Key Issues Guidance

Version 1.0

For more information, go to: www.ise.gov

Table of Contents

Guidance Papers Outline ii

Note on ISE Privacy and Civil Liberties Implementation Guidance ii

A. REDRESS A1-A8
GUIDANCE 1
BACKGROUND AND COMMENTARY A3
RESOURCES AND TOOLS A7

B. NOTICE MECHANISMS B1-B9
GUIDANCE B1
BACKGROUND AND COMMENTARY B4
RESOURCES AND TOOLS B9

C. DATA QUALITY C1-C12
GUIDANCE C1
BACKGROUND AND COMMENTARY C4
RESOURCES AND TOOLS C12

D. DATA SECURITY D1-D9
GUIDANCE D1
BACKGROUND AND COMMENTARY D3
RESOURCES AND TOOLS D9

E. ACCOUNTABILITY, ENFORCEMENT, AND AUDIT E1-E10
GUIDANCE E1
BACKGROUND AND COMMENTARY E4
RESOURCES AND TOOLS E10

Guidance Papers Outline

Background

- The guidance papers in these sections provide additional in-depth guidance on selected areas of the ISE Privacy Guidelines. They were developed through extensive review and coordination by interagency working groups consisting of Federal privacy and civil liberties officials and attorneys and were reviewed and approved by the ISE Privacy Guidelines Committee and the Information Sharing Council.

Purpose

- The purpose of the guidance papers is to provide guidance in interpreting certain ISE Privacy Guidelines requirements and to outline possible methods or "best practices" to assist agencies in implementing those requirements. These guidance papers do not create new or modify existing policy.

Policy Guidance

- The **policy guidance section** identifies the core, or basic, elements that an agency must address in order to comply with key requirements of the ISE Privacy Guidelines that are the subject of a guidance paper. It also identifies optional suggested elements that contribute to the formulation of an exemplary privacy, civil rights, and civil liberties protection policy.

Background and Commentary

- The **background and commentary section** provides additional background information on the subject area, including its relationship to the Federal Information Processing Standards (FIPS), the background rationale for the ISE Privacy Guidelines provision, and a discussion of some of the key issues in that subject area. This section also cites resource documents and provides appropriate links.

Resources and Tools

- The **resources and tools section** provides helpful checklists, guidelines, documents, and best-practices information designed to assist agencies in formulating and implementing sound privacy, civil rights, and civil liberties policies.

Note on ISE Privacy and Civil Liberties Implementation Guidance

The ISE Privacy Guidelines contain references to requirements that agencies put in place—policies and procedures—as appropriate and consistent with their legal authorities and missions. Such references are not intended to imply that agencies are required to adopt policies and procedures that would impair the agencies' abilities to exercise their statutory authorities and responsibilities, including the ability to claim exemptions under the Privacy Act of 1974 or to comply with the requirements of any other law, or that

would negatively affect their position in litigation or administrative proceedings. As noted in Section 13 (d)(iv) of the ISE Privacy Guidelines: "These Guidelines…are intended only to improve the management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person."

REDRESS

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 8, provide that:

> To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

As the ISE is developed, individuals may experience circumstances that lead them to question whether protected information (PI)[1] about them might be erroneous, improperly collected, or inappropriately shared or used as part of the ISE, and they may wish to have the situation corrected. Because individuals will not always know the source of the information, complaints most likely will be lodged with the Federal agency which the complainant believes is responsible, rather than with the agency which originated the information and made it available in the ISE. Accordingly, in implementing Section 8, Federal agencies should review their existing complaint-handling procedures to determine whether they accommodate issues pertaining to PI shared in the ISE. The objective is to ensure that internal and external processes exist for handling complaints involving information originating with another agency and for assisting other agencies in receipt of complaints involving information for which an agency is the source. As

[1] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

needed, agencies shall establish procedures appropriate for addressing complaints arising from the sharing of PI in the ISE but only to the extent such procedures do not conflict with legal authorities and mission requirements.

Redress has been recognized as a useful mechanism to improving data integrity by ensuring data is current, complete, and accurate. However, as noted, this guidance is intended only to assist agencies in implementing the ISE Privacy Guidelines—it neither affects any existing agency policy or Privacy Act exemptions, nor is it intended to create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, entities, officers, employees, or agencies or any other person.

Agency ISE redress procedures should address the following core elements:

Core Elements

1. A description of the existing procedures for addressing complaints arising under the Constitution (including nonprivacy civil rights and civil liberties), Privacy Act, or other statutes (including civil rights and civil liberties statutes).

2. A description of policies, procedures, and personnel dedicated toward addressing complaints resulting from the agency's use of PI originating from another agency (if any).

3. A description of policies, procedures, and personnel dedicated toward assisting other agencies to address matters involving PI an agency provided through the ISE (if any).

4. A description of procedures (as needed) developed and implemented for addressing complaints regarding PI in the ISE that are not otherwise covered by existing procedures (see 2 and 3 above).

Additional Considerations

1. Identify record-keeping practices and objectives (i.e., improving processes).

2. Develop and disseminate (via public affairs office, privacy office, civil liberties/civil rights office, Equal Employment Opportunity [EEO] office, Web page, and other) information regarding agency policy/process for addressing PI/ISE-related complaints.

BACKGROUND AND COMMENTARY[2]

Section 8 of the ISE Privacy Guidelines states the following with respect to redress:

> Redress. To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

The persons covered by these Guidelines are described in paragraph 1(b) as follows:

> *Applicability*. These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

The ISE Privacy Guidelines require each agency participating in the ISE, consistent with its legal authorities and mission requirements, to provide "redress"; i.e., a procedure for addressing complaints relating to PI in the ISE. The ISE Privacy Guidelines contemplate that agencies will afford redress with respect to issues involving information privacy, as well as alleged infringements of civil rights, civil liberties, and other legal rights protected by law. Therefore, as appropriate, agency procedures would permit persons to use the agency's existing complaint/review procedures or any supplementary procedures developed for the ISE to address such complaints as alleged racial, ethnic, or religious profiling or retention in the ISE of information that has been expunged or determined to have been illegally collected.

Many participating ISE agencies already have in place procedures for handling all manner of complaints, including privacy, civil rights, and civil liberties unrelated to the ISE.[3] The redress procedures contemplated by the ISE Privacy Guidelines are limited to situations involving complaints that the agency determines implicate PI in the ISE (although not necessarily under the control of the agency receiving the complaint). The ISE policy requirement to implement internal complaint-handling procedures for ISE-

[2] The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[3] H.R. 1, Title VIII, Section 803, amends Section 1062 of the IRTPA to require that named Federal agencies "(3) ensure that such department, agency, or element has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege such department, agency, or element has violated their privacy or civil liberties."

related issues neither alters agency rules regarding record access or other rights nor requires agencies to either acknowledge the existence of records or inform complainants of case status or resolution where no such right currently exists. As is true under existing processes, many information privacy, Privacy Act, or civil rights and civil liberties complaints identified as involving PI in the ISE will not result in the complainant being informed of measures the agency takes to investigate a complaint, rectify an alleged error, or remedy an issue.

