

Office of the Director of National Intelligence
Open Government Plan
2017

Introduction

The following is the 2017 Open Government Plan of the Office of the Director of National Intelligence (ODNI) as required by the Open Government Directive issued by the Director of the Office of Management and Budget on December 8, 2009 and subsequent guidance issued on July 14, 2016.

The ODNI was created by the Intelligence Reform and Terrorism Prevention Act and began operations when Ambassador John D. Negroponte was sworn in as the first Director of National Intelligence (DNI) on April 21, 2005.

The current DNI, James R. Clapper, supports increased transparency, participation, and collaboration within the Government and with the American people, as articulated by the President in his January 21, [2009 "Memorandum on Transparency and Open Government"](#). Therefore, the ODNI will continue to make every effort to increase transparency and openness, while also protecting classified and sensitive national security information and intelligence sources and methods from unauthorized disclosure.

The following plan describes how the ODNI currently promotes openness, identifies active public disclosure initiatives, and presents new initiatives planned for FY 2017 and beyond. This plan *does not* represent the entirety of Open Government initiatives within the Intelligence Community (IC) as a whole.

New or Expanded Initiatives

A. Open Data.

In the interest of increased transparency, the ODNI routinely publishes information concerning the ODNI and IC on its public website, www.dni.gov/open. This information includes speeches, press releases, Congressional testimony, and statements for the record by the DNI and other senior ODNI officials, in various formats, including video recordings, podcasts, RSS feeds, and e-mail subscriptions.

In addition, the ODNI, through the Office of the Program Manager for the Information Sharing Environment, released a series of tools and resources on [GitHub](#), called Project Interoperability, an open collaborative platform popular with web developers across the country. The tools and resources provide a start-up guide for information interoperability between federal agencies, state and local governments, and the private sector. Project Interoperability was created in the same spirit as the White House's

[Project Open Data](#) – government should be transparent, participatory, and collaborative.

Pursuant to Executive Order 13392 and memorandums on openness issued by the President and the Attorney General, the ODNI continues to pro-actively publish information on its public website to increase public knowledge and understanding. Examples of this information include various unclassified policy documents including Intelligence Community Directives and Intelligence Community Policy Guidance. These disclosures are unprecedented within the IC and have been viewed positively by public interest groups.

B. Proactive Disclosures.

In order to earn and retain public trust, the IC has launched a strategic effort to enhance transparency of IC activities (i.e., intelligence transparency), consistent with protecting national security as required by the Executive Order (EO) on Classified National Security Information (EO 13526) and ensuring that intelligence sources and methods are not compromised.

In August 2013, President Obama directed the IC to make public as much information as possible about its surveillance programs with the goal of enhancing transparency. As part of this effort, President Obama directed the Director of National Intelligence (DNI) to create a website to “serve as a hub for further transparency” – resulting in the creation of the Tumblr site [IC on the Record](#) to provide the public with direct access to factual information on the IC’s foreign surveillance activities.

Additionally, the DNI directed an interagency effort to enhance transparency which culminated in the October 2015 publication of the [Principles of Intelligence Transparency for the IC](#), the [Transparency Implementation Plan](#) and the creation of the inter-agency body, the Intelligence Transparency Council. The Principles, Implementation Plan, and the Council were developed to institutionalize transparency; at the same time, the ODNI Civil Liberties and Privacy Office was renamed the Office of Civil Liberties, Privacy, and Transparency (CLPT).

The IC has and continues to execute a range of transparency initiatives including (a) releasing thousands of pages of documents, mostly focused on surveillance issues, such as significant Foreign Intelligence Surveillance Act (FISA) court opinions; (b) publishing annual reports of surveillance-related statistics; and (c) identifying other sources of information that will aid in the public’s understanding of the IC without large-scale audits of IC information. Executing these types of transparency initiatives and identifying other potential transparency efforts enables the IC to build public understanding and trust of the IC’s mission.

In the Principles of Intelligence Transparency for the Intelligence Community (IC) (Reference A), we committed to “taking affirmative steps... to provide timely transparency on matters of public interest.” Taking affirmative steps with regard to topics of historical interest will help facilitate

timely determinations of whether declassification would be appropriate in the interest of enhancing public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security.

To this end, the DNI has requested the [IC Senior Historians Panel](#) to develop recommendations for topics of historical interest, for which the declassification and release, if deemed appropriate, would help the public better understand the work of the IC and contribute to a public dialogue surrounding significant historical intelligence events. If the DNI determines a declassification review of a specific topic is appropriate, D/IMD will conduct the declassification review, in coordination with the affected departments and agencies.

