



## PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE INTELLIGENCE COMMUNITY

The Principles of Intelligence Transparency for the Intelligence Community (IC) are intended to facilitate 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. These Principles do not modify or supersede applicable laws, executive orders, and directives, including Executive Order 13526, Classified National Security Information. Instead, they articulate the general norms that elements of the IC should follow in implementing those authorities and requirements.

### **The Intelligence Community will:**

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