

# PRINCIPLES OF INTELLIGENCE TRANSPARENCY **IMPLEMENTATION PLAN**



OCTOBER 27, 2015

# The Implementation Plan for the Principles of Intelligence Transparency

## The Principles of Intelligence Transparency

---

In February 2015, the Director of National Intelligence (DNI) published the Principles of Intelligence Transparency for the Intelligence Community (Principles). These Principles are intended to facilitate Intelligence Community (IC) decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security. There are four Principles:

- 1) Provide appropriate transparency to enhance public understanding of the IC
- 2) Be proactive and clear in making information publicly available
- 3) Protect information about intelligence sources, methods, and activities
- 4) Align IC roles, resources, processes, and policies to support transparency implementation

To be transparent, as provided by the Principles, the IC must institutionalize a strategic, coordinated, and proactive approach to inform and enhance the public's understanding of the IC, its activities, and its governance framework. Transparency includes not only sharing information about the rules that apply to the IC and its compliance under those rules, but also sharing information about what the IC actually does in pursuit of its national security mission.

To be effective, this strategic approach to transparency must account for the new and changing ways in which information is communicated. While it is critical for the IC to continue to respond to Freedom of Information Act (FOIA) requests and to execute other disclosure responsibilities as expeditiously as possible, the IC must also make information available through other channels that the public uses. Therefore, the IC should communicate with the public through social and traditional media, direct engagement with external stakeholders, and participation in academic and other conferences and deploy a broader range of communicators.

Transparency efforts must first be guided by the vital responsibility the IC has to protect intelligence sources, methods, and activities from unauthorized disclosure. In light of rapidly evolving and complex threats to the nation's security, the need for timely and reliable intelligence has never been greater. The IC can only be effective at protecting against those threats if intelligence sources, methods, and activities remain unknown to our adversaries. Because informing the public inevitably includes the unintended consequence of informing the

nation's adversaries as well, the IC must find a way to enhance transparency while continuing to preserve the nation's secrets.

Finally, in an era of increasing demands and declining budgets, the IC must devote the necessary resources to enhance transparency while also executing its vital national security duties. This requires clarity and well-defined roles and responsibilities among the offices of general counsel, civil liberties and privacy, public affairs, information management, and others that are responsible for information classification, declassification, release, and publication decisions.

## Background: The Transparency Imperative

---

On his first day in office, President Obama signed a Memorandum on Transparency and Open Government, and in October 2009, the White House issued an unprecedented Open Government Directive requiring federal agencies to take specific steps to achieve key milestones in transparency, participation, and collaboration. Like the rest of government, transparency is an imperative for the IC.

This imperative has since been underscored by President Obama, who stated in his national security speech on January 17, 2014, “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...we will reform programs and procedures in place to provide greater transparency.” And in June 2014, the DNI instructed the ODNI's Civil Liberties Protection Officer to coordinate the development of a new strategic approach to intelligence transparency as part of the imperative and to earn and retain public trust. The significance of increased transparency was also reflected in the 2014 National Intelligence Strategy, which called upon the IC to “continue to implement approaches to provide appropriate transparency.”

In recent years, the IC has made major strides toward enhancing transparency. For example:

- The ODNI established *IC on the Record* as a repository for declassified documents, official statements, speeches, and testimony. *IC on the Record* has published over 5,000 pages of officially released documents.
- The ODNI, in coordination with IC elements, published a detailed report describing the measures taken to implement intelligence reforms in the year since the President's January 2014 speech. The report included links to IC elements' policies specifying how they will safeguard personal information collected via signals intelligence activities, regardless of nationality, consistent with section 4 of Presidential Policy Directive (PPD) 28 Signals Intelligence Activities.

- The IC facilitated oversight by the Privacy and Civil Liberties Oversight Board by conducting intensive classification and declassification reviews of sensitive information to support the Board in publishing comprehensive descriptions of intelligence activities under the Foreign Intelligence Surveillance Act (FISA).
- The IC prepared and published two annual statistical transparency reports that presented data on the use of key surveillance authorities. In addition, the IC reached agreement with providers so that they can publish statistics on the national security orders they receive.
- The IC publicly supported the passage of the USA FREEDOM Act, which includes additional transparency requirements that the IC will be implementing over the coming year.
- IC officials participated in a wide range of public engagements, including speeches, media interviews, panel discussions, and meetings with civil society and other external stakeholders.
- IC offices carefully reviewed and responded to large numbers of FOIA requests and conducted Pre-Publication Reviews of official information, resulting in the authorized release of substantial volumes of information.

