

United States Department of Homeland Security

Information Quality Guidelines

INTRODUCTION

Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554, app C § 515, 114 Stat. 2763A-153-4 (Dec 21, 2000)) directs the Office of Management and Budget (OMB) to issue government-wide guidelines that provide policy and procedural guidance to Federal agencies for ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information, including statistical information, disseminated by Federal agencies. Section 515 specifically requires OMB's guidelines to direct agencies to issue their own guidelines and establish administrative mechanisms allowing affected persons to seek and obtain correction of information disseminated by the agency that does not comply with OMB's guidelines. OMB issued its guidelines on February 22, 2002. See 67 Fed. Reg. 8452.

The Department of Homeland Security (DHS or Department) disseminates a variety of information to the public. As directed under OMB's guidelines, DHS is issuing these information quality guidelines to provide transparency into the processes DHS and its components use to ensure the quality of disseminated information and to provide a process by which affected persons may seek or obtain correction of information disseminated by DHS and its components.

Background

The focus of Section 515 is on the Federal Government's information dissemination activities. Federal agencies have disseminated information to the public for decades. Until recently, agencies have disseminated information principally by making paper copies of documents available to the public. In recent years, Federal dissemination of information has grown.

Section 515 builds upon the existing Government-wide responsibility to ensure information quality. According to the Paperwork Reduction Act (PRA), the agency Chief Information Officers (CIO) must manage information resources to "improve the integrity, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring dissemination of public information, public access to government information, and protections for privacy and security."

PURPOSE

These guidelines should be used to ensure and maximize the quality of disseminated information. The Department's guidelines are based on the guidelines of the Office of Management and Budget (OMB), "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of the Information Disseminated by Federal Agencies" 67 Fed. Reg. 8452 (Feb. 22, 2002). The guidelines are not intended to be, and should not be construed as, legally binding regulations or mandates. These guidelines are intended only to improve the internal management of DHS and, therefore, are not legally enforceable and do not create any legal rights or impose any legally binding requirements or obligations on the agency or the public. Nothing in these guidelines affects any available judicial review of agency action.

SCOPE

The DHS guidelines will become effective on March 18, 2011. These guidelines will cover information disseminated on or after March 18, 2011, regardless of when the information was first disseminated.

These guidelines will serve as the minimum standards for quality within the Department. DHS Components may expand upon these guidelines as necessary, and should use these guidelines to develop or improve their processes for ensuring information disseminated by the Component meets the quality standards. DHS Components should implement processes and mechanisms for receiving, reviewing, and responding to information request that are consistent with these guidelines. DHS Components with existing directives,

instructions, and correction processes for information quality may continue to use them, providing they are consistent with the standards and processes established in these guidelines.

The guidelines apply to information disseminated to the public in any medium including textual, graphic, narrative, numerical, or audiovisual forms, including information posted on the Internet. The guidelines also apply to Component-sponsored distribution of information – where the Component directs a third party to distribute information or DHS has the authority to review and approve the information before release. If the Department is to rely on information submitted by a third party that information would need to meet appropriate standards of objectivity and utility.

The guidelines do not override other compelling interests such as privacy, trade secrets, intellectual property, and other confidentiality protections. The guidelines do not apply to hyperlinks or to information that others disseminate. The guidelines do not apply to opinions where the Department's presentation makes it clear that the material is only an opinion or the Department's views, rather than fact. In addition, the guidelines do not apply to information disseminated in the following contexts:

- Dissemination of information limited to government employees or agency contractors or grantees.
- Dissemination of information intended to be limited to intra- or inter-agency use or sharing of government information.
- Correspondence with individual persons, archival records, public filings, subpoenas or adjudicative processes.
- Response to requests for agency records under the Freedom of Information Act, the Privacy Act, the Federal Advisory Committee Act, or other similar laws.

The DHS guidelines adhere to the basic standards cited in the OMB guidelines and focus on the following areas:

- **Basic Standard of Quality.** Overall, all DHS Components disseminating information shall adopt a basic standard of quality (including objectivity, utility, and integrity) and should take appropriate steps to incorporate information quality criteria into the Component's information dissemination practices.
- **Process for Reviewing the Quality of Information.** As a matter of good and effective agency information resources management, all DHS Components shall have a process for reviewing the quality (including the objectivity, utility, and integrity) of information before it is disseminated.
- **Process for Citizen Complaint.** To facilitate public review, all DHS Components shall establish administrative mechanisms allowing affected persons (individual or entity that may use, benefit, or be harmed by the disseminated information at issue) to seek and obtain, where appropriate, timely correction of information maintained and disseminated that does not comply with OMB or agency guidelines. The purpose of the information complaint and appeal process is to address information quality matters, not resolve underlying substantive policy or legal issues.

