

INFORMATION QUALITY IMPLEMENTATION

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 139-02, "Information Quality," and facilitates DHS compliance with applicable legal requirements, including those associated with Public Law 106-554, "Treasury and General Government Appropriations Act for Fiscal Year 2001." Section 515 of this act requires federal agencies to issue guidelines ensuring and maximizing the quality, utility, objectivity and integrity of disseminated information. Recent innovations in information generation and management have significantly increased information availability, requiring all federal agencies to revisit their dissemination control procedures and ensure adherence to appropriate information quality (IQ) standards.

II. Scope

- A. This Instruction applies throughout DHS to:
1. Influential scientific, financial, or statistical information disseminated to the public in any medium including textual, graphic, cartographic, narrative, numerical, or audiovisual forms;
 2. DHS-sponsored distribution of information (where the agency directs a third party to distribute information, or the agency has the authority to review and approve the information before release); and
 3. Information posted on the DHS public website (www.dhs.gov) and the public websites of DHS Components.
- B. This Instruction **does not** apply to information disseminated in the following contexts:
1. Between government employees, agency contractors, or grantees;
 2. Interagency use or sharing of government information;

3. Hyperlinks posted on the DHS public website (www.dhs.gov) and the websites of DHS Components that are disseminated and posted elsewhere by others;
4. Correspondence with individual persons, press releases, archival records, public filings, subpoenas, or adjudicative processes; and
5. Responses to requests for agency records under the Freedom of Information Act, the Privacy Act of 1974, the Federal Advisory Committee Act, or other similar laws.

C. This Instruction **does not**:

1. Override other compelling interests such as privacy interests, trade secrets, intellectual property, and other confidentiality protections;
2. Release DHS from its export control compliance responsibilities;
3. Affect any otherwise available judicial review of agency action;
4. Apply to opinions where the agency's presentation makes it clear that the material is an opinion or the agency's views rather than fact; and
5. Apply to any patents, trademarks, copyrights, licenses or any other documents filed by the Department's Office of General Counsel on behalf of a DHS program at another agency, for DOJ, for a Court or to a third party.

D. Notwithstanding the scope described above, which applies only to disseminated information, all DHS personnel and officials are encouraged to adopt a basic standard of quality (including objectivity, utility, and integrity), whenever practicable, as part of their information management practices.

III. References

- A. Office of Science and Technology Policy Memo: Scientific Integrity (March 9, 2009 and December 17, 2010), as referenced in [DHS Directive 026-07, "Scientific Integrity"](#)
- B. Office of Management and Budget (OMB) Memorandum M-19-15, "Improving Implementation of the Information Quality Act"¹

¹ A complete list of related authorities is provided in DHS Directive 139-02, "Information Quality."

IV. Definitions

- A. **Affected Persons**: Individuals who may benefit or be harmed by the disseminated information. This includes persons who are seeking to address information about themselves, as well as persons who use information.
- B. **Dissemination**: Agency initiated or sponsored distribution of information to the public [see Title 5, Code of Federal Regulations, Section 1320.3(d) (definition of "Conduct or Sponsor")].
- C. **Government information**: Information created, collected, processed, disseminated, or disposed of by or for the Federal Government.
- D. **Influential**: When used in the phrase "influential scientific, financial, or statistical information," means that the agency can reasonably determine that dissemination of the information will have or does have a clear and substantial impact on important public policies or important private sector decisions. Each agency is authorized to define "influential" in ways appropriate for it given the nature and multiplicity of issues for which the agency is responsible. Agency definitions and determinations do not preempt agency requirements for rulemaking under existing statutes and executive orders.
- E. **Information**: Any communication or representation of knowledge such as facts or data, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. This definition includes information that an agency disseminates from a web page, but does not include the provision of hyperlinks to information that others disseminate. Unlike the OMB Circular A-130 definition for information, this definition does not include opinions, where the agency's presentation makes it clear that what is being offered is someone's opinion rather than fact or the agency's views.
- F. **Information dissemination product**: Any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, an agency disseminates to the public. This definition includes any electronic document, CD-ROM, or web page.
- G. **Integrity**: Refers to the security of information or the protection of information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.
- H. **Objectivity**: Involves two distinct elements: presentation and substance.