Because individuals and entities covered by these guidelines often may not recognize that there is any relationship between the complaint and the ISE, agencies must establish, as part of their procedure to address complaints, a process that will identify those complaints that are related to PI in the ISE. These complaints generally will be received through existing agency avenues of redress (e.g., Privacy Act requests, existing agency civil rights and civil liberties processes). Once an agency determines that a complaint, which may be received as a general complaint, concerns PI originating with the agency or obtained through the ISE, the principles of ISE redress require the agency to coordinate with all involved agencies to investigate and correct (or remove) any identified information deficiencies.

Agencies must review their existing complaint policies and procedures to ensure that processes exist to identify complaints involving PI in the ISE and to bring them to the attention of the agency's ISE Privacy Official or designee. (See Data Quality issue paper addressing the ISE Privacy Official's responsibility for data quality.) Thus, the ISE Privacy Guidelines' focus is on providing a process by which complaints implicating PI in the ISE are identified and addressed.

The ISE Privacy Guidelines protect the information privacy and other legal rights of United States citizens and lawful permanent residents and, for the intelligence community, United States persons. However, these categories of PI may be expanded to include other information that the United States government expressly determines by Executive Order, international agreement, or other similar instrument shall be covered by the ISE Privacy Guidelines. Indeed, many agencies share PI pursuant to international agreements that allow foreign nationals access to review procedures (e.g., the agreement with the European Union [EU] involving Passenger Name Records). Where a complaint/review process is required by international agreement, special procedures may be employed for foreign nationals (to the extent that such details are not spelled out in the agreement).

The following is a list of authorities that may assist ISE participants in developing their redress policies and procedures for PI in the ISE:

Executive Orders

Executive Order 12333, *United States Intelligence Activities,* December 4, 1981, as amended.
http://www.whitehouse.gov/news/releases/2004/08/20040827-6.html

Executive Order 13353, *Establishing the President's Board on Safeguarding Americans' Civil Liberties,* August 27, 2004.
http://www.whitehouse.gov/news/releases/2004/08/20040827-3.html

Executive Order 13356, *Strengthening the Sharing of Terrorism Information to Protect Americans*, August 27, 2004.
http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html

Executive Order 13311, *Homeland Security Information Sharing,* July 29, 2003.
http://a257.g.akamaitech.net/7/257/2422/20apr20040800/edocket.access.gpo.gov/cfr_2004/janqtr/pdf/3CFR13311.pdf

Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October, 25, 2005.
http://www.ise.gov/docs/eo%2013388%20-%2010252005.pdf

Policy Guidance and Standards

OMB *Privacy Act Implementation, Guidelines, and Responsibilities* ("OMB Guidelines") 40 *Federal Register* 28,948 and 28,965 (July 9, 1975).
http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf

U.S. Department of Homeland Security (DHS) Privacy Policy Guidance Memorandum, 2007-1, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.*
http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information.*
http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf

Memorandum of Understanding on Terrorist Watchlist Redress Procedures.
http://www.fbi.gov/terrorinfo/counterrorism/redress_mou.pdf

Commentators

Paul Rosenzweig and Jeff Jonas, *Correcting False Positives: Redress and the Watch List Conundrum*, June 17, 2005 (Heritage Foundation).
http://www.heritage.org/Research/HomelandDefense/upload/79671_1.pdf

Markle Foundation, *Implementing a Trusted Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability*, February 2006.
http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf

Center for Democracy and Technology, *Analysis of Privacy Guidelines for the Information Sharing Environment for Terrorism Information*, February 2, 2007.
http://www.cdt.org/security/20070205iseanalysis.pdf

Web Sites—Examples of Federal Agency Redress Policies

DHS Traveler Redress Inquiry Program (DHS TRIP)—single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—such as airports and train stations—or crossing U.S. borders.
http://www.tsa.gov/travelers/customer/redress/index.shtm

Federal Bureau of Investigation (FBI), Terrorist Screening Center, Redress Procedure.
http://www.fbi.gov/terrorinfo/counterrorism/redress.htm

RESOURCES AND TOOLS

In developing their ISE redress procedures, agencies may wish to use the following checklist and consider the following specific matters:

Core Elements

1. Describe existing redress and complaint procedures:
   a. Identify all agency-internal avenues for handling complaints (i.e., for all manner of complaints cognizable under statute or regulation or policy):
      (i) Civil Rights/Civil Liberties
      (ii) Privacy Act
      (iii) EEO
      (iv) OIG
      (v) Ombudsman
      (vi) Other
   b. Identify all interagency complaint initiatives that your agency supports:
      (i) DHS Traveler Redress Inquiry Program (TRIP)
      (ii) TSC Terrorist Watchlist Redress Process (MOU)
      (iii) Other

2. Describe policies, procedures, and resources for identifying and addressing PI/ISE-related complaints resulting from the agency's use of PI originating elsewhere.

3. Describe policies, procedures, and resources for assisting other ISE agencies to address complaints arising from their use of PI originating with your agency.

4. Establish procedures (as needed) for addressing privacy or civil liberties complaints relating to PI in the ISE and not otherwise subject to existing procedures:
   a. Provide identity and contact information for agency office of the ISE Privacy Official—e.g., a mailing address (USPS or e-mail) and/or a telephone number(s) of responsible staff.
   b. Ensure that all agency complaint-handling components are familiar with the ISE and understand when a complaint received implicates PI subject to ISE redress.
      - Establish process/information to assist non-ISE-complaints staff in identifying when a complaint involves PI in the ISE.
   c. Establish appropriate liaison with ISE participants from which data will likely originate to facilitate complaint investigation processes.
      - Provide a point of contact and responsible official to ensure appropriate reciprocal support to complaint recipients.

d. Explain processes for coordinating investigation of PI/ISE-related complaints both internally and externally.
e. Develop tools required under the Privacy Act for administering the PI/ISE complaint "program," such as:
   (i) Establish or identify an appropriate system of records to maintain complaints and related information.
   (ii) Ensure that the system of records notice associated with the redress system contains a routine use to allow disclosure of complaint and personally identifiable information to other agencies and organizations to the extent necessary to investigate and address the complaint.
   (iii) Identify records retention obligations.
f. Develop procedures for responding to identified ISE-related complaints.
   (i) Leverage existing agency procedures for establishing/verifying identity or status where appropriate.
   (ii) Develop protocol for acknowledging complaint.
      (a) May wish to articulate scope of redress available:
         - Investigation of alleged errors.
         - Correction of alleged errors/removal of data.
         - Notification of correction to originator and downstream recipients of record.
      (b) May wish to articulate limits of redress afforded:
         - No remedy for underlying injury.
         - No right of action.
         - Particular forms of redress (e.g., right of access to records, notice of resolution of complaint, explanation of investigatory process) may be unavailable given national security, law enforcement equities, or other security considerations relating to terrorism.