In urgent situations which may pose an imminent threat to public health or welfare, the environment, the national economy, or homeland security, DHS may temporarily waive these guidelines in whole or in part.

GUIDELINES

It is DHS policy to ensure and maximize the quality, objectivity, utility, and integrity of the information that it disseminates to the public. DHS will take appropriate steps to incorporate information quality criteria into its information dissemination practices, and will ensure the quality of information the agency disseminates in accordance with the standards set forth in these Guidelines. DHS is committed to integrating the principle of information quality into every step of its development of information, including creation, collection, maintenance, and dissemination. High quality information is a performance goal for all DHS information that is disseminated.

At a minimum, all DHS Components should:

- adopt the standards of information quality outlined in these guidelines;

- establish the standards as a performance goal;
- incorporate the standards in information dissemination practices; and
- ensure quality and establish levels of quality appropriate to the nature and timeliness of the information disseminated.

To ensure and maximize quality information, the standards should focus on the three underlying requirements for quality: utility, objectivity, and integrity of information.

Utility

In assessing the usefulness of information disseminated to the public, Components should consider the uses of the information from the perspective of the public. When transparency of information is relevant for assessing information's usefulness from the public's perspective, Components should consider transparency when developing and reviewing the information. (Transparency refers to the clear, obvious and precise nature of the information.)

Objectivity

Objectivity involves two distinct elements: presentation and substance. When disseminating information, Components should ensure that they satisfy both elements.

A. Presentation:

- Disseminate information in an accurate, clear, complete, and unbiased manner. This involves presenting information within a proper context.
- Where appropriate, data should have full, accurate, and transparent documentation, and should identify and disclose error sources affecting data quality.
- Sometimes, in disseminating certain types of information to the public, other information must also be disseminated in order to ensure an accurate, clear, complete, and unbiased presentation.
 1. Identify the sources of the disseminated information (to the extent possible, consistent with confidentiality protections).
 2. In a scientific, financial, or statistical context, identify 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.

B. Substance:

- Focus on ensuring accurate, reliable, and unbiased information.
- In a scientific, financial, or statistical context, generate the original and supporting data, and develop the analytic results, using sound statistical and research methods.
 1. 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.
 2. If agency-sponsored peer review is employed to help satisfy objectivity, the review process shall meet the general criteria for competent and credible peer review, namely:
 - a. peer reviewers must be selected primarily on the basis of necessary technical expertise;
 - b. peer reviewers must be expected to disclose to agencies prior technical/policy positions they may have taken on the issues at hand;
 - c. peer reviewers must be expected to disclose to agencies their sources of personal and institutional funding (private or public sector); and
 - d. peer reviews must be conducted in an open and rigorous manner.

- When disseminating influential scientific, financial, or statistical information, Components should include a high degree of transparency about data and methods to facilitate the reproducibility of such information by qualified third parties.
 1. DHS Components may identify, in consultation with the relevant scientific and technical communities, those types of data that can practicably be subjected to a reproducibility requirement, given ethical, feasibility, or confidentiality constraints. Reproducibility of data is an indication of transparency about research design and methods and thus a replication exercise (i.e., a new experiment, test, or sample) is not required prior to each dissemination.
 2. Concerning analytic results, DHS Components should provide sufficient transparency about data and methods so that a qualified member of the public could undertake an independent reanalysis. These transparency standards apply to analysis of data from a single study as well as to analyses that combine information from multiple studies.
 3. The guidelines do not override other compelling interests such as privacy, the need to protect classified or sensitive security information, protection of trade secrets, intellectual property, or other confidentiality protections.
 - a. In situations where public access to data and methods will not occur due to other compelling interests, apply especially rigorous robustness checks to analytic results and document what checks were undertaken.
 - b. Disclose the specific data sources that have been used and the specific quantitative methods and assumptions that have been employed.
 - c. Define the type of robustness checks, and the level of detail for documentation, appropriate for the nature and multiplicity of issues for which the agency is responsible.
- Influential data/information is that which the Department can reasonably determine will have or does have a clear and substantial impact on important public policies or important private sector decisions.
 1. A “clear and substantial impact” is one that has a high probability of occurring. The impact must be on “important” public policy or private sector decisions. Even if information has a clear and substantial impact, it is not influential if the impact is not on a public or private decision that is important to policy, economic, or other decisions.
 2. The definition applies to “information” itself, not to decisions that the information may support. Even if a decision or action by DHS is itself very important, a particular piece of information supporting it may or may not be “influential.”
- Each Component can supplement the above definition of “influential information” and develop function/program appropriate definitions as they develop processes for disseminating quality information.
- In rulemaking, “influential information” is generally considered to be scientific, financial, or statistical information that can reasonably be regarded as being one of the major factors in the resolution of one or more key issues in an economically significant rulemaking, as the term economically significant is defined in Executive Order 12866, as amended. Economically significant rulemakings are defined in Executive Order 12866 as a rulemaking action that is likely to have an annual effect on the economy of \$100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, Tribal, or local governments or communities.