1. "Objectivity" includes whether disseminated information is being presented in an accurate, clear, complete, and unbiased manner. This involves whether the information is presented within a proper context. Sometimes, in disseminating certain types of information to the public, other information is disseminated in order to ensure an accurate, clear, complete, and unbiased presentation. In addition, the Department/Agency needs to identify the sources of the disseminated information (to the extent possible, consistent with confidentiality protections) and, in a scientific, financial, or statistical context, the supporting data and models, so that the public can assess for itself whether there may be some reason to question the objectivity of the sources. Where appropriate, data should have full, accurate, transparent documentation, and error sources affecting data quality should be identified and disclosed to users.

2. In addition, "objectivity" involves a focus on ensuring accurate, reliable, and unbiased information. In a scientific, financial, or statistical context, the original and supporting data is generated, and the analytic results are developed, using sound statistical and research methods.

a. If data and analytic results have been subjected to formal, independent, external peer review, the information may generally be presumed to be of acceptable objectivity. However, this presumption is refutable based on a persuasive showing by the petitioner in a particular instance. If department/agency-sponsored peer review is employed to help satisfy the objectivity standard, the review process employed meets the general criteria for competent and credible peer review recommended by OMB's Office of Information and Regulatory Affairs to the President's Management Council, date September 20, 2001, namely, "that

(1) peer reviewers be selected primarily on the basis of necessary technical expertise,

(2) peer reviewers be expected to disclose to agencies prior technical/policy positions they may have taken on the issues at hand,

(3) peer reviewers be expected to disclose to departments/agencies their sources of personal and institutional funding (private or public sector), and

(4) peer reviews be conducted in an open and rigorous manner."

b. If an agency is responsible for disseminating influential scientific, financial, or statistical information, agency guidelines will include a high degree of transparency about data and methods to facilitate the reproducibility of such information by qualified third parties.

I. **Quality**: Is an encompassing term comprising utility, objectivity, and integrity. Therefore, the guidelines sometimes refer to these four statutory terms, collectively, as "quality."

J. **Reproducibility**: The information is capable of being substantially reproduced, subject to an acceptable degree of imprecision. For information judged to have more (less) important impacts, the degree of imprecision that is tolerated is reduced (increased). If agencies apply the reproducibility test to specific types of original or supporting data, the associated guidelines provides relevant definitions of reproducibility (e.g., standards for replication of laboratory data). With respect to analytic results, "capable of being substantially reproduced" means that independent analysis of the original or supporting data using identical methods would generate similar analytic results, subject to an acceptable degree of imprecision or error.

K. **Utility**: Refers to the usefulness of the information to its intended users, including the public. In assessing the usefulness of information that the department/agency disseminates to the public, the agency needs to consider the uses of the information not only from the perspective of the agency but also from the perspective of the public. As a result, when transparency of information is relevant for assessing the information's usefulness from the public's perspective, the agency takes care to ensure that transparency has been addressed in its review of the information.

V. Responsibilities

A. The **DHS Information Quality (IQ) Officer**:

1. Submits the annual report to the Director of OMB on the number and nature of requests for correction (RFCs) by the public or organization;
2. Works with each Component Information Quality (IQ) Officer or Official to track and respond to information corrections and appeals;
3. Conducts an internal review to identify necessary updates to the standards of the IQ Program; and
4. Coordinates IQ corrections that are posted on any DHS website, working with affected Component, the Office of the General Counsel, and the Office of Public Affairs, as appropriate.

- B. The **DHS Component Information Quality (IQ) Officers/Officials**:
1. Post IQ standards on the Component internet web site;
 2. On a quarterly basis, submit reports to the DHS IQ Officer, which identify the number and natures of RFCs received regarding compliance with the guidelines, and explain how the requests for correction were resolved; and
 3. Submit the reports and information as requested by the DHS IQ Officer to complete the annual report to OMB.
- C. The **Office of the General Counsel** reviews DHS responses to RFCs for legal sufficiency.

VI. Content and Procedures

- A. DHS is committed to compliance with the following OMB IQ Standards and Implementation requirements:
1. **Identifying "Influential" Information**: Drawing on experience, DHS Component should revisit the parameters for identifying "influential information." Components should provide specific guidance to program managers for determining the amount and type of pre-dissemination review necessary. Components should identify specific types of information they produce that are "influential" and should provide a rigorous process for determining whether types of information not specifically listed by the guidelines qualify as "influential."
 2. **Peer Review of Influential Scientific Information**: When using scientific information, including third-party data or models, to support their policies, Components must ensure compliance with the requirements of OMB's Information Quality Bulletin for Peer Review. When conducting peer review, Components should ensure reviewers are asked to evaluate the objectivity of the underlying data and the sensitivity of the agency's conclusions to analytic assumptions. When influential information that has been peer reviewed changes significantly (e.g., as a result of the peer reviewer comments, additional agency analysis, or further consideration), the agency should conduct a second peer review.