Additional Considerations

1. Identify record-keeping objectives intended to enhance ISE processes:
   a. Record PI/ISE complaints received and disposition.
   b. Maintain unresolved PI/ISE complaints.
   c. Examine policy/process changes (if any) needed for PI/ISE review process.

2. Develop outreach/public awareness materials regarding agency PI/ISE redress framework:
   a. Explain process for identifying ISE-related complaints.
   b. Explain processes for investigating and addressing complaints, internally and externally.
   c. Explain "redress" available; i.e., data quality activities

NOTICE MECHANISMS

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 4(b), provide the following Notice Mechanisms requirement:

> b. *Notice Mechanisms.* Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:
>
> (i) The information pertains to a United States citizen or lawful permanent resident;
> (ii) The information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and
> (iii) There are limitations on the reliability or accuracy of the information.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

Section 4(b) of the ISE Privacy Guidelines recognizes that enabling agencies to determine important characteristics of protected information (PI)[4] available in the ISE—

[4] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly

such as the status of an individual; any restrictions on access, use, or disclosure of PI; and any limitations on its reliability and accuracy—will promote a trusted information sharing environment as recipient agencies are made aware of these aspects of PI and can determine whether access to, use of, and further disclosure of the data are consistent with agency missions and applicable legal requirements. Providing restrictions and limitations on information as part of a record, data set, or record system will also serve to mitigate potential risks arising from information sharing activities for all agencies participating in the ISE.

This ISE Privacy Guidelines Notice Mechanisms Guidance comports with the proposed marking of Controlled Unclassified Information (CUI) recommended under the framework described in the proposed Presidential Guideline 3 report, *Standardized Procedures for Sensitive But Unclassified (SBU) Information* (issuance pending). While the proposed CUI framework under Guideline 3 contemplates a limited set of approved "markings" reflecting handling and dissemination requirements, the elements of notice set forth above from the ISE Privacy Guidelines relating to the status of an individual and reliability and accuracy of the information are intended to reflect the nature and quality of the information itself and to be incorporated within an individual record, data set, or record system. These notice mechanisms for privacy requirements are not a handling or dissemination requirement. This guidance should be read in conjunction with the proposed CUI framework and should not be read to foreclose the possibility that notice of "specific information privacy or other similar restrictions on access, use, or disclosure" may be addressed through a CUI marking in the future.

To incorporate appropriate notice, agencies creating reports or disseminating products containing PI in the ISE may continue their customary practices in providing information about their individual records, data sets, or record systems that assists in determining whether the information pertains to an individual's status, any restrictions on access, use, or disclosure, and any limitation on reliability or accuracy of the information. Agencies may use, among other methods, a simple cover sheet to flag such issues or, for electronic information, may use banners, legends, or full-screen notices signaling the general character of and restrictions on access, use, or disclosure of records in the data set or record system.

As may be reasonable and consistent with agencies' legal authorities and mission requirements, agencies engaging in the ISE should consider adopting mechanisms to provide notice of each of the following core elements of information:

Core Elements

1. Status of record subject(s):
   a. U.S. citizen
   b. Lawful permanent resident (LPR)

---

determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

c. Noncitizen or non-LPR protected by treaty or international agreement
d. Undetermined

2. Restrictions on access, use, or disclosure:
   a. Nature of restriction
   b. Source of restriction

3. Reliability and accuracy of information:
   a. Nature of the source—indicating the origin of the information
   b. Confidence—source reliability and content validity
   c. Data quality—inconsistencies or other accuracy concerns based on:
      (i) Notice received from previous recipients of the data
      (ii) Disagreements about accuracy received from the record subject or other person negatively impacted by the record
      (iii) Evaluation of data in context with other existing records (See Data Quality Guidance)
      (iv) Results of compliance reviews or external audits

Additional Considerations

1. Basic source and point-of-contact information
   a. Originating department, component, or office
   b. Agency system from which information is disseminated
   c. Date of collection/date last used to make a determination about an individual, if applicable
   d. Title/contact for questions about the information or access request, if appropriate

2. Date of last data accuracy review conducted in accordance with agency policy and procedure (see Data Quality Guidance)

BACKGROUND AND COMMENTARY[5]

Background and Purpose

In the ISE, the information that is accessed or disseminated (disclosed) comes from numerous sources and often includes (1) protected information (PI), (2) information to which information privacy or other legal protections have been extended, and (3) information for which the status is undetermined or is not privacy-protected. Consequently, ISE participants may be bound by various legal requirements that govern access, use, and disclosure. The quality of the information in the ISE will also vary in reliability and accuracy. Therefore, as information is disclosed in the ISE, the ISE Privacy Guidelines require agencies to implement mechanisms to indicate to recipients whether information disclosed pertains to a U.S. citizen or lawful permanent resident; whether there are legal requirements that protect information privacy or other legal rights of the subject or restrict access, use, or disclosure of the information; and whether the source or providing agency considers the information to be of limited reliability or accuracy.

The purpose of this document is not to examine the range of notice mechanisms technology or to list all of the specific restrictions that might apply with respect to access, use, and disclosure of information in the ISE. Instead, this document focuses on the information about PI that could be included in individual records, data sets, or record systems that may be shared in the ISE.

In the ISE, information regarding PI; any specific information privacy; or other similar restrictions on access, use, or disclosure, and limitations on the reliability or accuracy of the information may be incorporated in a record, data set, or record system before it flows from its originating source or other provider to its end user.

Nature of the Information—Identify Status of Individuals

The status of data subjects may determine the degree of protection, if any, that they will receive in the ISE. Therefore, notice regarding limitations on access, use, or dissemination will necessarily begin with a determination of whether the information applies to U.S. citizens, lawful permanent residents (LPRs), or non-U.S. citizens who are not LPRs but who may, nevertheless, receive protection in the ISE. Suggested categories include:

[5]The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. This section neither establishes policy under the ISE nor is binding on any department or agency participating in the ISE. It is not a binding interpretation of law, regulation, or policy.

1. U.S. citizen[6]
2. Lawful permanent resident[7]
3. Non-U.S. citizen or non-LPR protected by treaty or other international agreement[8]
4. Undetermined

Limitations on Access, Use, or Disclosure—Identify Restrictions on Access, Use, or Disclosure:

Identify any legal restrictions on access, use, or disclosure of PI and the nature of the restrictions. There are numerous statutory and regulatory limitations that pertain to different types of information that may be shared in the ISE.[9]

Limitations on Reliability and Accuracy (Validity)—Identify Confidence Limitations:

There are existing efforts in some law enforcement and intelligence agencies at the Federal, state, local, and tribal levels to provide law enforcement information in a way that conveys to the recipient the originating agency's level of confidence in the information; i.e., its assessment of the information's (source) reliability and (content) validity. The U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative's *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*[10] (hereinafter "Justice PCRCL Policy Templates") recommends that the following assessment typology be incorporated into the body of the record as appropriate to the nature of the information and the level of protection required:

---

[6] U.S. citizenship can be obtained in one of two ways: (1) by birth, either within the territory of the United States or to U.S. citizen parents, or (2) by naturalization. http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=96719c7755cb9010VgnVCM10000045f3d6a1RCRD&vgnextchannel=96719c7755cb9010VgnVCM10000045f3d6a1RCRD. See also United States Immigration and Nationality Act, Title 8 of the U.S. Code (8 U.S.C.).