The IC Senior Historians Panel shall, when possible, collaborate with other public historians or private subject-matter experts to solicit input for such topics. This will ensure that when intelligence activities are declassified and released to the public, they are put in their appropriate historical context and made available in an easily accessible medium

C. Privacy.

Consistent with statutory and policy requirements for agencies to inform individuals who visit their websites about the use of information automatically collected or affirmatively provided, ODNI posts its information-handling policies and practices to its public website (www.dni.gov). ODNI's Privacy Act Regulation, its Privacy Act Routine Uses, its Privacy Act Exemption Rules, and all of its Privacy Act Systems of Records Notices are linkable from the website's main page. All entry points to the website provide a link to the Privacy Policy, and all collection of personally identifiable information is accompanied by a Privacy Notice at the point of collection. Social media applications are supported by required Privacy Impact Assessments.

In addition, ODNI has made public its [policy](#) for protecting civil liberties and privacy in the interchange of terrorism information among agencies. This policy conforms to Privacy Guidelines issued pursuant to Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 and Section 1 of Executive Order 13399 (Further Strengthening the Sharing of Terrorism Information to Protect Americans), which called for the establishment of a policy framework to facilitate the sharing of terrorism information while protecting the freedom, information privacy and other legal rights of Americans.

Beyond complying with legal requirements to publish certain documents and reports, ODNI's Office of Civil Liberties Privacy and Transparency (CLPT) has affirmatively undertaken to promote broader understanding regarding the incorporation of civil liberties and privacy protections into the IC's policies, procedures, and activities. CLPT has formally established as one of several strategic goals the goal of providing the ODNI workforce,

mission partners, oversight bodies, Congress, and the American public appropriate transparency into the IC's civil liberties and privacy protections, including oversight. To this end, it has populated a website with materials such as media releases, speeches and interviews, congressional testimonies, policies and reports, summaries of relevant authorities, and other pertinent materials.

Informing the public regarding the existence of "action offices" for redress of complaints is critical to open government. CLPT's web page provides clear guidance for submitting a complaint for investigation in the event an individual experiences or perceives an abuse of civil liberties and privacy in the administration of ODNI or IC programs or operations.

Likewise the National Counterterrorism Center (NCTC) is proactively providing greater transparency into how it performs its counterterrorism mission while protecting the privacy and civil liberties of the individuals whose data we access.

To this end, NCTC established a Transparency Working Group in summer 2016. Members, who are representatives of NCTC directorates and offices, collaborate on future transparency initiatives and seek to further establish transparency as a component of NCTC's normal business practices. The TWG also supports the greater Intelligence Community Transparency Council.

In addition to documents that can be posted on its public website (www.nctc.gov), NCTC is committed to a continued exchange with civil liberties and privacy advocacy groups, heritage and faith-based advocacy groups, and national security academics through outreach events.

D. Whistleblower Protection.

The DNI has recently issued Intelligence Community Directive (ICD) 120, [*Intelligence Community Whistleblower Protection*](#). ICD 120 was developed in response to the requirement in Section D of Presidential Policy Directive (PPD) 19, [*Protecting Whistleblowers with Access to Classified Information*](#), 10 October 2012, that the DNI issue policies and procedures for ensuring that all employees serving in IC elements are aware of the protections and review processes available to individuals who make protected disclosures. The ICD also clarifies that PPD 19 protects contractors from reprisal in the form of adverse decisions concerning eligibility for access to classified information based on a protected disclosure. The IC policy directs the heads of all IC elements to communicate information about the protections and review processes to their employees (including contractors serving at their elements) when they enter on duty, and to the workforce on an annual basis, and to make this information easily and readily available to their employees. In executing ICD 120, the DNI is supported by the Inspector General of the Intelligence

Community who serves as the chairman of the External Review Panel hearing whistleblower appeals and conducting outreach and training to stakeholders in the IC.

Under the *Third Open Government National Action Plan*, issued on October 27, 2015, the Director of National Intelligence committed to develop a common whistleblower training curriculum that can be adopted by all federal agencies covered under PPD 19. In coordination with other government stakeholders and civil society, the Director of National Intelligence developed the *Protecting Whistleblowers with Access to Classified Information* training curriculum to ensure that all Executive Branch employees – including contractors, managers, and supervisors – understand the roles, responsibilities, and rights of whistleblowers eligible for access to classified information.