Integrity

Protect information from unauthorized access or revision, to prevent corruption or falsification of information. Comply with Government-wide, DHS-wide, and Component security and privacy requirements and OMB

Circulars A-123, A-127, and A-130 when disseminating information. In addition, comply with other applicable regulations.

Quality Standards: Human health, safety and the environment

With regard to analysis of risks to human health, safety and the environment maintained or disseminated by the Department or any component, the following adaptation of the quality principles applied by Congress to risk information used and disseminated pursuant to the Safe Drinking Water Act Amendments of 1996 (42 U.S.C. 300g-1(b)(3)(A) & (B)) as may be further detailed in Departmental Directives on Environmental Planning (Dir 023-01) and Environmental Compliance (Dir 023-02) applies:

The use of science in decision-making.— To the degree that an action is based on science, the decision-maker within the Office of the Secretary or any component shall use **(i)** the best available, peer-reviewed science and supporting studies conducted in accordance with sound and objective scientific practices; and **(ii)** data collected by accepted methods or best available methods (if the reliability of the method and the nature of the decision justifies use of the data).

Public information.— The decision-maker shall ensure that the public presentation of information on environmental, safety and public health effects is comprehensive, informative, and understandable. The decision-maker shall, in any document made available to the public in support of a regulation promulgated or other decision of direct public impact, identify to the extent practicable—

- (i)** each population addressed by any estimate of public health effects;
- (ii)** the expected risk or central estimate of risk for the specific populations;
- (iii)** each appropriate upper-bound or lower-bound estimate of risk;
- (iv)** each significant uncertainty identified in the process of the assessment of public health effects and studies that would assist in resolving the uncertainty; and
- (v)** peer-reviewed studies known to the decision-maker that support, are directly relevant to, or fail to support any estimate of public health effects and the methodology used to reconcile inconsistencies in the scientific data.

Decision-makers responsible for dissemination of vital health and medical information shall interpret the reproducibility and peer-review standards in a manner appropriate to assuring the timely flow of vital information from agencies to medical providers, patients, health agencies, and the public. Information quality standards may be waived temporarily by the Secretary under urgent situations as may be required by imminent threats to public health or homeland security, provided that such waiver is noted publicly at the time it is utilized.

INFORMATION REVIEW, COLLECTION, AND CORRECTION PROCESSES

Information Review Process

As a matter of good and effective information resources management, all DHS Components should develop or improve processes for reviewing the quality (including the objectivity, utility, and integrity) of information before it is disseminated.

- Treat information quality as integral to every step of the development of information, including creation, collection, maintenance, and dissemination.
- Substantiate the quality of the information disseminated through documentation or other means appropriate to the information.

Information Collection Process

It is important that all DHS Components make use of OMB's Paperwork Reduction Act (PRA) clearance process to help improve the quality of information that the Department collects and disseminates to the public. DHS Components are already required to demonstrate in their PRA submissions to OMB the "practical utility" of a proposed collection of information the Components plan to disseminate. Additionally, for all proposed collections of information that will be disseminated to the public, DHS Components should demonstrate in their PRA clearance submission to OMB that the proposed collection of information will result

in information that will be collected, maintained, and used in a way consistent with the OMB and DHS information quality guidelines.

