Office of the Director of National Intelligence
Open Government Plan
2014

Introduction

The following is the 2014 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 February 24, 2014.

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 DNI supports the President's commitment to increase transparency, participation, and collaboration within the Government and with the American people, as stated in the President's 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 2014 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.

1. *High-Value Information Currently Available for Download and Collaboration*

In the interest of increased transparency, the ODNI routinely publishes information concerning the ODNI and IC on its public website. This information includes speeches, press releases, Congressional testimony, and statements for the record by the DNI and other senior ODNI officials, in various formats. The formats include 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, 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, local, and tribal 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.

2. Increase Public Knowledge and Promote Scrutiny of Agency Services

Pursuant to Executive Order 13392 and memorandums on openness issued by the President and the Attorney General, the ODNI continues to proactively 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.

Currently, the ODNI publicly releases a variety of speeches, transcripts of public testimony, documents, and press releases relating to senior staff appointments in order to inform the public of significant actions and the business of the ODNI. In addition, ODNI established the ICONTHERECORD Tumblr page and has posted, among other things, several thousand pages of declassified documents in order to better inform the public.

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. 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, also accessible by hyperlink.

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 Civil Liberties and Privacy Office (CLPO) has affirmatively undertaken to promote broader understanding regarding the incorporation of civil liberties and privacy protections into the IC's policies, procedures, and activities. CLPO 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 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. CLPO'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.

NCTC embarked on this initiative in 2012, when it publicly posted its revised Attorney General Guidelines, drafted at the unclassified level, in part so that it could be disclosed to the public. NCTC published a mission justification paper explaining the need to revise the Guidelines, and also a white paper explaining the civil liberties and privacy protective features of the new Guidelines.

NCTC continues to look for additional ways to provide transparency to the public, balancing the commitment to openness with the need for security. To this end, NCTC has held several outreach events, e.g., a symposium for civil liberties and privacy advocacy groups, heritage and faith-based advocacy groups, and national security academics in July of 2013, and on May 5, 2014, a second session with a number of these advocacy groups, led by the Director of NCTC, Hon. Matthew G. Olsen. In addition, NCTC publishes relevant documents to its website from time to time (see URL at Section E).

Going forward, NCTC continues to explore avenues for providing transparency, e.g., documents that can be posted on its public website, topics that might lend themselves to the creation of white papers, and continued exchange with the public and advocacy communities.

D. Whistleblower Protection.

The DNI 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.

E. Websites and Social Media.

As mentioned above, ODNI routinely posts material to both www.dni.gov and ICONTHERECORD.tumblr.com.

The Office of the Program Manager for the Information Sharing Environment also maintains a public website and blog at www.ise.gov and active accounts on Twitter, Facebook, and LinkedIn. The accounts are used to share information with federal, state, local, tribal, private sector, and international partners about ongoing programs and initiatives, government and industry best practices, and information sharing and safeguarding success stories.

Ongoing Initiatives

A. Records Management.

Since the ODNI began operations in April 2005, the ODNI Records Management program has been working with the National Archives and Records Administration (NARA) to create ODNI Records Control Schedules. The Records Management Office has drafted over 90% of the schedules and has submitted them to NARA. Draft schedules have been completed for various components of the ODNI, including the NCTC, the largest organization within the ODNI. A portion of the draft schedules have also been published in the Federal Register for public comment. The office is currently hosting appraisal visits from NARA staff and providing answers to their questions on technology issues. These responses will assist NARA with their evaluation of the ODNI's electronic records management program.

B. Freedom of Information Act Requests.

ODNI has taken steps to apply the presumption of openness to its FOIA program. 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 addition, the Chief FOIA Officer made 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 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.

C. 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 internally and with 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 its guiding documents to the public, 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 polices.

D. 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" that would put uniform identity management, information security standards, user authorization, and access control in place to promote common trust. Similar initiatives, such as privilege management control technologies and access control pilots, are under discussion as part of the Information Sharing Environment (ISE).

Additional information relating to the ODNI and IC information sharing initiatives and the ISE may be found at these sites.

<u>Flagship Initiatives</u>

A. IC On The Record Tumblr site

Created at the direction of the President, ICONTHERECORD provides immediate, ongoing, and direct access to factual information related to the lawful foreign surveillance activities of the U.S. IC. In addition to comprehensive explanations of the authorities under which the IC conducts certain foreign surveillance, ICONTHERECORD addresses the use of collected data and oversight and compliance. It is an unclassified online repository for declassified official documents, statements, and speeches that members of the public can reference to inform their thinking about surveillance issues. The aims of ICONTHERECORD are to increase transparency and build the public trust through openness and education.

B. NCTC Transparency Initiative

As discussed above, in 2013, NCTC proactively posted a number of documents on its website, including its 2012 revised Attorney General Guidelines, a mission justification fact sheet, and an ODNI CLPO white paper explaining the civil liberties and privacy protection features of the new Guidelines.

In April 2014 NCTC posted three additional documents on its website, all designed to provide greater insight into how NCTC accesses, uses, and protects data under its

stewardship. Specifically, NCTC posted:

- A white paper overview of NCTC's Data Access under its 2012 Attorney General Guidelines, detailing the categories of data that NCTC replicates, as well as how this data is used by NCTC to fulfill its counterterrorism mission;
- NCTC's first annual report (redacted) to the ODNI OGC and CLPO, and the IC Inspector General (redacted), on NCTC's access, retention, use, and dissemination of non-terrorism datasets, as required under NCTC's revised 2012 Attorney General Guidelines; and
- The Memorandum of Agreement between Department of Homeland Security (DHS) and NCTC (redacted) allowing NCTC to gain bulk access to DHS APIS travel data for up to 1 year.

In May 2014 NCTC posted additional transparency documents on its website:

- A white paper that describes how NCTC has implemented Baseline Safeguard protections mandated by its Attorney General Guidelines, as well as the compliance checks and audits of NCTC's adherence to those safeguards;
- The decision matrix used by NCTC in assessing each replicated non-terrorism dataset for potential application of additional Enhanced Safeguards, over and above the Baseline Safeguards; and
- NCTC's Compliance Incident Procedures for reporting, assessing, investigating, and resolving compliance incidents relating to NCTC's handling of data.