiate such SIGINT collection must reflect both the value of the collection to our national interests and the potential risks, including economic interests, privacy concerns, and diplomatic, law enforcement, and other relationships. The Office of the Director of National Intelligence works with

the Intelligence Community to help ensure that SIGINT activities remain consistent with any collection restrictions established by senior policymakers.

The Office of the Director of National Intelligence facilitates a process to ensure policymakers regularly review and revalidate the targets for SIGINT collection. During this process, policymakers are presented with collection profiles, and they assess the risk and value of the Intelligence Community's collection. They assess the value of SIGINT collection on targets related to all national priorities. In cases where policymakers decide the risk outweighs its value, they establish restrictions for terminating and preventing collection. The Office of the Director of National Intelligence has maintained this process since 2013 and continues to ensure that policymakers conduct updates.

Limits on Use of SIGINT Collected in Bulk

Section 2 of PPD-28 articulated limits on the use of SIGINT collected in bulk. PPD-28 generally limits Intelligence Community use of SIGINT collected in bulk for six specific purposes: (i) to counter espionage and other threats and activities of foreign powers or intelligence services against the U.S. and its interests; (ii) counterterrorism; (iii) counter-proliferation; (iv) cybersecurity; (v) to detect and counter threats to U.S. or allied armed forces or other U.S. or allied personnel; and (vi) to combat transnational criminal threats, including illicit finance and sanctions evasion. In 2015, senior policymakers re-evaluated these six criteria for the purpose of the annual SIGINT review under PPD-28, and recommended that the current list of permissible uses be maintained.

Back to Top

ENHANCING AND INSTITUTIONALIZING TRANSPARENCY

The Intelligence Community continues to recognize that public trust and support of its activities can only be achieved with greater transparency. To that end, since the last report, the Intelligence Community has worked to institutionalize our transparency efforts and has declassified and publicly released additional documents, engaged with civil liberties and privacy advocates, and participated in numerous public events.

Public Release of Previously Classified Information

Last year, the Office of the Director of National Intelligence's report discussed the development of IC on the Record. IC on the Record, and the accompanying Twitter account, provide direct access to factual unclassified or declassified information related to lawful surveillance activities of the U.S. Intelligence Community. In addition to comprehensive explanations of the authorities under which the Intelligence Community conducts foreign intelligence surveillance, the site addresses appropriate use and dissemination of collected data, oversight and compliance. Since its launch in August 2013, IC on the Record has provided a central hub for Intelligence Community-related official statements, declassified documents, congressional testimony, transparency reporting and multimedia content, making these materials more readily available and broadly accessible than ever before. To date, the IC has released on **IC on the Record** approximately 350 documents consisting of more than 6500 pages.

Examples of some recent postings include:

- The Office of the Director of National Intelligence's concurrence with the Department of State revocation of Anwar al-Aulaqi's American passport
- The Office of the Director of National Intelligence's Freedom of Information Act release of emails and correspondence pertaining to the overall situation in and around Benghazi, Libya
- The public release of the "Bin Laden's Bookshelf" documents collected during the Abbottabad raid
- The Department of Justice's release of additional information from Inspector General reports concerning collection activities authorized by President George W. Bush after the attacks of September 11, 2001
- The Fiscal Year 2015 budget figure for the National Intelligence Program, including details on the National Intelligence Program appropriations and access to historical Intelligence Community budget information
- The Report to the Director of National Intelligence by the Intelligence Community Review Panel on the Fort Hood and Northwest Flight 252 Incidentss
- The declassification of the renewal of collection under section 215 of the USA PATRIOT Act, as amended by the USA FREEDOM Act
- The 2008 FISA Court opinion on section 702 – the first FISA Court opinion to approve a FISA section 702 certification – as well as the FISA Court's 2014 opinion evaluating and approving the U.S. Government's continued use of FISA section 702 authorities
- A 2014 FISA section 702 certification application
- All the 2014 FISA section 702 Standard Minimization Procedures

In addition to IC on the Record, the Office of the Director of National Intelligence is currently developing intelligence.gov, which will be a new hub for transparency about the Intelligence Community's activities and how the Intelligence Community generally operates.

