
DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 8/1

INTELLIGENCE COMMUNITY POLICY ON INTELLIGENCE INFORMATION SHARING

(EFFECTIVE: 4 JUNE 2004)

This directive is promulgated pursuant to sections 102 and 103(c) of the National Security Act of 1947, 50 U.S.C. § 403 (as amended); Executive Order 12333, United States Intelligence Activities, 4 December 1981; and Executive Order 12958, Classified National Security Information (as amended), 25 March 2003. Applicable provisions of DCID 1/1 (19 November 1998) are included by reference.

A. PURPOSE

This directive establishes Director of Central Intelligence (DCI) policy to maximize intelligence information sharing, identifies key policy elements that will govern implementation of the policy by members of the Intelligence Community (IC), and assigns responsibilities for ensuring that the policy is effectively carried out Community-wide.

B. POLICY

1. IC Information Sharing Policy

It is DCI policy that the broadest possible sharing of intelligence information is fundamental to the mission of the IC. All IC members are hereby directed to put this policy into practice by developing supporting policies, procedures, processes, and training needed to achieve the maximum degree of information exchange among IC agencies, with our customers, and with our foreign partners. This policy will be implemented consistent with the DCI's statutory responsibility to protect intelligence sources and methods from unauthorized disclosure. We will share, and we will protect sources and methods.

The overarching imperative for the IC is to provide intelligence information in a way that maximizes its value to the customer—intelligence sharing will be the rule rather than exception. All IC agencies will provide intelligence information at the earliest point at which customers can understand and effectively use it to support their mission objectives and will, whenever possible, separate intelligence content from sensitive sources and methods, while still providing customers with sufficient context and background.

IC agencies will forge close working partnerships with customers, and will use customer requirements as the basis for need-to-know determinations. Customers, in turn, will ensure that access to intelligence information is limited to those who need it. The IC agencies will collaborate closely and share information freely to ensure the best overall product for the customers; invest in and deploy information technology (IT) systems and adopt standards that support secure sharing; and educate their work forces on DCI policy and supporting information sharing practices. Supplements to this directive will provide detailed implementation guidelines on specific aspects of information sharing.

2. Key Policy Elements

Accordingly, all IC members will

Improve Customer Relationships. The quality and utility of intelligence depend heavily on an understanding by IC agencies of customer needs, plans, and intentions, and a corresponding appreciation by customers of the strengths and limitations of intelligence capabilities. To achieve this mutual understanding, IC members will forge close working partnerships with customers using a variety of approaches including exchanges of personnel, collaborative activities, and the maximum exchange of intelligence information through interoperable information systems and shared databases.

Maximize Production of Intelligence at Multiple Security Levels. To better support mission needs and protect sensitive sources and methods, IC organizations will provide intelligence at multiple security levels appropriate to the security authorizations of the intended recipients. Depending on circumstances, a variety of techniques will be used to achieve this goal, including "write-to-release," use of tearlines, and content management and tagging approaches. Supplementary guidance to this basic policy will provide specific guidance on approaches, procedures, and techniques for increasing the volume of intelligence disseminated at multiple security levels.

Expand Collaboration Across the Intelligence Community. Experience has demonstrated that, when multiple data sources, collection techniques, and analytic viewpoints are brought to bear on a problem, the result is improved intelligence support; the whole can indeed be greater than the sum of its parts. IC agencies will enhance efforts to collaborate and ensure that such efforts are based on purposeful, open, and consistent information exchanges.

Apply Need-to-Know. Intelligence information exchanges are governed by the principle of need-to-know as defined in Executive Order 12958. Need-to-know demands not merely that customers receive only what they need, but also that they receive all the information they need to carry out their missions. To effectively implement this directive, IC agencies must work cooperatively with customers to understand their requirements and ensure that they receive all applicable intelligence information while minimizing the risk of unauthorized disclosure. Customers, in turn, will be responsible for ensuring the application of need-to-know within their organizations.

Manage Risk. Balancing the goal of greater intelligence information sharing with the need to protect sources and methods requires IC members to apply a risk management methodology. This policy must be implemented in ways that balance the risk of unauthorized disclosure of sources and methods against the imperative to provide the most useful and responsive intelligence. The information needs of the customer must be given important weight in this risk management determination.

Invest in Information Technology. All IC agencies will invest in and deploy IT systems and adopt standards that support secure sharing of intelligence information within the Community and with customers. Categories of investments include tools and systems that support sharing of intelligence at multiple security levels, cross-Community collaboration, uniform and implementable content management techniques, and improved information assurance. All new IC systems, whose mission involves secure information sharing and collaboration with other IC organizations and customers, will utilize the Intelligence Community System for Information Sharing (ICSIS) enabled infrastructure and IC Enterprise Architecture (EA) common policies, services, and standards to ensure compliance of their mission system architecture and implementation with the Community's enterprise architecture.

Educate the Work Force. Effective implementation of this directive across the IC requires a committed training, education, and acculturation effort that results in a complete, common, and consistently applied understanding of this policy. The IC members will educate their work forces on up-to-date information sharing policies and practices to effect implementation of this policy consistent with accomplishment of mission objectives.

C. RESPONSIBILITIES

The Deputy DCI for Community Management (DDCI/CM) is responsible for ensuring that IC policies, procedures, and processes support this policy. The Special Assistant for Information Sharing, whose specific responsibilities are set forth below, will serve as the DDCI/CM's agent in carrying out these functions.