[7] According to United States Citizenship and Immigration Services (USCIS), "[A] lawful permanent resident is a foreign national who has been granted the privilege of permanently living and working in the United States." http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=077566 7706f7d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=4f719c7755cb9010VgnVCM10000045f3d6 a1RCRD

[8] Individuals who are not U.S. citizens or lawful permanent residents may receive certain protections in the ISE under the terms of an international agreement (e.g., the agreement with the EU involving Passenger Name Records).

[9] See "2006 Interagency Assessment of Federal Privacy and Civil Liberties Policies that Impact Information Sharing," Privacy and Civil Liberties Implementation Manual, Tab V, Section D2.

[10] DOJ's Global Justice Information Sharing Initiative, *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*, September 2006, at p. 17. http://www.it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf

1. Nature of the Source. Nature of the source simply identifies the origin of the information.
   a. Anonymous tip
   b. Informant
   c. Interview or written statement (subject, victim, witness, etc.)
   d. Public records (space should be provided for identifying the government system from which the information was derived because that may bear on its reliability)
   e. Private sector (notice should be given if the information was collected from a data aggregator or broker)
   f. Other (please specify)

2. Source Reliability. Source reliability addresses the consistency of the content validity of information obtained from a particular source over time.
   a. Reliable—the reliability of the source is trusted or has been well tested in the past
   b. Usually Reliable—the source can usually be relied upon
   c. Unreliable—the reliability of the source has been sporadic in the past
   d. Unknown—the reliability of the source cannot be judged

3. Content Validity. Information content deals with the accuracy or truth of the information independent of its source (i.e., even generally unreliable sources can sometimes provide reliable information).
   a. Confirmed—information has been corroborated by an investigator or
   b. Another reliable source
   c. Probable—the information is consistent with past accounts
   d. Doubtful—the information is inconsistent with past accounts
   e. Cannot be judged—the information cannot be judged

This type of assessment allows investigators to determine the extent to which they may rely on the information and the extent to which verification from other sources will be required.

The ISE Data Quality Guidance provided at Divider VI, Tab C, of the Privacy and Civil Liberties Implementation Manual (PM-ISE 2007) suggests additional considerations regarding notice of information accuracy, relevancy, timeliness, and completeness; e.g., based on specific challenges to accuracy of the data received from recipient entities or record subjects or unresolved concerns arising from internal review.

Identify Basic Information

To the extent feasible and consistent with agency legal authorities and mission requirements, agencies should consider developing or expanding individual records, data sets, or record systems to include information about the provider of the data. The following elements of information would facilitate follow-up or inquiry:

1. The name of the originating department, component, or subcomponent.
2. The name of the agency system from which the information is disseminated.
3. The date the information was collected and the date it was last used to make a determination about an individual.
4. The title and contact information for the person to whom questions regarding the information should be directed.

The following is a list of authorities that may assist ISE participants in developing their notice mechanisms policies and procedures for PI in the ISE:

Policy Guidance and Directives

Presidential Guideline 3 report, *Standardized Procedures for Sensitive But Unclassified (SBU) Information* (issue pending), Privacy and Civil Liberties Implementation Manual (PM-ISE, 2007) (see also www.ise.gov).

ISE Data Quality Guidelines, Divider VI, Tab C, Privacy and Civil Liberties Implementation Manual (PM-ISE, 2007) (see also www.ise.gov).

DHS Privacy Office Privacy Policy Guidance Memorandum Number 2007-1, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, January 19, 2007.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

U.S. Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, at p. 23.
http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf (discussing redress issues at the Terrorist Screening Center).

Web Sites

United States Citizenship and Immigration Services Web site:
http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=0775667706f7d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=4f719c7755cb9010VgnVCM10000045f3d6a1RCRD (defining requirements for U.S. citizenship) and

http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=8b76194d3e88d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=4f719c7755cb9010VgnVCM10000045f3d6a1RCRD (defining requirements for becoming a lawful permanent resident).

RESOURCES AND TOOLS

RESERVED

DATA QUALITY

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 5, provide the following Data Quality requirement:

a. *Accuracy*. Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.

b. *Notice of Errors.* Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in Section 12 below).

c. *Procedures.* Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:

(i) Take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;
(ii) Investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and
(iii) Retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This

guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

Section 5 of the ISE Privacy Guidelines requires each agency participating in the ISE to adopt and implement procedures, as appropriate, regarding quality assurance measures to facilitate the prevention, identification, and correction of any errors in protected information (PI)[11] in order to ensure the information is accurate and has not erroneously been shared through the ISE. The full value of the ISE may be realized only if PI shared in the ISE is accurate, relevant, timely, and complete to the extent the providing and receiving agencies' missions require and any information identified as erroneous or deficient is corrected, updated, deleted, or not used, as administratively and technically feasible.[12]

Consistent with legal authorities and mission requirements, agency policies and procedures should address the following core data quality elements for information shared through the ISE:

Core Elements

1. PI originating in the agency is as accurate, complete, and internally consistent as the agency requires for use in making determinations, given its authorities and mission.

2. PI is relevant and timely as appropriate for agency use, and when it becomes outdated or irrelevant for such agency use, it is updated, deleted, or not used in the ISE.

3. PI originating in the agency indicates to recipients any known limitations on its reliability or accuracy (see also Notice Mechanisms Guidance).

[11] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

[12] Erroneous or deficient information does not include information for which the reliability or validity may not be fully established. These elements of confidence in the information are the subject of Notice Mechanisms Guidance implementing Section 4(b) of the ISE Privacy Guidelines.

4. Where feasible, written notice[13] is given to the providing agency's ISE Privacy Official of specific PI that the receiving agency has determined is erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the subject may be affected.

5. Alleged or identified errors or deficiencies in PI about which the agency is notified are investigated in a timely manner.

6. PI an agency investigation determines is erroneous or deficient for its purposes is corrected or deleted, or if not corrected or deleted, the agency refrains from sharing it through the ISE.

7. PI recipients, to the extent they can be identified, are notified of alleged or identified errors or deficiencies in the providing agency's information that has been disseminated in the ISE, including incorrect mergers/matches/insertions of information.

8. Information the agency has matched against or consolidated from multiple sources relates to the same individual.

Additional Considerations

1. The agency maintains a record/accounting of data corrections/ additions provided and/or received.

2. The agency, in addition to providing written notice to the providing agency under Core Element 4 above, provides written notice to the originating (acquiring) agency where such agency is known and is not the providing agency.

