
INTELLIGENCE COMMUNITY DIRECTIVE
NUMBER 208



WRITE FOR MAXIMUM UTILITY

(EFFECTIVE: 17 DECEMBER 2008)

A. AUTHORITY: The National Security Act of 1947, as amended; Executive Order (EO) 12958, as amended; EO 13388; EO 12333, as amended; and other applicable provisions of law.

B. PURPOSE:

1. This Intelligence Community Directive (ICD) establishes fundamental intelligence production principles and a common perspective from which to plan, organize, write, and disseminate intelligence products that provide the greatest use to customers. It directs Intelligence Community (IC) elements to produce intelligence in accordance with the "Write for Maximum Utility" (WMU) construct and its underlying principles. Utility is maximized when customers receive or are able to expeditiously discover and either pull or request information, intelligence and analyses in a form they can easily use and are able to share with appropriately cleared colleagues, subordinates, and superiors to facilitate mission accomplishment.

2. Applying WMU principles is integral to the success of the IC in meeting its responsibility to provide customers with usable intelligence. The WMU approach directly responds to the Intelligence Reform and Terrorism Prevention Act, building on a growing body of IC policy designed to advance information and intelligence sharing and strengthen analytic tradecraft (Appendix C). The construct provided by WMU helps resolve issues that can arise when attempting to share intelligence more broadly while continuing to protect sensitive intelligence sources and methods.

C. APPLICABILITY: This ICD applies to the IC, as defined by the National Security Act of 1947, as amended; and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

D. POLICY:

1. Elements of the IC shall produce intelligence in accordance with the six principles on which WMU is based (see paragraph F for principles and Glossary; Appendix B, for complete definition). WMU will guide the way that IC elements plan, format, produce, and disseminate products in order to maximize their usability. These principles—like doctrine—capture and codify IC best practices while establishing a shared foundation from which to produce intelligence of greatest utility to multiple customers.

2. Although fundamental, the principles of WMU require judgment in their application. WMU allows for multiple ways to reach the objective of most effectively serving the primary customer(s) and other IC customers who would benefit from the intelligence or who might not be immediately evident. The goal of WMU is to ensure that the IC produces intelligence that communicates the right information in the right form to the right people at the right time.

E. WMU FRAMEWORK:

1. The success of WMU requires collaboration among collectors and analysts directly involved in generating intelligence products. WMU likewise relies upon effective alignment with the IC's information technology and security and disclosure elements. Intelligence systems, processes, and procedures should enable intelligence producers and information stewards to identify risk mitigation strategies that will facilitate effective information and intelligence sharing while protecting intelligence sources and methods. The WMU principles and processes associated with their implementation should aid IC elements in producing intelligence that will expedite sanitization, disclosure and release decisions while getting the intelligence and information to those who need it.

2. WMU shares certain goals and techniques with previous and ongoing IC Write-to-Release (WTR) efforts. Like WTR, WMU seeks to maximize support to multiple customers—including nontraditional IC customers at the federal, state, local, and tribal level—by producing intelligence products that are or can be modified to be disseminated at lower security classification levels. WMU will use portion marking, sanitized text, and metadata tagging as well as new techniques to protect intelligence sources and methods while still providing insight, to the extent possible, into the quality and reliability of underlying sources and confidence in the analytic judgments and information contained in products.

3. However, WMU and WTR do differ in important ways. WMU goes farther than WTR in linking knowledge of the customer's operating environment to the intelligence production effort. The result is not "one size fits all" or production of all intelligence products at the lowest classification, but products tailored to best meet a customer's requirements. This may mean producing the definitive assessment on a given topic area based on all available information and intelligence, regardless of classification. Thus, tailored production in some cases may result in less production; however, innovative product organization and segmentation will facilitate tailored reuse of the product and broader dissemination if needed. More important, better knowledge of customers and their needs will translate into more focused, relevant, and usable intelligence.