Although these efforts represent an unprecedented increase in intelligence transparency, the IC recognizes that more work remains to be done in order to fully institutionalize the Principles. Moreover, the IC's transparency efforts have contended with multiple challenges, including:

- A dramatic increase in external requests for information and documents, which has strained resources.
- New and persistent public narratives about intelligence activities based on unauthorized disclosures that often lack context and reflect an incomplete or erroneous understanding of the IC and its governance framework.
- Many of the documents that the IC releases to the public are highly technical and lack the context necessary for clarity and broader public understanding.

Thus, while large volumes of information have been officially released, the public's understanding of the IC remains incomplete in many ways. A strategic approach to transparency will enable the IC to more actively participate in the public discussion on the role of intelligence in protecting national security.

## Approach: Institutionalizing Transparency

---

To begin the pioneering effort of developing a new strategic approach to intelligence transparency as directed by the DNI in 2014, the ODNI Civil Liberties Protection Officer established and chaired the Intelligence Transparency Working Group (ITWG), comprising cross-functional representatives from nearly all of the IC elements. Given the broad scope of the task at hand, the ITWG divided its work into two phases. In phase one, the ITWG developed high-level Principles to provide general transparency guidance for the IC. This was completed in February 2015. In phase two, the ITWG developed this implementation plan for the Principles.

To earn and retain public trust and ensure accountability, the IC must institutionalize transparency. In large part, this implementation plan addresses a cultural reform that seeks to transition a community predisposed to making little information public into a community resolved to engage in greater public transparency. The obligation rests with the IC as a community to establish how to institutionalize transparency, while protecting intelligence sources, methods, and activities from unauthorized disclosure. As the IC determines how to do so, it is important to bear in mind that neither the Principles nor this implementation plan modify or supersede applicable laws, executive orders, and directives, including Executive Order 13526.

## Approach: Developing the Transparency Implementation Plan

---

From the outset, the ITWG recognized that developing an IC-wide plan for implementing the Principles presented an integration challenge. Accordingly, the group developed the plan based on the Unifying Intelligence Strategy (UIS) framework, which is used to integrate IC efforts on a given subject area by identifying priorities, gaps, and challenges and proposing specific initiatives. The UIS, a “living document,” is reviewed and updated on a regular basis. It facilitates interagency coordination to provide guidance to—and be continuously informed by—the IC in order to achieve integration goals in a coordinated and efficient manner.

Like a UIS, this implementation plan reflects the collective efforts of IC members. It will be used to guide the IC’s efforts to achieve the common strategic goal of enhanced transparency and will remain responsive to change.

Set forth below is a general description of the gaps and challenges in achieving transparency. This is followed by a specific listing of priorities and initiatives for each of the four Principles.

## Transparency Implementation Gaps and Challenges

---

Gaps are capabilities, capacities, policies, or processes that are *not in place* but that are necessary to support the realization and practice of transparency in the current working environment. The most prominent gaps, as identified by the ITWG, were noted as:

- Workforce understanding of the IC's approach to transparency and the public's expectations for transparency.
- Processes to identify and prioritize appropriate transparency topics.
- Consistent and coordinated determinations on the categories of information to be made public and the processes for communicating that information.
- Defined internal and interagency processes — guidance on how offices such as FOIA, general counsel, civil liberties and privacy, public affairs, and information management should interact to integrate transparency within and across the IC.
- Appropriate staffing and training to support transparency initiatives.

Often corresponding to, but distinct from the gaps, challenges are issues that *impede* transparency efforts in the current working environment. The most prominent challenges, as identified by the ITWG, were noted as:

- Adapting the IC culture to one of enhanced transparency.
- Continuing to protect intelligence sources, methods, and activities from unauthorized disclosure while seeking to enhance transparency.
- Preserving trusted relationships with entities the IC relies upon to accomplish its mission, including foreign partners.
- Resource constraints and complications in implementing transparency initiatives, and in reviewing and clearing content for public release.
- Lack of trained personnel in specific areas necessary to successfully implement transparency initiatives.

Once the ITWG had identified the obstacles tied to transparency, the group then determined transparency priorities.

## Transparency Implementation Priorities and Initiatives

---

In order to institutionalize transparency, the ITWG recognized that public transparency must be executed in a manner consistent with the IC's core mission of protecting national security. Therefore, to be effective, institutional transparency must be grounded in priorities that are

carefully identified in light of the IC's responsibility to protect intelligence sources, methods, and activities.