[13] Written notice could include any form of nonverbal communication (such as e-mail or formal letter) that is capable of being retained as an official agency record. It is in the agency's discretion to determine who will be authorized to provide written notice to the providing agency and in what form.

BACKGROUND AND COMMENTARY[14]

The core principles for protecting privacy and civil liberties in the ISE require Federal agencies, consistent with agency legal authorities and mission requirements, to "[e]stablish data quality, accuracy, and retention procedures" that reflect basic privacy protections and best practices. The principles established in Section 5, Data Quality, of the ISE Privacy Guidelines, incorporate and build upon the data quality requirements of the Privacy Act of 1974.

The ISE Privacy Guidelines contemplate that Federal agencies will comply with both the Guidelines and all applicable Privacy Act requirements for all information in the ISE. This will require agencies to review their existing data quality policies and procedures and, where necessary, develop new policies and procedures applicable to ISE information that meet each of the requirements for accuracy, notice, information merger protection, investigation of alleged errors and deficiencies, and retention of information that are set forth in Section 5.

Section 8 of the ISE Privacy Guidelines, Redress, requires a procedure for identifying complaints involving PI in the ISE and for bringing them to the attention of the ISE Privacy Official or designee. This individual should be enabled, through the agency's Section 5 policies and procedures, to provide the redress contemplated under Section 8 and the Redress Policy Guidance, thereby furthering the agency's interest in limiting dissemination and maintenance of information in the ISE to information that is accurate, timely, relevant, and complete.

In the Federal government, there are two primary statutes that impose data quality requirements on Federal agencies: (1) the Privacy Act of 1974, P.L. 93-579, as amended, and (2) the Information Quality Act, Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001, P.L. 106-554 (codified at 44 U.S.C. §§ 3504(d)(1) and 3516)).[15]

[14] The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[15] The Information Quality Act (IQA) requires Federal agencies subject to the Paperwork Reduction Act (44 U.S.C. § 3502(1)) to issue guidelines ensuring and maximizing the quality, objectivity, utility, and integrity of information including statistical information disseminated by the agency. The OMB Guidelines implementing the IQA (67 *Federal Register* 8452, February 22, 2002) define the term *dissemination* to mean "agency initiated or sponsored distribution of information to the public." Public dissemination includes posting information on government Web sites and in government manuals that are distributed to the public. However, per the OMB Guidelines, "Dissemination does not include distribution limited to government employees." Consequently, the IQA does not apply to records containing information about individuals that Federal agencies may share only internally or between agencies.

Data Quality Related Provisions of the Privacy Act of 1974

The Privacy Act can generally be characterized as an omnibus "code of fair information practices"[16] for the collection, maintenance, use, and dissemination of information about individuals by Federal agencies. The Privacy Act's protections apply to "individuals," which the act defines as U.S. citizens and lawful permanent residents (LPRs).[17]

The majority of the Privacy Act's provisions are limited to "records" (in paper or electronic form) that are in a "system of records" maintained by a Federal agency. In order to qualify as a "record" under the Privacy Act, the item, collection, or grouping of information must contain an identifying particular assigned to the individual (name, social security number, employee number, finger- or voiceprint, photograph, etc.) and be "about" the individual (i.e., include some descriptive item of information about the individual,[18] such as the individual's education, medical history, employment history, home address, or even any information provided by the system name alone; e.g., "Quarantined Persons"). Furthermore, the "record" must be maintained in a "system of records," which the Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[19]

Federal agencies that maintain systems of records must comply with the Privacy Act's data quality requirements. For example, unless a system of records is exempt (see below), Subsection (e)(5) of the Privacy Act requires that an agency "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[20] Accuracy, timeliness, relevance, and completeness are all elements of data quality. In addition, Subsection (e)(1) requires that an agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive Order of the President."[21]

---

[16] In 1972, a U.S. Department of Health, Education, and Welfare advisory committee proposed a "Code of Fair Information Practices." These practices formed the basis for the Privacy Act of 1974, and these "Fair Information Practices" are embodied as principles in the Privacy Act, as well as in a number of subsequent codes related to information collection, security, and privacy.

[17] In some circumstances, agencies may also provide certain Privacy Act protections to non-U.S. citizens and LPRs under the terms of an international agreement or as a matter of policy (see, for example, the agreement with the EU involving Passenger Name Records and DHS Privacy Policy Guidance Memorandum Number 2007-1 *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, January 19, 2007).

[18] OMB Guidelines, 40 *Federal Register* 28,948, 28,951-2 (July 9, 1975).

[19] 5 U.S.C. § 552a(a)(5)

[20] 5 U.S.C. § 552a(e)(5).

[21] 5 U.S.C. § 552a(e)(1).

Subsection (d) of the Privacy Act requires agencies to allow individuals to access information pertaining to them that is maintained in a system of records and to request that the agency amend a record if the individual believes the information is not accurate, relevant, timely, or complete. If the agency refuses to amend the record in accordance with the request, administrative and judicial remedies are provided. Subsections (j) and (k), however, allow agencies to exempt certain records from specified provisions of the act, including Subsections (d), (e)(1), and (e)(5).

In enacting the Privacy Act, Congress recognized that the application of all of the act's requirements to certain categories of records could have undesirable and often unacceptable effects upon certain agencies in the conduct of necessary public business, particularly law enforcement[22] and national security agencies.[23] Consequently, Congress specifically authorized agencies to exempt particular systems of records from certain provisions of the Privacy Act. Nonetheless, no system of records is automatically exempt from any provision of the act. The agency that maintains a system must determine whether the system may be exempted and then promulgate a rule subject to the requirements of general notice and public comment as required by the Administrative Procedure Act, 5 U.S.C. § 551, 553 (1994). The rule must include the specific provisions from which the system is proposed to be exempted and specific reasons why the agency considers the exemption necessary.