Administrative Correction Request Mechanism

Section 515 and OMB's guidelines require each agency to develop an administrative mechanism for receiving correction requests and appeals regarding information quality. Using the administrative mechanism, affected persons can seek, and obtain, where appropriate, timely correction of information that does not comply with OMB guidelines, DHS guidelines, or Component standards. DHS Components must establish administrative mechanisms that are flexible, appropriate to the nature and timeliness of the disseminated information, and incorporated into Component information resources management and administrative practices. The request for correction and appeal administrative mechanism should be conducted within the Component that disseminated the information.

Overall, OMB and DHS do not envision administrative mechanisms that would burden the Components with frivolous claims. Instead, the correction process should serve to address the genuine and valid needs of DHS and its constituents without disrupting agency processes. In making determinations of whether or not to correct information, Components may reject claims made in bad faith or without justification. Components need undertake only the degree of correction that they conclude is appropriate for the nature and timeliness of the information involved and explain such practices in their annual fiscal year reports to DHS.

A. Request for Correction Process

DHS Components should respond to requests for correction in writing within 60 calendar days of receipt. If the request for correction requires an extended period of time for processing, the Component should notify the petitioner.

The Department considers that the complainant has the burden of demonstrating that the information does not comply with DHS guidelines, OMB guidelines, or Component standards, and that a particular corrective action would be appropriate.

The Component should develop or identify the initial administrative correction request process for affected persons to seek and obtain correction of information that does not comply with OMB Guidelines, DHS Guidelines, or Component standards. The process should specify the name and address of the Component office or point of contact responsible for evaluating and responding to requests for correction of information disseminated. The process should meet the established timeframes for requests, evaluations, and the Component's response.

The process should identify what the petitioner should include in a Request for Correction of Information, including:

- A statement that a request for information is submitted under DHS's (or, if applicable, the Component's) Information Dissemination Quality Guidelines;
- The petitioner's contact information, including: name, mailing address, fax number, or email address, telephone number and organizational affiliation if any;
- Description of the information deemed to need correction and how the information in question affects the petitioner (e.g. how the alleged error harms the petitioner, and/or how the correction will benefit the petitioner).
- The petitioner should clearly identify the report, data set, or other document that contains the information he or she is requesting DHS to correct. The petitioner should be as specific as possible and include such identifying characteristics as: title, date, and manner disseminated (e.g. website, publication).
- Within that document, the petitioner should clearly identify the specific information that he or she wants the Department to correct. The petitioner should be as specific as possible, including such characteristics as the name of the DHS component that originated the data, title, date etc. For example, a petitioner should not rely solely on general statements that allege some type of error. Requests for information that are specific and provide evidence to support the need for correction

will likely be more persuasive than requests that are general, unfocused, or simply indicate disagreement with the information in question.

- The petitioner should specify, in detail, why he or she believes the information in question is inconsistent with DHS's or OMB's information quality guidelines (i.e. how the information fails to meet standards of integrity, utility, and/or objectivity).
- Include a copy of the documentary evidence, or provide a citation to the evidence, the petitioner believes is relevant to the request (e.g., comparable data or research results on the same topic and copies of any professional or academic journal articles cited by the petitioner).
- The petitioner should specify his or her recommendations for what corrections DHS should make to the information in question and the reasons for believing that these recommended corrections would make the information consistent with DHS's and/or OMB's information quality guidelines

In advance of DHS Components establishing their information quality guidelines and administrative mechanisms to address information correction requests, petitioner inquiries can be routed through the Department via mail, e-mail, or fax, as indicated below.

Mail: Department of Homeland Security
Chief Information Office
245 Murray Lane, SW
Washington, DC 20528

E-mail: DHS.InfoQuality@dhs.gov

Fax: 202-447-0338

Website: DHS website for IQ to be inserted

PRIVACY ACT STATEMENT

AUTHORITY: Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554, app C § 515, 114 Stat. 2763A-153-4 (Dec 21, 2000)); and OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies; Republication (67 FR 8452, February 22, 2002).

PRINCIPAL PURPOSE(S): This information is being collected in order to process your request, allow the Department to maximize the quality of disseminated information, and to reply to you accordingly. The information you furnish is rarely used for any purpose other than to process and respond to your request. Please do not submit your Social Security Number.

ROUTINE USE(S): The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using this information as necessary and authorized by the routine uses published in DHS/ALL – 002 DHS Mailing and other lists systems (73 FR 71659, November 25, 2008). For example, we may disclose information to a congressional office in response to an inquiry made on your behalf, to appropriate law enforcement when the information appears on its face or in conjunction with other information to violate the law, to the Department of Justice, a court, other tribunal when information is relevant and necessary to litigation, or to a contractor or other Federal agency to help accomplish a function related to this process.