National Foreign Intelligence Program Managers and Senior Officials of the Intelligence Community will ensure that this directive is implemented in their organizations, that they provide their work forces with the necessary training and tools to carry it out, that supporting goals, objectives, and measures are included in strategic and performance plans, that the resources necessary to achieve these goals are included in programs and budgets, that information systems and associated business processes conform to the IC enterprise architecture, and that subordinates are held accountable for supporting this policy and carrying out the steps required to implement it.

The Special Assistant to the DDCI/CM for Information Sharing (SA/IS) is responsible for improving information sharing across the IC and with customers. The SA/IS will coordinate all intelligence information sharing initiatives and identify policy, technology, and business process issues requiring leadership attention to the DCI through the Intelligence Community Deputies Committee and the Program Managers. The SA/IS will establish performance measurements for improved information sharing, track progress against those metrics on a regular basis, and report regularly (at least annually) to the DDCI/CM and the DCI on progress made in implementing this directive. This report will include recommendations for needed actions, to include resource adjustments if required.

The Assistant Directors of Central Intelligence (ADCI) for Analysis and Production and for Collection will ensure that collaborative Community processes are used for the collection and production of intelligence. In addition, the ADCIs will provide assessments to the DDCI/CM Special Assistant for Information Sharing for inclusion in reports to the DDCI/CM and the DCI on progress made in their respective domains in implementing this policy.

The Intelligence Community Chief Information Officer (IC CIO) will ensure that the IC enterprise architecture, associated business processes, and IT security practices support efficient and effective information exchange across the Community and with our customers and partners as called for in this policy. In addition, the IC CIO will coordinate plans and actions with counterparts in the IC and customer organizations.

The Director of the DCI's Special Security Center will review all security-relevant DCI Directives and supporting policies, processes, and procedures to ensure that they support the sharing of intelligence information within the IC and with other departments and agencies that process or hold Sensitive Compartmented and other intelligence information.

The Director of the Terrorist Threat Integration Center (TTIC) is responsible for managing a structure that institutionalizes sharing of terrorist threat-related information across appropriate federal agency lines in order to form the most comprehensive possible threat picture and minimize any seams between analysis of terrorist threat-related information collected domestically or abroad.

The Special Assistant to the DCI for Foreign Intelligence Relationships is responsible for working with IC agencies to ensure that collaboration and information exchanges with foreign intelligence partners are conducted in accordance with this and other relevant policies.

D. DEFINITIONS

Content Management. The process of capturing and creating, managing and storing, and delivering the substantive details of structured and unstructured data.

IC Enterprise Architecture (IC EA). The IC EA is the DCI's information technology enterprise architecture and enabling infrastructure that will provide for the sharing of intelligence information across all elements of the IC and the dissemination of intelligence information to both traditional and non-traditional customers including the homeland security community. The ICSIS is the IC's implementing program for the IC enterprise-wide IT portion of the IC EA.

Intelligence Information. Intelligence information and related materials include the following, whether written or in any other medium, classified pursuant to E.O. 12958, as amended or any predecessor or successor Executive Order:

- Foreign intelligence and counterintelligence defined in the National Security Act of 1947, as amended, and in Executive Order 12333;

Information describing US foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from US intelligence collection efforts; and

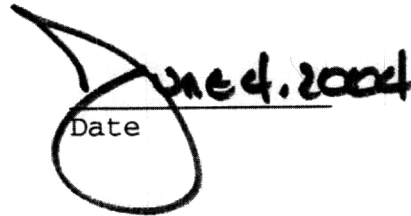
Information on IC protective security programs (e.g. personnel, physical, technical, and information security).

Senior Official of the Intelligence Community (SOIC). The head of an agency, office, bureau, or other intelligence element as identified in Section 3 of the National Security Act of 1947, as amended, 50 U.S.C. 401a(4), and Section 3.4(f) (1 through 6) of Executive Order 12333.

Tearline Reporting. An automated or manual technique for separating an intelligence report into multiple portions separated by machine-or human-readable Tearlines. A Tearline section is the area in an intelligence report or finished intelligence product where the sanitized version of a more highly classified and/or controlled report is located. The sanitized information within the Tearlines contains the substance of the more detailed information without identifying the sensitive sources and methods, allowing wider dissemination of the substantive intelligence information to authorized customers.

Write-to-Release. A general approach whereby intelligence reports are written in such a way that sources and methods are disguised so that the report can be distributed to customers or intelligence partners at lower security levels. In essence, write-to-release is proactive sanitization that makes intelligence more readily available to a more diverse set of customers. The term encompasses a number of specific implementation approaches, including sanitized leads and Tearline reporting.


Director of Central Intelligence


Date

REFERENCES

- DCID 2/4, Terrorist Threat Integration Center, 1 May 2003
2. DCID 6/1, Security Policy for Sensitive Compartmented Information, 1 March 1995.
 3. DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, 5 June 1999.
 4. DCID 6/5, Policy for the Protection of Certain Non-SCI Sources and Methods Information, 12 February 2001.
 5. DCID 6/6, Security Controls on the Dissemination of Intelligence Information, 11 July 2001.
 6. DCID 6/7, Intelligence Disclosure Policy 30 June 1998