---

[22]From OMB Privacy Act Implementation, Guidelines and Responsibilities [hereinafter OMB Privacy Act Guidelines], 40 *Federal Register* 28,948, 28,972 (July 9,1975), concerning provisions to exempt certain law enforcement records:

> This provision allows agency heads to exempt a system of records compiled in the course of an investigation of an alleged or suspected violation of civil laws, including violations of the Uniform Code of Military Justice and associated regulations, except to the extent that the system is more broadly exempt under the provision covering records maintained by an agency whose principal function pertains to the enforcement of criminal laws (subsection (j)(2)) . This exemption was drafted because '[i]ndividual access to certain law enforcement files could impair investigations, particularly those which involve complex and continuing patterns of behavior. It would alert subjects of investigations that their activities are being scrutinized, and thus allow them time to take measures to prevent detection of illegal action or escape prosecution.' (House Report 93-1416, p. 19)

[23]From OMB Privacy Act Guidelines, 40 *Federal Register* at 28,972, concerning provisions to exempt certain national security records:

> Useful guidance in the application of this provision is found in the Senate Committee report discussion of a similar provision on classified materials. 'The potential for serious damage to the national defense or foreign policy could arise if the notice describing any information system included categories or sources of information … or provided individuals access to files maintained about them…. The Committee does not by [the passage of the Privacy Act] intend to jeopardize the collection of intelligence information related to national defense or foreign policy, or open to inspection [classified information] to persons who do not have an appropriate security clearance or need to know.' (Senate Report 93-1183, p. 74)

The exemption provisions are permissive; that is, an agency is authorized, but not required, to exempt a system from all or any portion of selected provisions of the Privacy Act when an agency deems it to be in the best interest of the government and consistent with the act and the OMB Privacy Act Guidelines.[24]

Subsection (e)(6) of the Privacy Act requires that "prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to Subsection (b)(2) [the Freedom of Information Act (FOIA)] of this section, [the agency must] make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes."[25] While this requirement does not apply when information is being shared between Federal agencies, it is not a provision from which an agency can claim exemption. Consequently, an agency that has exempted records from Subsections (d) (access and amendment) and (e)(5) (accuracy, relevance, timeliness) of the act must nevertheless make reasonable efforts to ensure the accuracy, completeness, timeliness, and relevance of the records when it disseminates them outside the agency to authorized recipients, other than other Federal agencies and FOIA requesters.

An individual may bring a civil action against an agency under Subsection (g)(1)(C) of the Privacy Act if the agency "fails to maintain any record concerning [the] individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual."[26]

For guidance in interpreting and applying the Privacy Act's provisions, agencies should consult the Office of Management and Budget's (OMB) Privacy Act guidance and the case law interpreting the act.

In addition to review under the Privacy Act, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires all Federal agencies to inventory their holdings of personally identifiable information and to undertake the following data quality review:

---

[24]The OMB Privacy Act Guidelines, 40 *Federal Register* at 28,971, reflect the need for the exercise of agency discretion. In commenting on this provision, the House Committee noted:

> The Committee also wishes to stress that this section is not intended to require the CIA and criminal justice agencies to withhold all their personal records from the individuals to whom they pertain. We urge those agencies to keep open whatever files are presently open and to make available in the future whatever files can be made available without clearly infringing on the ability of the agencies to fulfill their missions. (House Report 93-1416, p. 19)

[25]5 U.S.C. § 552a(e)(6).

[26]5 U.S.C. § 552a(g)(1)(C).

> Review Current Holdings. Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.…
>
> Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act systems of records notices.

The following is a list of authorities that may assist ISE participants in developing their data quality policies and procedures for PI in the ISE:

Statutes

Privacy Act of 1974, 5 U.S.C. § 552a. http://www.usdoj.gov/oip/privstat.htm

The Information Quality Act, 44 U.S.C. §§ 3504(d)(1) and 3516. (See OMB, *Information Quality: A Report to Congress*, April 30, 2004, detailing implementation of the IQA during Fiscal Year 2003. http://www.whitehouse.gov/omb/inforeg/fy03_info_quality_rpt.pdf (See also Congressional Research Service, *The Information Quality Act: OMB's Guidance and Initial Implementation*, September 17, 2004, CRS-2). http://www.it.ojp.gov/documents/CRS_IQ_Act_OMB_Guidance_and_Implementation.pdf.

Health Insurance Portability and Accountability Act of 1996 (HIPAA), August 21, 1996. http://aspe.hhs.gov/admnsimp/pl104191.htm

Gramm-Leach-Bliley Act (GLB),15 U.S.C. § 6801. http://www.ftc.gov/privacy/glbact/glbsub1.htm

Paperwork Reduction Act, Public Law 104-13, 44 U.S.C. § 3501 *et seq*. http://www.archives.gov/Federal-register/laws/paperwork-reduction/

National Archives and Records Administration, 44 U.S.C. § 2101 *et seq.* http://www.archives.gov/about/laws/nara.html#def (enabling legislation requiring NARA to determine data retention issues).

Regulations and Guidelines

Office of Management and Budget (OMB) *Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal*

Agencies; Republication, 67 *Federal Register* No. 36, at 8452-60. http://www.whitehouse.gov/omb/fedreg/reproducible2.pdf

28 CFR Part 23. http://www.it.ojp.gov/documents/28CFR_Part_23.PDF (requirements for Crime Control Act-funded criminal intelligence systems).

Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), 45 CFR Parts 160 and 164. http://www.hhs.gov/ocr/combinedregtext.pdf

Gramm-Leach-Bliley Privacy Regulations, 16 CFR § 313, 65 *Federal Register* 33646 (May 24, 2000). http://www.infolinkscreening.com/InfoLink/Resources/LegalIssues/PrivacyIssues.pdf

Policy Guidance and Standards

OMB *Privacy Act Implementation, Guidelines and Responsibilities*, 40 *Federal Register* 28948, 28965 (July 9, 1975). http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf

Implementation of the Privacy Act of 1974, Supplemental Guidance, 40 *Federal Register* 5674, (December 4, 1975). http://www.whitehouse.gov/omb/inforeg/implementation1974.pdf

Appendix I to OMB Circular No. A-130, *Federal Agency Responsibilities for Maintaining Records About Individuals.* http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html

OMB *Privacy Act Guidance—Update* (May 24, 1985). http://www.whitehouse.gov/omb/inforeg/guidance1985.pdf

Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 *Federal Register* 25818 (June 16, 1989). http://www.whitehouse.gov/omb/inforeg/final_guidance_pl100-503.pdf

OMB M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management* (June 13, 2005). http://www.whitehouse.gov/omb/memoranda/fy2005/m05-15.html

OMB M03-02, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 30, 2003). http://www.whitehouse.gov/omb/memoranda/m03-22.html

OMB M-01-05, *Guidance on Inter-Agency Sharing of Personal Data—Protecting Personal Privacy*, (December 20, 2000). http://www.whitehouse.gov/omb/memoranda/m01-05.html

OMB M-99-05, *Instructions on Complying With President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"* (January 7, 1999). http://www.whitehouse.gov/omb/memoranda/m99-05.html

OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*. http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf (requiring Federal agencies to review their data holdings and ensure data quality requirements are being met).

DOJ Overview of the Privacy Act of 1974. http://www.usdoj.gov/oip/04_7_1.html (links to discussion and citations to court decisions interpreting agency Privacy Act of 1974 data quality requirements).