Priorities identify areas in which the IC should concentrate efforts based on their importance in achieving the overall strategic goal of transparency. Priorities also reflect assessments of feasibility. In sum, priorities provide the highest return on the investment of time, attention, and resources. The ITWG identified two or three priorities for each of the four Principles.

Once priorities were identified, the ITWG identified initiatives that best support and realize those priorities. The ITWG first considered efforts already underway that could be expanded or improved. Though not widely recognized, and not always integrated, longstanding efforts are currently being undertaken by the IC to promote transparency and share information with the public. The ITWG reviewed the extent to which existing efforts could be leveraged into IC-wide initiatives.

In addition, the ITWG considered proposals for new initiatives to address priorities that did not appear to be met by current activities. The ITWG focused on the most viable options for establishing a strong and enduring foundation of transparency. All initiatives must be assessed to ensure that the proper resources, tools, and mechanisms are in place to facilitate transparency. Such assessments would include the means necessary to measure performance and hold organizations accountable in their efforts to achieve transparency.

The priorities and initiatives for the implementation plan are listed below beneath each of the Principles they support.

# The Transparency Implementation Plan

---

## **PRINCIPLE 1: Provide Appropriate Transparency to Enhance Public**

### **Understanding about:**

- a. the IC's mission and what the IC does to accomplish it (including its structure and effectiveness);
- b. the laws, directives, authorities, and policies that govern the IC's activities; and
- c. the compliance and oversight framework that ensures intelligence activities are conducted in accordance with applicable rules.

Principle 1 refers to the “what” of transparency—what should the IC be transparent about? It addresses two general areas. First, the IC should be transparent about its governance framework—the rules, authorities, compliance mechanisms, and oversight that guide its activities. Second, the IC should provide more insight into its mission, supported by appropriate information on how it accomplishes that mission.

### **Priority 1.1 - Provide more information about the IC's governance framework.**

A great amount of time and effort has already been expended to review and release information about the IC's governance framework in a way that recognizes the need for secrecy in intelligence operations. These efforts should continue and be adopted across the IC to support public understanding of the rules that govern IC activities and the oversight mechanisms in place to ensure compliance. Providing such information will also enhance the ability of external oversight entities to publicly describe their functions and findings. Current efforts include:

- ✓ Facilitating release of certain legal and oversight documents relating to intelligence surveillance under the FISA, including opinions and orders of the Foreign Intelligence Surveillance Court (FISC), procedures approved by the FISC, and FISA compliance reports.
- ✓ Publication of key policies and procedures, such as those implementing PPD-28, Attorney General (AG)-approved guidelines under Executive Order 12333, and unclassified Intelligence Community Directives (ICDs).
- ✓ Publication of annual transparency reports providing statistics on the use of key national security authorities, and agreement with providers on their release of statistical information (statistical transparency requirements are now embodied in the USA FREEDOM Act).

Building on these existing efforts, potential initiatives include:

- ✓ *Information on Governance Framework.* Consistent with the protection of intelligence sources, methods, and activities, IC elements should provide information to the public that explains the rules they operate under, their compliance with those rules, and their oversight mechanisms. As part of this effort, IC elements should describe, in understandable terms, their governance framework and release certain corresponding legal and policy documents, such as policies, guidelines, procedures, and reports consistent with the protection of intelligence sources, methods, and activities.
- ✓ *Institutionalization through Process.* Because different offices are involved in transparency decisions, such as general counsel, civil liberties and privacy, public affairs, and information management, the IC must establish a process to effectively coordinate the identification and publication of legal, policy, compliance, and oversight information.

### **Priority 1.2 - Provide more information about the IC's mission and activities.**

The IC has been transparent about its general mission and has undertaken substantial transparency efforts in certain areas, and those efforts can be leveraged to provide more details on intelligence while protecting intelligence sources, methods, and activities. For example:

- The CIA's Historical Collection Program, which released documents highlighting the intelligence support provided on matters such as Bosnia and Berlin in the Cold War, and to leaders such as President Carter during the Camp David Accords.
- The ODNI public release of the "Bin Laden's Bookshelf" documents collected during the Abbottabad raid.
- The NGA's public sharing of geospatial imagery in response to humanitarian and environmental crises.