F. PRINCIPLES OF WRITING FOR MAXIMUM UTILITY:

1. Know Your Customers and What They Need: Knowing your customers and their requirements is integral to current IC practices and the central tenet upon which WMU is based; yet, WMU also requires the analyst and the IC element to appreciate the totality of the audience of customers served. Although many primary customers are cleared for Top Secret and compartmented materials, most are supported by staff, or provide information and intelligence to elements, that are not cleared at these levels.

a. To facilitate and ensure a current and accurate understanding of customers' needs, each IC element should routinely identify the question or requirement being addressed by an intelligence product; specify customers that require the product's judgments and/or information; and assess whether the product can be shared with or discovered by other customers.

b. Understanding a customer's operating environment—to include information systems access and physical security restrictions—is crucial to producing intelligence that is of the greatest utility. Analysts and IC elements shall develop a better understanding of how their customers receive products—i.e., briefings, written products, online pull—and how the products will be used by the customers to aid in the planning and production of intelligence products that they can use and share.

c. IC elements shall aggressively seek and incorporate customer feedback to ensure that intelligence products best meet the customer's needs.

2. Write for Tailored Reuse: WMU recognizes that IC elements may not know all the potential customers for their products. Thus intelligence products shall—when appropriate and feasible—be conceived and structured in a manner that increases their potential for tailored reuse, thereby enhancing their utility. Such efforts span the spectrum; from writing multiple versions of a product, to formatting paragraphs and characterizing sourcing information in ways that to the extent possible provide insight but do not reveal sources and methods. IC elements are encouraged to consider writing base products at the collateral level with annotations indicating when higher classification versions are available to those who are appropriately cleared and who require them.

a. Where appropriate and feasible, intelligence products—to include text-based, multimedia, and other formats—should be constructed using tools and strategies (e.g., templates, ontologies, portion markings) that facilitate reuse and wider dissemination. These tools and strategies should be selected to minimize post-production manipulation, facilitate sanitization and the production of tearlines if needed, and aid in tailoring products to meet the needs of multiple, diverse customers. Products, product segments, portions, and tearlines shall be marked using only those markings and formats prescribed in the DNI's "Authorized Classification and Control Markings Register" and the accompanying implementation manual.

b. The tearline portion of products shall have unique product identifiers. These unique identifiers shall provide links or trace back to higher classifications reports for those who require them and are appropriately cleared.

c. Intelligence production elements shall consult with disclosure and release officers to identify measures that may increase the product's usability and facilitate dissemination to a wider audience.

3. Products must be discoverable by those who might need them: IC personnel or customers must be able to discover intelligence, information and analyses that address their requirements or aid in mission accomplishment. IC elements shall create or restructure current processes so that customers can search and discover intelligence products of interest and easily request and get what they need in a timely manner; consistent with DNI security, classification, and access management policies. WMU combines traditional WTR efforts to "push" products to IC customers with a more comprehensive and integrated process that allows them to discover and "pull" the products they need.

a. To enable customer discovery, IC elements shall create and disseminate or post machine-identifiable summary information (resource metadata) for all products in compliance with DNI Standards.

b. IC elements shall ensure that customers can discover a product by electronically disseminating all their products to the Library of National Intelligence (LNI), when operational, and/or one or more web-accessible network locations or enterprise catalogs.

4. Tradecraft Essential, Not Expendable: Regardless of classification level, products must adhere to ICD 203, Analytic Standards; and ICD 206, Sourcing Requirements for Disseminated Analytic Products. Quality products that reflect strong intelligence tradecraft are fundamental to WMU. Like the tension confronted by the IC in protecting sensitive sources and methods and meeting its "responsibility to provide," WMU may generate a conflict between maximizing the utility of a product by broadening its dissemination and providing the insight into the quality of sources and confidence levels required by the IC Analytic Standards. To resolve this tension, IC elements may have to explore new ways to convey such insights without explicit source identification or description.

a. WMU seeks to convey insight into the quality of the sourcing through a variety of techniques and means. Although full visibility on product sourcing may not always be possible, in order to broaden dissemination, IC elements shall, whenever appropriate and feasible, work with collectors to include sanitized source descriptors and other collection parameters. Sourcing insight can also be conveyed via methods, such as a numeric scale or broad credibility statements, which are currently the norm for unclassified terrorist threat tearline reporting. Reference to a fully sourced version of the product available in the LNI or the ability of appropriately cleared personnel to trace back tearline products through a unique product identifier are other ways to reconcile sound intelligence tradecraft with efforts to make intelligence products usable for IC customers.

b. Sanitized products should never render facts or judgments in a manner inconsistent with their higher-classified version—facts, judgments, confidence levels, and probabilistic language must be congruent.