DOJ's Global Justice Information Sharing Initiative, *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems* (September 2006), at pp. 4 and 17. http://www.it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf

DOJ's Global Justice Information Sharing Initiative, *Privacy Policy Development Guide and Implementation Templates*, at pp. 7–11, October 2006. http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

DOJ's Global Justice Information Sharing Initiative, Global Privacy and Information Quality Working Group, *Privacy and Information Quality Policy Development for the Justice Decision Maker* (September 2005). https://it.ojp.gov/documents/200411_global_privacy_document.pdf

DOJ's Global Justice Information Sharing Initiative, *Information Quality: The Foundation for Justice Decision Making* (February 2007). https://it.ojp.gov/documents/IQ_Fact_Sheet_Final.pdf

DOJ's Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Illinois IJIS Privacy Policy Subcommittee report on *Privacy Issues Confronting the Sharing of Justice Information in an Integrated Justice Environment*, at p. 3 (October 2005). http://www.icjia.state.il.us/iijis/public/pdf/PRV/PRV_commiteeIssues_September2006.pdf

DOJ Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, at p. 24. http://www.usdoj.gov/oig/reports/FBI/a0534/final.pdf (discussing data quality issues at the Terrorist Screening Center).

U.S. Government Accountability Office (GAO), *Agency and Reseller Adherence to Key Privacy Principles* (April 2006). http://www.gao.gov/highlights/d06421high.pdf

GAO, *Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data* (June 2006). http://www.gao.gov/highlights/d06674high.pdf

GAO Highlights, *Agencies and Resellers Vary in Providing Privacy Protections* (April 2006). http://www.gao.gov/new.items/d06609t.pdf

Other GAO privacy-related testimony and reports can be found at: http://www.gao.gov/docsearch/app_processform.php?app_id=docdblite_topicsearch&submit=search&topic_search=Privacy

RESOURCES AND TOOLS

In crafting any needed ISE data quality policies and procedures for protected information (PI) in the ISE, agencies may wish to adopt some of the following suggested approaches and considerations:

1. Consider whether data quality reviews conducted pursuant to other requirements are current and appropriate in the ISE context, such as:
   a. Computer Matching Agreement
   b. Privacy Impact Assessment
   c. Memorandum of Understanding
   d. OMB Memorandum M-07-16 (May 22, 2007)

2. Articulate a process to identify priority areas for data quality review, such as:
   a. PI residing in systems of records subject to the data quality requirements of the Privacy Act (i.e., records that are not exempt from the Privacy Act's data quality requirements).
   b. PI residing in information systems subject to the data quality requirements contained in international agreements.
   c. Circumstances in which an erroneous record could result in an erroneous decision (versus circumstances permitting a range of accuracy).
   d. Circumstances in which subjective findings are critical and assessment of the author's expertise bears on a determination regarding data quality.

3. Articulate a process to evaluate PI in context with other existing records to detect inconsistencies or other concerns about accuracy.

4. Articulate a process for evaluating the integrity of data matching and merging activities vis-à-vis the identity of the record subject.

5. Articulate a process for correcting, supplementing, or annotating erroneous or deficient PI reported to the agency ISE Privacy Official (regardless of any exemption from data quality standards that may apply).

6. Articulate a process to prevent the use or dissemination of erroneous or deficient PI.

7. Articulate a process to notify a providing or receiving agency's ISE Privacy Official of errors, changes, clarifying or contrary information, or information alerting the recipient agency to possible limitations on the accuracy of the data, such as:

a. Including contrary or qualifying information in order to clarify the information in the record.
b. Clearly identifying opinions as such.
c. Identifying and advising recipients regarding records that are of questionable accuracy or have known limits on their accuracy[27] (see also Notice Mechanisms Guidance).
d. Including in the record a concise statement of any disagreement submitted by a record subject, when appropriate.[28]
e. Providing the last date on which the record was reviewed for accuracy.

8. Articulate a process to ensure timeliness of records maintained and shared, such as:
   a. Refraining from disseminating information known to be outdated.[29]
   b. Revisiting data retention schedules to determine whether shorter retention periods will reduce the number of outdated or irrelevant records.[30]
   c. Developing procedures for handling criminal history record information that has been sealed or expunged by court order.

9. Articulate a process to create an accounting of data quality reviews, identifying the reviewer and dates of correction/notice to providing or recipient agency ISE Privacy Officials.

[27] OMB Guidelines, *supra*, at 40 *Federal Register* 28965.

[28] *Id*. at 28959.

[29] Illinois IJIS Privacy Policy Subcommittee report on *Privacy Issues Confronting the Sharing of Justice Information in an Integrated Justice Environment*, at p. 3 (September 2006) (hereafter "Illinois IJIS Privacy Policy Subcommittee"). http://www.icjia.state.il.us/iijis/public/pdf/PRV/PRV_commiteeIssues_September2006.pdf

[30] Illinois IJIS Privacy Policy Subcommittee, *supra*, at p. 3.

DATA SECURITY

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 6, provide the following Data Security requirement:

> Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

To ensure the viability of the ISE and its use for the purposes intended, protected information[31] and associated information technology systems must be safeguarded from unauthorized access, disclosure, modification, use, or destruction.

The governing legal and regulatory security framework prescribes the process for determining the information security categories and associated information security controls applicable in specific operating environments. This legal and regulatory framework establishes the core elements for agency information assurance policies.

This guidance identifies the security standards that apply to Federal civilian, military, and intelligence information systems.

[31]Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

Core Elements

1. Non-National Security Systems
   a. Security categorization standards (low-, moderate-, high-impact)
      - *Standards for the Security Categorization of Federal Information and Information Systems* (NIST/FIPS 199)
   b. Minimum security requirements (keyed to system impact category)
      - *Minimum Security Requirements for Federal Information and Information Systems* (NIST/FIPS 200)
   c. Implementation of controls (keyed to minimum security requirements)
      - *Recommended Security Controls for Federal Information Systems* (NIST/SP 800-53)

2. National Security Systems
   a. Defense Information Assurance Certification/Accreditation Process (DIACAP)
   b. National Information Assurance Certification/Accreditation Process (NIACAP)
   c. Director of Central Intelligence Directive (CID) 6/3 (*Protecting Sensitive Compartmented Information Within Information Systems*)
   d. National Information Assurance Policy No. 11 (NSTISSP No. 11)

BACKGROUND AND COMMENTARY[32]

Introduction:

Section 6 of the ISE Privacy Guidelines provides the following Data Security requirement:

> Each agency shall use appropriate physical, technical, and administrative measures as required by law and policy to safeguard protected information in the ISE from unauthorized access, disclosure, modification, use, or destruction.

All Federal government systems involved in the ISE operate within environments that impose specific physical, technical, and administrative requirements that will be applicable to protected information (PI) shared in the ISE. Therefore, the purpose of this document is to identify the applicable computer-security requirements and suggest that participants in the ISE renew their focus and attention to this critical issue in order to safeguard PI in the ISE from unauthorized access, disclosure, modification, use, or destruction.