This four-part curriculum trains personnel eligible for access to classified information to effectively report illegality, waste, fraud, and abuse while protecting classified national security information. The curriculum includes stand-alone modules that address (1) general information on whistleblowing and the process for making a protected disclosure; (2) processes for addressing adverse, retaliatory actions affecting a security clearance; (3) processes for addressing adverse, retaliatory personnel actions; and (4) best practices for managers and supervisors. The training also defines key terms and provides references for applicable whistleblower laws and policies. This training is provided as a resource for Executive Branch agencies and is intended to be customized to suit each agency's whistleblower training program.

E. Access to Scientific Data and Publications

ODNI has drafted a plan to make federally funded research publications and data available to the public and plans to use the Defense Technical Information Center (DTIC) to support this effort. The final plan, once approved by the Office of Science and Technology Policy, will be posted to the ODNI public website.

Ongoing Initiatives

F. Public Notice

The ODNI has modified the Instruction which creates the position Civil Liberties Protection Officer to include in the mandatory responsibilities outreach to the public and advocacy communities.

G. Records Management

Effective records management has been an integral part of the ODNI since it began operations in April 2005. The ODNI Records Management Program establishes policy, implements guidelines, and defines individual responsibilities to ensure records comply with federal records management statutes and regulation. It also ensures records are maintained throughout their lifecycle according to approved disposition authorities found in ODNI Records Control Schedules (RCS). Current ODNI RCS disposition authorities have been approved by the National Archives and Records Administration (NARA) and are posted on [NARAs website](#). The ODNI is currently developing a consolidated RCS that employs a big bucket file plan approach that will modernize and supersede current RCS disposition authorities. This effort will improve the records management program and comply with the [Presidential Memorandum on Managing Government Records](#) as ODNI transitions from paper-based records management to electronic records management. ODNI is developing a program to manage both permanent and temporary email records according to NARA's Capstone approach by December 2016. Government agencies are required to manage all permanent electronic records by 2019 per the Office of Management and Budget (OMB) and the aforementioned memorandum. Additionally, ODNI is currently working toward annual mandatory training for all ODNI personnel informing them of their records management responsibilities per NARA Bulletin 2017-01.

H. Freedom of Information Act (FOIA) Requests

ODNI has taken steps to apply the presumption of openness to its FOIA program. In a May 21, 2009 memorandum to the workforce, the ODNI's Chief FOIA Officer affirmed ODNI's commitment to accountability and transparency by reminding all agency employees that unless disclosure of information would harm national security, cause an unwarranted invasion of personal privacy, or impede law enforcement proceedings, openness should prevail. In this memorandum, the Chief FOIA Officer made it clear that while the FOIA office has the leading role in processing requests, every individual plays a part in ensuring full compliance with all aspects of the FOIA. The President's FOIA Memorandum and the Attorney General's FOIA Guidelines were attached to that memorandum to ensure complete understanding. The ODNI FOIA Office hosts IC FOIA Days twice a year to engage IC FOIA Officers in discussions on improving the FOIA process to ensure greatest transparency. The ODNI FOIA page contains the ODNI FOIA Handbook and regulations, information about office staffing and organizational structure, and information on how to submit a FOIA request by e-mail, in addition to links to other IC FOIA pages.

I. Declassification

The DNI's Congressionally-Directed Action Report, *Improving the Intelligence Community's Declassification Process and the Community's Support to the National Declassification Center*, was delivered to Congress on 3 January 2017.

ODNI recently published regulations regarding its Mandatory Declassification Review program.

J. Public Participation

Since the mission of ODNI is to protect and advance U.S. national security interests, and much of the work the ODNI performs is classified, the public's participation in the decision-making process of the office may be impractical. The ODNI is working with internal ODNI components and IC partners to evaluate potential security and counterintelligence issues associated with the development of more automated disclosure of ODNI information to the public in order to keep the public informed. The ODNI continues to provide to the public its guiding documents such as the *National Intelligence Strategy*, and welcomes public feedback and comments relating to any aspect of this strategy, and to its FOIA, disclosure, and declassification policies.

The ODNI recently updated the foundational document for the Civil Liberties, Privacy and Transparency Office to include language enshrining the office's current business model of regular interaction with privacy, civil liberty and transparency advocates.

K. Collaboration.

Information sharing is a key component of the DNI's strategy to better enable the IC to provide timely and accurate information to decision- makers, war fighters, and other U.S. Government departments and agencies. The ODNI has several active initiatives that enable information sharing between agencies of the U.S. Government, and state, local, and tribal governments. A key technical innovation in these initiatives is the development of a "Common Trust Environment" which would put in place uniform identity management, information security standards, user authorization, and access control to promote common trust. Similar initiatives, such as privilege management control technologies and access control pilots, are being discussed as part of the [Information Sharing Environment \(ISE\)](#).