DISCLOSURE: The disclosure of the information here is voluntary; however, failure to provide the information requested may prevent your request from being processed, the

Department from maximizing the quality of disseminated information, and in responding to your request.

When developing their request for corrections and appeals processes, Components should include the appropriate contact information for the Information Quality point of contact within that Component. The Component instructions for the public to submit requests for correction and appeals should also include the appropriate Privacy Act language referenced above.

B. Administrative Appeal Process

DHS Components should develop an administrative appeal process in the event a petitioner is not satisfied with the reply to the correction request. When the response to the correction request is provided to the petitioner it should also notify the petitioner of the right to appeal, and include instructions on how to submit an appeal.

After the petitioner receives a decision from the Component on a request for correction, if he or she wishes to appeal that decision, the petitioner should send their appeal of the ruling within 45 business days in accordance with the instructions in the initial Component reply. In advance of Components establishing their administrative processes for managing appeals, all appeal requests should be sent through the same routing as the initial correction request (see above). The Component should respond to appeals and/or requests for correction in writing within 60 calendar days of receipt. If the response requires an extended period for processing, the Component must notify the petitioner. The Component's appeal process should include a final judgment by an official independent from the initial response. In the absence of an existing applicable reconsideration process, the DHS component will designate a reconsideration official. This official should be someone who can offer objectivity (i.e., was not involved in making the decision on the original request for correction or in producing the underlying information) and who has a reasonable knowledge of the subject matter. The official can either be within the DHS Component to which the request for reconsideration pertains or in another DHS Component.

C. Information on which the Agency Requested Public Comments

Information in rulemakings and other documents concerning which public participation and comment are sought are subject to these guidelines. However, the Department may respond to requests for correction concerning such information through a different process than what we use for other types of information. When the Department seeks public comment on a document and the information in it (e.g., a notice of proposed rulemaking (NPRM), studies cited in an NPRM, a regulatory evaluation or cost-benefit analysis pertaining to the NPRM, a draft environmental impact statement, or a request for comments on an information collection subject to the Paperwork Reduction Act), there is an existing mechanism for responding to a request for correction. This mechanism is a final document that responds to public comments (e.g., the preamble to a final rule).

Consequently, the DHS component response to a request for correction of such information will normally be incorporated in the next document we issue in the matter. The Department would consider making an earlier response, if doing so (1) would not delay the issuance of the final action in the matter; and (2) the Department determined that there would be an unusually lengthy delay before the final document would be issued or the requester had persuaded the Department that there was a reasonable likelihood that the requester would suffer actual harm if the correction were not made before the final action was issued.

If there is a request for reconsideration of information relating to a final rule a DHS component has issued and the DHS component has an existing process for handling requests for the reconsideration of a final rule, the DHS component could use that process. If the information relates to a final Environmental Impact Statement, the DHS component may handle the reconsideration request as though it were a request for a Supplemental EIS.

REPORTING REQUIREMENTS

DHS Component Reporting Requirements to the Department

All DHS Components will post their information quality standards on the Internet. These documents will be elements of the required DHS periodic reporting to OMB. Periodically, the DHS Office of the Chief Information Officer (OCIO) will conduct an internal review to identify necessary updates of the standards to maintain quality and accuracy of the Information Review Process and the Administrative Correction Request Mechanism.

On a fiscal-year basis, DHS Components should submit a report to the Deputy Assistant Secretary for Information Systems and Chief Information Officer (DASIS/CIO). The reports should identify the number and natures of requests for correction received regarding compliance with the guidelines, and explain how the requests for correction were resolved. DHS Components should submit the reports by November 1 of each following year. Periodically, there will be internal review and update of the guidelines to ensure and maximize the quality of disseminated information.

Department Reporting Requirements to OMB

On a fiscal year basis, the DASIS/CIO will submit a report to the Director of OMB providing information on the number and nature of requests for correction and how such requests were resolved. DASIS/CIO will submit the reports no later than January 1, of each following year with the first report due as requested by OMB.

RESPONSIBILITIES

The DASIS/CIO shall:

- provide management and oversight to the DHS-wide implementation of the law;
- develop and issue final information quality guidelines and post them on the Internet;
- coordinate standards formulation and posting by the DHS Components; and
- report to the Director of OMB the number of and nature of requests for correction regarding compliance with the guidelines for the quality of disseminated information and how such requests were resolved.