Specific Transparency Efforts

The Intelligence Community has also made significant efforts to engage with the public. These efforts include:

- The Principles of Intelligence Transparency – The Intelligence Community, through an interagency working group, developed **The Principles of Intelligence Transparency for the Intelligence Community**, which was released in February 2015. The Principles provide guidance to the Intelligence Community on making information publicly available in a manner that enhances understanding of the Intelligence Community while protecting classified national security information.

- Transparency Implementation Plan – Following release of the Principles, the Office of the Director of National Intelligence developed an **Implementation Plan for the Principles**, which was released in October 2015. The Plan puts forth an Intelligence Community-wide strategy of proactive transparency and provides specific initiatives for Intelligence Community elements to undertake in establishing sustainable transparency practices.

- Support to Humanitarian Crises – The National Geospatial-Intelligence Agency supported lead federal agencies during the 2014 Ebola crisis by **providing public online access to geospatial data**, including relevant cultural information, maps of affected areas across West Africa, electric and power infrastructure information, and ground transportation methods.

- The Public and Academia – In September 2015, **the CIA released more than 2,500 historical Presidential Daily Briefs**, which are highly sensitive and classified documents, in a public event at the LBJ Presidential Library at the University of Texas, Austin. Just a few months earlier, the CIA had also released declassified documents related to the Agency's performance in the period before 9/11. Separately, Intelligence Community leaders participated in a wide range of public engagements, including the Council on Foreign Relations in New York, the GEOINT Symposium in Washington D.C., the Annual Space Symposium in Colorado, and the Georgetown Cyber Conference.

- Privacy and Technology – In July 2015, representatives from the Intelligence Community and the National Academy of Sciences held a **public workshop on Future Technology, Civil Liberties and Privacy**. The workshop was attended by technologists, academics, and company representatives, and focused on the critical role of transparency in informing the public on privacy and civil liberties laws. The workshop explored privacy implications of emerging technologies, the social science of privacy, and ethical approaches to data collection and use.

- Freedom of Information Act (FOIA) – The Office of the Director of National Intelligence is participating in the Administration's **Proactive Disclosure pilot program**. The intent of the pilot is to determine if FOIA policy should require agencies to proactively post all documents released through FOIA to their public website or to FOIA.gov. The six-month pilot allows participating agencies to assess the impact on their respective FOIA programs, while the Department of Justice examines the resulting benefits to the public.

- Open Government – Participating in the White House's Open Government initiative to promote government transparency, the Intelligence Community ***provided input to the 2015 Open Government National Action Plan***, committing for the first time to publish an Intelligence Community-wide Open

Government Plan. The Intelligence Community also pledged to conduct more structured engagements with civil society as part of the Open Government initiative to facilitate public exchange and input.

- The Intelligence Community continues to consider additional forums for engagement on its efforts to implement transparency in a consistent, coordinated, and credible manner. Intelligence Community representatives are considering possible outreach efforts to discuss enhanced transparency in the U.S. Intelligence Community with foreign partners in addition to engagement with the public.

The Intelligence Community believes that it is important that we give the public greater insight into the laws and policies that we operate under and how we interpret these authorities. We hope that our continuing efforts of transparency will demonstrate to both the American people and the rest of the world that our intelligence activities are not arbitrary, but conducted responsibly and pursuant to the law.

Back to Top

IC ON THE RECORD:

Direct access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community.

Created at the direction of the President of the United States and maintained by the Office of the Director of National Intelligence.

SEARCH TOOLS:

Find it faster with the full text search IC on the Record Database at Intelligence.gov

Review our online "Guide to Posted Documents Regarding Use of National Security Authorities"

CONTENT:

- **Official Statements**

- **Declassified Documents**

- **Testimony**

- **Speeches & Interviews**

- **Fact Sheets**

- **Oversight & Compliance**

- **Video**

- **IC Budget**

NOTE: Before searching here on Tumblr, try the IC on the Record Database at Intel.gov for a new and improved full text search of all posted documents and statements.

Search this site

This website is maintained by the Office of the Director of National Intelligence.