Building on those efforts, the IC should focus on providing additional information to the public regarding its mission and activities that go beyond its governance framework, such as:

- ✓ *Information of Public Utility.* The IC should review and provide appropriate information that is of current public utility, such as certain types of foundational information (including imagery). To facilitate the foregoing, the IC should develop a repeatable process of moving unclassified material not subject to other statutory protections to unclassified systems where it may be released.
- ✓ *Historical Information of Current Relevance.* Information on a topic that has been of public interest and that will shed light on current issues, such as the documents collected at Abbottabad.

- ✓ *Institutionalization through Process.* Given the sensitivity of information about intelligence activities, it is particularly important that determinations of what to release in this area be coordinated and consistent. Such processes will ensure that different IC department or agency views are appropriately taken into account as part of release determinations.

### **Priority 1.3 - Establish common criteria for identifying transparency priority topics.**

The IC must seek both to accomplish overarching national security imperatives and provide information in the public interest, and do so with limited resources. It is important, therefore, to establish common criteria for identifying specific topics on which to focus the IC's transparency-related efforts. These criteria must include assessments of the topics that would enhance the public's understanding of intelligence, along with considerations of what is achievable given available resources and the sensitivity of underlying information that warrants continued protection of intelligence sources and methods.

For example, as noted above, an identified priority is sharing information on the IC's governance framework relating to certain intelligence surveillance authorities and activities. It is evident that the time and resources allocated to this effort are justified by its importance as a matter of public debate. What broader lessons can be drawn from this current experience and applied to IC-wide efforts to identify transparency topics?

In light of the foregoing, potential initiatives include:

- ✓ *Criteria for Identifying Transparency Topics.* Offices currently working on transparency should define criteria for selecting and prioritizing transparency topics, considering views from inside and outside the IC.
- ✓ *Prompt Identification of Priority Topics.* These criteria should promptly be applied to a range of topics suggested by sources inside and outside the IC, including civil society, intelligence partners, and oversight entities. Priority topics should be determined through an interagency process that includes a coordinated approach for publicly releasing information on that topic.

**PRINCIPLE 2: Be proactive and clear in making information publicly available through authorized channels, including taking affirmative steps to:**

- a. provide timely transparency on matters of public interest;
- b. prepare information with sufficient clarity and context, so that it is readily understandable;
- c. make information accessible to the public through a range of communications channels, such as those enabled by new technology;
- d. engage with stakeholders to better explain information and to understand diverse perspectives; and
- e. in appropriate circumstances, describe why information cannot be made public.

Principle 2 is the “how” of transparency—how should information that can educate the public on intelligence be made available to the public? This Principle’s focus is to ensure that information on and about the IC is accessible, understandable, contextualized, available through multiple channels, and, where appropriate, presented in a manner that encourages feedback.

**Priority 2.1 - Share information with the public through multiple platforms; encourage public engagement.**

The IC typically publishes information by posting material on its websites, or by supporting other organizations’ efforts to prepare public reports. For example, the IC works closely with review and oversight entities, including congressional committees, the Privacy and Civil Liberties Oversight Board, and the President’s Review Group on Intelligence and Communications Technologies. In addition, in recent years, IC leadership and subject matter experts have increased their engagement with civil society and participation in public forums. These engagement opportunities, however, have been largely ad hoc in nature. Taking a strategic, coordinated, and proactive approach to providing information will help ensure that important information is available through the diverse channels used by the public.

In light of this approach, potential initiatives include:

- ✓ *Online Portal.* The ODNI should establish [www.intelligence.gov](http://www.intelligence.gov) as the primary portal for the IC’s publicly posted electronic information. This hub would provide a single venue to present IC-wide information, including readily understandable public descriptions of the IC’s mission and activities and the IC’s governance framework. This portal would link to other relevant IC websites—including that of the IC elements—so that the public has a single point of entry to clear and accurate information about the IC.