DHS Components shall:

- develop and issue final implementation plans for ensuring and maximizing the quality, objectivity, utility, and integrity of information, including statistical information, and post them to the Internet;
- develop an administrative mechanism for receiving and responding to information quality requests for correction;
- designate an objective organization responsible to serve as final arbiter regarding an appeal of the Component decision on an information quality request; and designate officials(s) to be responsible for compliance with the information quality processes within their Component and who shall:
 1. maintain quality information procedures and educate officials on their use;
 2. develop and manage an administrative mechanism for receiving and responding to information quality correction requests and appeals;
 3. provide multiple media sources for the filing of correction requests (via mail, Internet, etc.);
 4. post the information quality procedures and the administrative mechanism on the official Internet Web pages;
 5. keep official records on requests for correction and retain statistics necessary for annual reports to DASIS/CIO; and
 6. prepare annual reports to DASIS/CIO.

APPENDIX A - DEFINITIONS

Affected Persons are people 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.

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

Utility refers to the usefulness of the information to its intended users, including the public. In assessing the usefulness of information that the 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 must take care to ensure that transparency has been addressed in its review of the information.

Objectivity involves two distinct elements: presentation and substance.

- "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 must also be disseminated in order to ensure an accurate, clear, complete, and unbiased presentation. Also, the 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.
- 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 shall be generated, and the analytic results shall be developed, using sound statistical and research methods.

i. 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 agency-sponsored peer review is employed to help satisfy the objectivity standard, the review process employed shall meet the general criteria for competent and credible peer review recommended by OMB-OIRA to the President's Management Council (9/20/01) (http://www.whitehouse.gov/omb/inforeg/oira_review-process.html), namely, "that (a) peer reviewers be selected primarily on the basis of necessary technical expertise, (b) peer reviewers be expected to disclose to agencies prior technical/policy positions they may have taken on the issues at hand, (c) peer reviewers be expected to disclose to agencies their sources of personal and institutional funding (private or public sector), and (d) peer reviews be conducted in an open and rigorous manner."

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

- With regard to analysis of risks to human health, safety and the environment maintained or disseminated by the agencies, agencies shall either adopt or adapt the quality principles applied by Congress to risk information used and disseminated pursuant to the Safe Drinking Water Act Amendments of 1996 (42 U.S.C. 300g-1(b)(3)(A) & (B)). Agencies responsible for dissemination of vital health and medical information shall interpret the reproducibility and peer-review standards in a manner appropriate to assuring the timely flow of vital information from agencies to medical providers, patients, health agencies, and the public. Information quality standards may be waived temporarily by agencies under urgent situations (e.g., imminent threats to public health or homeland security) in accordance with the latitude specified in agency-specific guidelines.
- If, at the end of the public comment period, an agency is not prepared to identify what kinds of original and supporting data will be subject to the reproducibility standard, then the agency must include in its guidelines a statement to the effect that the agency shall assure reproducibility for

those kinds of original and supporting data according to - commonly accepted scientific, financial, or statistical standards

Integrity refers to the security of information -- protection of the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.

Information for purposes of the data quality law, Section 515, means 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 130 definition, 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.

Government information means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Information dissemination product means 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.

Dissemination means agency initiated or sponsored distribution of information to the public (see 5 C.F.R. 1320.3(d) (definition of "Conduct or Sponsor"). Dissemination does not include distribution intended to be limited to: government employees or agency contractors or grantees; intra- or inter-agency use or sharing of government information; and responses to requests for agency records under the Freedom of Information Act, the Privacy Act, the Federal Advisory Committee Act or other similar law. This definition also does not include distribution intended to be limited to: correspondence with individuals or persons, press releases, archival records, public filings, subpoenas or adjudicative processes.

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.

Reproducibility means that 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 shall provide 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.

APPENDIX B –REFERENCES

Public Law 104-13, "Paperwork Reduction Act of 1995."

(Site for public laws enacted from the 104th Congress to the present:
<http://www.gpoaccess.gov/plaws/index.html>)

(OMB circulars can be found at [http://www.whitehouse.gov/omb/circulars/.](http://www.whitehouse.gov/omb/circulars/))

(OMB site for Federal Register announcements can be found at
http://www.whitehouse.gov/omb/fedreg_default/)