3. **Public Access to Government Information (Open Data)**: When a Component makes information originally collected or developed by other Federal agencies available to the public in a cross-agency dissemination, each agency and its Components are responsible for the quality of the information they contribute, and that responsibility should be clearly communicated to the public. Components should provide the public with sufficient documentation about each dataset released to allow data users to determine the fitness of the data for the purpose for which third parties may consider using it. Robust practices may include developing a standard template or framework that provides data users with the relevant information. Safeguarding privacy and confidentiality is vital in the context of open data.

4. **Re-use Of Existing Agency Program Data**: Components should consider the potential for using existing data sources from both inside and outside the agency for statistical and research purposes, while fully protecting privacy and confidentiality. When designing or improving data collection systems, Components should actively solicit comment from their statistical, research, and evaluation agencies about potential downstream uses. Components should describe such uses in the Information Collection Request submitted to OMB for review under the Paperwork Reduction Act (PRA). If Components are considering analysis of data that includes personally identifiable information, the Components are required to work with their Privacy Officer (or Privacy point of contact) and with the DHS Chief Privacy Officer to meet all privacy requirements and manage privacy risks. Components should develop procedures for clearly documenting and communicating the quality of administrative data that have the potential to be used for statistical purposes.

5. **Models and Machine Learning**: Consistent with the Office of Science and Technology Policy's Memo and DHS Directive 026-07: Scientific Integrity, agencies should ensure that influential information is communicated transparently by "including a clear explication of underlying assumptions; accurate contextualization of uncertainties; and a description of the probabilities associated with both optimistic and pessimistic projections, including best-case and worst-case scenarios. When a Component has performed analysis using a specialized set of computer code, the computer code used to process it should be made available to the public for further analysis, if consistent with applicable law and policy.

6. **Non-Government Information:** Component should ensure that when using non-government sources to create influential information they communicate to the public sufficient information on the characteristics of the data and analysis, including its scope (e.g., temporal or demographic), generation protocols, and any other information necessary to allow the public to reproduce the agencies' conclusions.

7. **Access to and Considerations for Protecting Data:** Components should prioritize increased access to the data and analytic frameworks (e.g., models) used to generate influential information. All data disclosures must be consistent with statutory, regulatory, and policy requirements for protections of privacy and confidentiality, proprietary data, and confidential business information. Per the Open Public, Electronic and Necessary Government Data Act, Components should explore methods that provide wider access to datasets while, to the greatest extent possible, minimizing the risk of disclosure of personally identifiable information. In particular, tiered access offers promising ways to make data widely available while protecting privacy. Implementation of such approaches must be consistent with principles for ethical governance, which include employing sound data security practices, protecting individual privacy, maintaining promised confidentiality, protecting the intellectual property of third parties, and ensuring appropriate access and use. Components should adopt as a default position that all PII shall be anonymized before disclosing data.

8. **Processing Timelines:** Components should revise their procedures to reflect more realistic timelines for RFCs. Revised procedures should, at minimum, provide that agencies will not take more than 120 days to respond to an RFC without the concurrence of the party that requested the request for correction.

9. **Sharing Draft Responses with OMB Prior to Release:** In its response to an RFC, the Component should not opine on the requestor's or the Department's policy position. Responses should contain a point-by-point response to any data quality arguments contained in the RFC and should refer to a peer review that directly considered the issue being raised, if available. Components should share draft responses to RFCs and appeals with OMB prior to release to the requestor for assessment of compliance with the above norms.

10. **Appeals Requests:** To ensure the integrity of the appeals process, Components should ensure that those individuals reviewing and responding to the appeals request were not involved in the review and initial response to the RFC.

B. DHS adopts a basic standard of quality (including objectivity, utility, and integrity) as a performance goal and takes appropriate steps to incorporate IQ criteria into the Department's information dissemination practices. Quality is to be ensured and established at levels appropriate to the nature and timeliness of the information to be disseminated. DHS has adopted specific standards of quality that are appropriate for the various categories of information disseminated.

C. As a matter of good and effective information resources management, DHS develops a process for reviewing the quality (including the objectivity, utility, and integrity) of information before it is disseminated. DHS treats IQ as integral to every step of an agency's development of information, including creation, collection, maintenance, and dissemination. This process enables the Department to substantiate the quality of the information it has disseminated through documentation or other means appropriate to the information.