- ✓ *Website Content Checklist.* In conjunction with the above, the IC should develop and implement a website checklist to ensure that IC element websites provide readily understandable information on key topics, such as descriptions of the element's mission, strategic goals and objectives, the role it plays within the IC, and its governance framework (including policies, procedures, guidelines, and compliance/oversight reports).
- ✓ *Diverse Representatives.* The IC should tap into the diverse IC workforce to help communicate with the public, and ensure that a broader range of intelligence professionals have a role in public communications. To achieve this goal, training must be provided to the IC workforce to better prepare them for interactions with the public while ensuring the protection of both operational intelligence and information concerning intelligence sources, methods, and activities. In addition, the IC should clarify and streamline review and approval processes so that the intelligence professionals involved fully understand the authorized channels to follow for any such interactions (further discussed below).
- ✓ *Engagement Strategy.* An IC office experienced in transparency and designated as the lead, should develop and implement a strategic, coordinated approach for direct engagement with external stakeholders, including the media, civil society, oversight entities, and foreign partners. Many such engagements would (and should) continue to be ad hoc and driven, for example, by external invitations. However, to ensure the IC is undertaking effective transparency initiatives in appropriate forums, and that feedback is obtained systematically, the IC should also affirmatively structure and coordinate such engagements.
- ✓ *Open Government.* Open Government initiatives focus on transparency in order to increase public input and ensure more government accountability. These initiatives dovetail naturally with the IC's commitment to enhance transparency, and provide an opportunity to align intelligence transparency efforts with those of other government agencies. Accordingly, the IC should develop an IC-wide plan for Open Government consistent with authorities and equity interests.
- ✓ *Expand Use of Social Media.* The IC has already made strides in using social media to communicate with the public. Examples include ODNI's use of the Tumblr blogging platform to host *IC on the Record*, and IC elements' use of Twitter and Facebook accounts. To facilitate expanded social media use, IC elements should identify and share best practices, including how to be more transparent while maintaining necessary operational security. In addition, the ODNI should lead a process to identify and update applicable processes and guidelines, so that social media use can become fully integrated in each IC element's public communications efforts.

**Priority 2.2 - Ensure authorized channels are appropriately used to share information with the public.**

While the IC is committed as an institution to enhancing transparency, each intelligence professional retains the responsibility for understanding and implementing existing guidance regarding information sharing with the public and being fully cognizant of counterintelligence concerns. IC elements have established authorized channels for communicating with the public. These channels help ensure that accurate information is provided in a manner that safeguards classified and statutorily protected information.

In light of the foregoing, potential initiatives include:

- ✓ *Review and Update Processes.* IC element processes for authorizing communications with the public should be reviewed and updated pursuant to applicable policy to ensure alignment with the Principles. Appropriate individuals and offices that are authorized to engage in public communications should be clearly identified. The process for authorizing particular individuals to engage in specific public communications should be streamlined according to applicable policy, and appropriate training, guidance, and support should be provided to such individuals.
- ✓ *Workforce Communication.* IC elements should clearly communicate policies and processes on the use of authorized channels to the workforce, including authorized channels for communicating with the public, requesting declassification review, and submitting concerns or observations on potential misconduct by IC offices or employees.

**PRINCIPLE 3: In protecting information about intelligence sources, methods, and activities from unauthorized disclosure, ensure that IC professionals consistently and diligently execute their responsibilities to:**

- a. classify only that information which, if disclosed without authorization, could be expected to cause identifiable or describable damage to the national security;
- b. never classify information to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment;
- c. distinguish, through portion marking and similar means, classified and unclassified information; and
- d. consider the public interest to the maximum extent feasible when making classification determinations, while continuing to protect information as necessary to maintain intelligence effectiveness, protect the safety of those who work for or with the IC, or otherwise protect national security.

Principle 3 addresses the ongoing responsibility of the IC and each intelligence professional to protect intelligence sources, methods, and activities from unauthorized disclosure, which includes an awareness of counterintelligence concerns. It highlights the provisions in existing classification directives and policies that would support enhanced transparency through consistent and diligent execution of the proper classification of intelligence. As such, Principle 3 reinforces Executive Order 13526, which governs classification standards, while also guiding the IC to consider the public interest to the maximum extent feasible in conducting declassification reviews in order to make as much information available as possible while protecting intelligence information.

**Priority 3.1 – Ensure that the IC workforce understands proper classification practices and how they relate to enhancing transparency.**

The IC's efforts to institutionalize transparency can only be effective in practice through the support of a trained and educated workforce. Training is essential to inform the workforce of the importance of coordinated transparency and to highlight how the diligent and consistent execution of existing classification guidance is aligned with transparency goals. Inaccurate or incomplete portion markings (classification) can have significant downstream consequences, requiring those involved in a particular transparency process—such as FOIA—to expend considerable time and effort to determine the proper classification of the material in question. In making classification determinations, IC elements should consistently follow approved guides and, when in doubt, use the lowest classification level.