5. Timely electronic dissemination is always the goal: With minimal exception, IC elements shall disseminate intelligence products electronically. This includes products that are produced at multiple classification levels. Tearline products generated by IC elements shall, when appropriate and feasible, be electronically detachable and automatically releasable electronically to appropriate web-based intelligence networks by the producing organization. Such efforts will expedite customer discovery, “pull” of needed products, and make it easier and faster for customers to share intelligence with those they support and direct. The formatting or tagging of products with tearlines shall facilitate automated posting of tearlines on non-Sensitive Compartmented Information systems, such as Secret Internet Protocol Router Network, consistent with DNI information and intelligence sharing and security policies.

6. Train to Think of Customers Inclusively; Write Differently: IC elements shall review and—where required—revise their training programs to address explicitly how to maximize product utility. Writing and production curricula shall address the manner in which analysts and collectors think about their customers and how they construct and write their products. This curriculum shall encourage contributors to the production process—from planning through dissemination—to think inclusively about their customers, their operating environment, and how their various customers use their products.

a. Developers of IC element training curricula are encouraged to focus on the manner in which products—to include releasable summaries—are organized and constructed and how judgments are communicated. Drafting and presenting information in segments that enable tailored reuse and techniques for conveying sourcing information and confidence levels in more nuanced ways shall be part of this curriculum. This may include training that encompasses the art of sanitization and the purpose and procedures for writing sanitized products. Such training shall emphasize creating products that are informed by all relevant information; however, to the extent possible, analytic judgments or relevant information shall be presented at the lowest classification level at which the essential message can be conveyed in order to allow optimum sharing and maximize utility.

b. IC element training shall incorporate measures to facilitate disclosure and release decisions consistent with applicable DNI disclosure policies.

c. IC element training shall incorporate guidelines for Controlled Access Program Coordination Office markings to facilitate marking standardization.

G. AUTHORITIES AND RESPONSIBILITIES:

1. The Deputy Director of National Intelligence for Analysis (DDNI/A) shall:

a. Work with other Office of the Director of National Intelligence (ODNI) and IC elements to ensure IC policies, procedures, processes, capabilities, and resources support these production principles and WMU;

b. Establish performance measures for implementation and monitor compliance;

c. Construct—with input from IC elements—and maintain an on-line website that will provide answers to frequently asked questions as well as contain WMU exemplars, best practices, and product templates.

2. The Deputy Director of National Intelligence for Collection (DDNI/C) shall work with other ODNI and IC elements to develop implementation guidance that will help in identifying ways collectors can produce products that minimize the use of caveats, support broader dissemination, and maximize product utility.

3. The DNI Chief Information Officer shall work with other ODNI and IC elements to ensure IC information technology standards, processes, procedures, and resources support WMU production principles.

4. The Deputy Director of National Intelligence for Policy, Plans, and Requirements shall:

a. Collaborate with DDNI/A and DDNI/C to assist IC elements in developing implementation guidance;

b. Through the Assistant Deputy Director of National Intelligence for Security, and in collaboration with the security directors of IC elements and other customers, review and revise security training as necessary to implement this policy and ensure the protection of intelligence sources and methods.

5. The Chancellor of the National Intelligence University, in collaboration with the heads of IC elements and appropriate ODNI offices, shall identify training to implement this policy and require IC agencies to develop appropriate training modules for their unique work forces.

6. IC elements shall:

a. Review and revise production plans and processes as necessary to ensure they are consistent with the WMU principles identified in this ICD and result in products that provide maximum utility;

b. Directly or through customer liaisons or departmental elements as appropriate, aggressively seek insight into customer requirements and solicit customer feedback concerning all aspects of the production and dissemination environment to ensure that product utility is maximized;

c. Train staff in skills necessary to implement WMU;

d. Develop plans in conjunction with ODNI to ensure that information systems and technical standards support WMU;

e. Ensure that employees have the necessary tools and guidance to execute this policy;

f. Collaborate with ODNI to develop and promulgate implementation guidelines for WMU; and

g. Report to the DDNI/A annually on efforts to implement this directive to include proposed program changes that affect intelligence production, analysis, or dissemination. Annual reports should address the effectiveness of WMU measures through an assessment of appropriate production and dissemination metrics and customer feedback.