D. To facilitate citizen review, DHS has established administrative mechanisms allowing affected persons to seek and obtain, where appropriate, timely correction of information maintained and disseminated by the agency that does not comply with OMB or DHS guidelines. These administrative mechanisms are flexible, appropriate to the nature and timeliness of the disseminated information, and incorporated into the Department's information resources management and administrative practices.

VII. Administrative Complaint Mechanism

A. Section 515 requires each agency to develop an administrative mechanism for receiving complaints and appeals regarding IQ. Within this structure, any person or organization may assert a claim that DHS information does not comply with OMB or DHS guidelines, and, if appropriate, may petition for correction or remedy. Using the administrative mechanism outlined below, affected persons can seek, and obtain where appropriate, timely correction of DHS information that does not comply with OMB or DHS guidelines. Direct DHS IQ complaints to the DHS or Component IQ Officer (per submission instructions on the Component Internet site) or to:

Department of Homeland Security
ATTN: Office of the Chief Information Officer/Information Quality Officer
245 Murray Lane, SW
Mail Stop 0136
Washington, DC 20528

Email: DHS.InfoQuality@hq.dhs.gov

DHS Website: <http://www.dhs.gov/dhs-information-quality-standards>

- B. When petitioning for correction or remedy, each request includes:
1. Description of the information deemed to need correction;
 2. Manner in which the information does not comply with the IQ guidelines;
 3. Manner disseminated and, if available, date of dissemination;
 4. Specific error(s) cited for correction and proposed correction or remedy, if any;
 5. How the person was affected and how correction would benefit them; and
 6. Petitioner's contact information for DHS to reply on whether and how the correction is made.
- C. The IQ Officer responds to complaints and/or requests for correction within 120 days of receipt. Notify the petitioner if the complaint requires additional time for processing.
- D. Complaint Review and Resolution: All materials responsive to an IQ complaint are collected and processed by the IQ Officer within the 120 day research and response period. The Department should share draft responses to the RFCs and appeals with OMB prior to release to the petitioner.
- E. After thorough review and conclusion, a response is sent to the petitioner on whether and how the correction is made. Any releasable information may be sent to the petitioner along with the written response. If applicable, the written response may also indicate the type of material withheld, the exemptions claimed, and the right to administratively appeal any denial of information.
- F. Administrative Appeal Process
1. DHS has developed an administrative appeal process in the event a petitioner is not satisfied with the reply. This right to appeal is included in the notice of denial issued during the complaint process.

2. For DHS Support Components (except the Federal Law Enforcement Training Centers) the responsible official is the DHS Chief Information Officer (CIO) or designee, unless that person is the same person who participated in the initial response to petitioner. In such event, the CIO or designee shall designate a different person within DHS OCIO, to coordinate the appeal process. In turn, such person shall request that the Component having IQ functions appoint an official to administer the IQ appeals, unless such person has participated in the initial response. In the appeal, the DHS CIO (or Component Appeal Official), or their designee, shall determine if DHS has properly administered and complied with IQ rules and regulations regarding request for correction or remedy, and undertake a discussion of why the request is not acceptable.

3. After the petitioner receives a response or decision from the Department on a complaint, the incumbent sends their appeal of the ruling within 30 calendar days of the decision date. Direct the appeals to:

Department of Homeland Security
ATTN: Office of the Chief Information Officer/Information Quality Officer
245 Murray Lane, SW
Mail Stop 0136
Washington, DC 20528

Email: DHS.InfoQuality@hq.dhs.gov

DHS Website: <http://www.dhs.gov/dhs-information-quality-standards>

4. Upon receipt, the IQ Officer forwards the appeal to the DHS CIO or Component Appeal Official.

5. DHS responds to appeals and/or requests for correction within 120 days of receipt. If the appeal requires an extended period of time for processing, the Department notifies the petitioner.

6. The Appeal Official's decision is the final step in the Department's administrative appeal process.

G. Exclusions: Certain disseminations of information include a comprehensive public comment process (e.g., notices of proposed rulemaking, regulatory analyses and requests for comment on an information collection subject to the Paperwork Reduction Act). The administrative complaint mechanism described in these guidelines does not apply to such documents. Persons questioning information disseminated as listed in Section II.B will need to make those request following the approved Department process.

VIII. Questions

Address questions or concerns to the Office of the Chief Information Officer, Business Management Office (BMO) or DHS.InfoQuality@hq.dhs.gov.



Elizabeth A. Cappello
Acting Chief Information Officer



Date