In light of the need for enhanced education, potential initiatives include:

- ✓ *Update Classification and Related Training.* IC elements should update classification training to emphasize the diligent and consistent execution of classification responsibilities, consistent with Principle 3. This should include, as appropriate, modules on the transparency-related provisions of EO 13526 (Classified National Security Information); ICD 710 (Classification Management and Controls Marking System); writing at lower classification levels (Write for Release); ICD 208 (Writing for Maximum Utility); ICD 209 (Tear line Dissemination); ICD 119 (Media Contacts); and ICD 120 (Whistleblower Protection).
- ✓ *Workforce Events to Discuss Transparency.* ODNI should work with appropriate offices across the IC to prepare and deliver workforce events to highlight the importance of transparency, and to answer questions on a topic that may elicit strong feelings.

### **Priority 3.2 - Enhance interagency coordination on classification, declassification, and release practices among information management professionals.**

The burden of recent transparency efforts has been borne by the information management professionals who are responsible for responding to FOIA requests, conducting declassification reviews, developing and implementing classification guidance and training, and the like. Although progress has been made, enhancing interagency coordination through a referral/consultation process would help ensure that determinations are made that take all relevant considerations into account.

In light of the foregoing, potential initiatives include:

- ✓ *Support and Update FOIA Processes.* IC elements should further support their FOIA-related functions to enhance transparency. The ODNI is participating in a FOIA pilot involving the publication of FOIA-released information on [www.dni.gov](http://www.dni.gov), and, if successful, this practice should be followed by other IC elements. IC elements should also consider streamlined processes for communicating with FOIA requestors about the status of their requests, and about informing the public of FOIA procedures. In addition, the ODNI should lead an interagency process within the IC to improve FOIA-related coordination and information sharing.
- ✓ *Provide Classification Guidance as part of the Fundamental Classification Guide Review.* The ODNI should work with the Information Security Oversight Office to provide guidance to IC elements on updating classification guides. This guidance should be aligned with the Principles as appropriate.

**PRINCIPLE 4:** Align IC roles, resources, processes, and policies to support robust implementation of these principles, consistent with applicable laws, executive orders, and directives.

Principle 4 directs IC elements to make the changes necessary to implement the Principles.

**Priority 4.1 - Clearly delineate transparency roles and responsibilities.**

Individual IC elements have their own internal organizations and processes that are involved with transparency decisions. Transparency decisions typically involve offices of general counsel, civil liberties and privacy, information management, FOIA, and public affairs. While these offices work hard to provide transparency, it is not always clear which should take the lead or to what extent other offices must be included. It is important, therefore, to clarify and align roles and responsibilities.

In light of the need for organizational clarity, potential initiatives include:

- ✓ *Transparency Officers/Coordinators.* IC elements should establish transparency coordinator/officer positions. These positions should have sufficient seniority and access to information and resources to facilitate coordination of all relevant IC offices on particular transparency matters. In addition, such positions should work with counterparts across the IC, under the leadership of the ODNI, to carry out the tasks outlined in this implementation plan.
- ✓ *Other Roles and Responsibilities.* Transparency officers should work with the offices of general counsel, civil liberties and privacy, public affairs, information management, FOIA, and other related offices, to delineate the respective roles and responsibilities of those offices on different types of transparency matters and to find ways to support and enhance their effectiveness while avoiding duplication of effort. Such offices should designate one or more transparency points of contact to work with transparency officers. In addition, the transparency officers should establish a baseline for metrics to evaluate the successful implementation of transparency across the IC.

#### **Priority 4.2 - Institutionalize transparency policies and procedures.**

Different aspects of transparency are reflected in a range of IC policies and procedures. It is important that these policies and procedures are aligned with the Principles. In addition, the various offices currently participating in transparency decisions may have existing procedures in place for interacting with counterparts at other IC elements, so institutional transparency requires close collaboration within IC elements as well as between them.

In light of the need for consistent application, potential initiatives include:

- ✓ *Establish Repeatable Processes.* Relevant intra- and interagency processes must be identified, streamlined, and updated to ensure alignment with the Principles. In particular, interagency coordination processes should be reviewed and updated for transparency. The goal should be to integrate and streamline the input of relevant offices within IC elements.
- ✓ *Intelligence Transparency Council.* The ODNI should establish an Intelligence Transparency Council, consisting of the transparency officers of the IC elements. The Council should serve as a forum that facilitates interagency coordination, identifies and addresses key issues, reviews the progress and guides implementation of the plan, and regularly updates the plan as a living document. This Council shall also be supported by a working group of counterintelligence professionals drawn from organizations across the IC to ensure that transparency efforts do not provide any insight or expose IC vulnerabilities, sources, methods, capabilities, operations, or partnerships to adversaries.