H. EFFECTIVE DATE: This ICD becomes effective on the date of signature.



Director of National Intelligence

17 DEC 08

Date

APPENDIX A-ACRONYM LIST**ICD 208 – WRITE FOR MAXIMUM UTILITY**

DDNI/A	Deputy Director of National Intelligence for Analysis
DDNI/C	Deputy Director of National Intelligence for Collection
DNI	Director of National Intelligence
EO	Executive Order
IC	Intelligence Community
ICD	Intelligence Community Directive
LNI	Library of National Intelligence
ODNI	Office of the Director of National Intelligence
WMU	Write for Maximum Utility
WTR	Write-to-Release

APPENDIX B-GLOSSARY

Customer: A person or entity that requires intelligence and information, consistent with applicable laws, EO, and Attorney General procedures promulgated in accordance with EO 12333, as amended. A customer external to the IC does not have the same rights to access, search, discover, and retrieve information and intelligence data in the form initially gathered as do IC personnel.

Discovery: The act of obtaining knowledge of the existence, but not necessarily the content, of information collected or analysis produced by any IC element. Discovery, as it is applicable under this directive, is not defined or intended to be interpreted as discovery under the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure or other individual state discovery rules regarding non-privileged matter that is relevant to any party's claim or defense.

Intelligence Product: An intelligence report disseminated to customers by an intelligence agency or element. The report contains information and/or analysis of potential intelligence value to meet the needs of intelligence users within and outside the Intelligence Community. It may involve current or future developments or the capabilities, intentions, and activities of entities of interest.

Metadata Tagging: Uses encoded data that describes characteristics of information entities to enable identification, discovery, assessment, and management of the described entities.

Tearline: 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 and information to authorized customers.

Write for Maximum Utility (WMU): An approach that guides the way that intelligence organizations conceive, format, produce, and disseminate intelligence products in order to increase their usability for the intended customers. Utility is maximized when customers receive or are able to expeditiously discover and pull or request intelligence, information, and analysis in a form they are able to easily use and able to share with their colleagues, subordinates, and superiors. WMU ensures intelligence, information, and analysis are produced in a manner to facilitate reuse—either in its entirety or in coherent portions—thereby enabling wider dissemination and enhancing its usability. WMU shares certain goals as well as techniques with previous and ongoing IC WTR efforts. WMU and WTR do, however, differ in important ways. WMU goes farther than WTR in linking knowledge of the customer's operating environment to the intelligence production effort. The resulting effort is not "one size fits all" or production of all intelligence

products at the lowest classification, but products tailored to best meet a customer's requirements. This may mean producing the definitive assessment on a given topic area based on all available intelligence, regardless of classification.

Write-to-Release (WTR): A general approach whereby intelligence reports are written in such a way that sources and methods are protected 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 usable by a more diverse set of customers. The term encompasses a number of specific implementation approaches, including sanitized leads and tearline reporting.

APPENDIX C-REFERENCES

1. ICD 203, *Analytic Standards*, 21 June 2007
2. ICD 206, *Sourcing Requirements for Disseminated Analytic Products*, 17 October 2007
3. ICPM 2007-500-1, *Unevaluated Domestic Threat Tearlines Reports*, 19 November 2007
4. ICPM 2007-200-2, *Preparing Intelligence to Meet the Intelligence Community's "Responsibility to Provide,"* 11 December 2007
5. ICPM 2007-500-3, *Intelligence Information Sharing*, 22 December 2007
6. ICS 2007 500-3, *Intelligence Community Standard for Information Resource Metadata*, 11 December 2007
7. ICS 2007 500-4, *Intelligence Community Standard for Publication Metadata*
8. United States Intelligence Community *Information Sharing Strategy*, 22 February 2008