Federal Information and Information System Security Requirements

The Federal Information Security Management Act (FISMA) of 2002 (Title III of the E-Government Act of 2002) requires that all Federal agencies develop and implement agency-wide information security programs. Different types of systems, however, are governed by different security regimes. FISMA requires that all agencies protect Federal information and information systems in any format (electronic, paper, etc.) and follow the standards and guidelines[33] developed by the National Institute of Standards and

---

[32]The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[33]Under certain circumstances, other Federal statutes may impose general security requirements on Federal agencies. These regulations and any new controls they create do not preclude agency responsibilities to implement FISMA. For example, the Privacy Act of 1974 requires that agencies that maintain information in a system of records must:

> Establish appropriate administrative, technical, and physical safeguards to insure [*sic*] the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. 5 U.S.C. § 552a(e)(10)

Additionally, there exist "sectoral" regulations that impose security requirements on entities that handle specific types of information; e.g., health, financial, and criminal intelligence. See *Health Insurance Reform: Security Standards; Final Rule* (a.k.a. the HIPAA Security Rule), 45 CFR Parts 160, 162, and 164 ("standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers"), at

Technology (NIST).[34] FISMA, however, exempts national security systems, as defined in 44 U.S.C. § 3542(b)(2), from NIST requirements. Per National Security Directive No. 42, national security systems are governed by security policies issued by the Committee on National Security Systems and the Director of the National Security Agency. Therefore, this paper will address applicable security requirements for (1) non-national security systems and (2) national security systems.

1. **Non-National Security Systems**

FISMA required NIST to develop Federal security categorization standards for Federal information and information systems according to impact levels. Therefore, in February of 2004, NIST issued Federal Information Processing Standards (FIPS) 199, *Standards for the Security Categorization of Federal Information and Information Systems*. FIPS 199 requires that agencies categorize their information systems as low-impact, moderate-impact, or high-impact as a starting point for ensuring the confidentiality, integrity, and availability of information in the system.

After agencies categorize their system security needs using FIPS 199, they are required to follow the mandatory security requirements contained in FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. FIPS 200 provides minimum security requirements for Federal information and information systems and establishes a risk-based process for determining the security controls necessary to ensure compliance with those requirements.

2. **National Security Systems**

As mentioned previously, FISMA specifically exempts national security systems from NIST requirements.[35] FISMA defines the term *national security system* at 44 U.S.C. § 3542(b)(2). NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System* (August 2003), assists agencies in identifying when they are operating a national security system.

---

http://www.hipaadvisory.com/regs/finalsecurity/finalsecurity.txt; Gramm-Leach-Bliley *Standards for Safeguarding Customer Information; Final Rule*, 16 CFR Part 314 (establishing "standards relating to administrative, technical, and physical information safeguards for financial institutions subject to" Federal Trade Commission jurisdiction) at http://www.ftc.gov/os/2002/05/67fr36585.pdf; and Criminal Intelligence System Operating Policies, 28 CFR §23.20(g), which impose information security requirements on Crime Control Act-funded criminal intelligence systems. http://www.iir.com/28cfr/guideline.htm

[34] "NIST is a non-regulatory Federal agency in the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." http://www.nist.gov/public_affairs/general2.htm

[35] "Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by Section 3542(b)(2) of Title 44, United States Code." *See* 44 U.S.C. § 3549(c)(1).

Agencies that deploy national security systems generally follow one of two different security methodologies: DoD Information Assurance Certification and Accreditation Process (DIACAP) or National Information Assurance Certification and Accreditation Process (NIACAP). With respect to certain types of intelligence information, agencies are also required to meet the security requirements contained in Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information Within Information Systems.*[36]

a. **DIACAP**

DIACAP[37] is the U.S. Department of Defense (DoD) information assurance (IA) certification and accreditation (C&A) process. DIACAP applies to both classified and unclassified[38] DoD information systems.[39] DIACAP is generally used only by defense agencies,[40] but civilian agencies sometimes apply DIACAP principles to their own C&A processes when not inconsistent with NIST guidance.

b. **NIACAP**

NIACAP is based on the National Security Telecommunications and Information System Security Instruction known as NSTISSI No. 1000.[41] NIACAP establishes the minimum national standards for certifying and accrediting certain national security systems. It is used in some form by the U.S. Department of State (http://www.state.gov/m/irm/rls/rm/21907.htm), the U.S. Department

[36]This document can be found at http://ftp.fas.org/irp/offdocs/DCID_6-3_20Manual.htm.

[37]DITSCAP was DIACAP's predecessor methodology. DIACAP superseded DITSCAP.

[38]FISMA specifically exempts DoD unclassified systems from the NIST guidance requirements that generally apply to unclassified systems. *See* 44 U.S.C. § 3543(c)(1).

[39]DoD Instruction Number 5200.40, at 2, § 2.3 ("Shall apply to the acquisition, operation and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information. It applies to any IT or information system life cycle, including the development of new IT systems, the incorporation of IT systems into an infrastructure, the incorporation of IT systems outside the infrastructure, the development of prototype IT systems, the reconfiguration or upgrade of existing systems, and legacy systems.")

[40]DITSCAP "[a]pplies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"), their contractors, and agents." DoD Instruction Number 5200.40, *Information Technology Security Certification and Accreditation Process (DITSCAP*), at 2, December 1997.

[41]This document can be found at http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

of the Treasury, the U.S. Department of Energy, the U.S. Department of Justice, and others as the methodology for protecting their national security systems. NIACAP is not used by DoD or members of the Intelligence Community who process Sensitive Compartmentalized Information (SCI).

c. **Central Intelligence Directive 6/3**

The Director of Central Intelligence issued Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information Within Information Systems*[42] to establish uniform security guidance and requirements for ensuring adequate protection of Sensitive Compartmentalized Information (SCI) and information used in Special Access Programs (SAPs). SCI refers to a method by which certain types of classified information must be handled. It applies primarily to information regarding national security issues or programs that have not yet been publicly acknowledged. SAPs are programs that require extraordinary security requirements.[43]

[42]This document can be found at http://ftp.fas.org/irp/offdocs/DCID_6-3_20Manual.htm.

[43]Army Regulation 380–381, *Special Access Programs*, at http://www.fas.org/irp/doddir/army/ar380-381-old.pdf, provides the following examples of SAPs: (1) a specific technology with potential for weaponization that gives the United States a significant technical lead or tactical advantage over potential adversaries; (2) sensitive technology that is especially vulnerable to foreign intelligence exploitation without special protection; (3) an emerging technology, proposed operation, or intelligence activity risking the compromise of other SAPs; (4) exposure of sensitive activities that could jeopardize the lives of U.S. citizens; (5) a capability that is so unique or sensitive that it requires protection beyond normal procedures; (6) an extremely sensitive activity requiring special protection from disclosure to prevent significant damage to national security or the reputation or interests of the United States; (7) methods used to acquire foreign technology or equipment; and (8) sensitive support to DOD and non-DOD agencies.

The following is a list of authorities that may assist ISE participants in developing their data security policies and procedures for PI in the ISE:

Statutes

Privacy Act of 1974, 5 U.S.C. § 552a(e)(10) (requiring that system of records owners establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records).
http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552----000-.html

Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 *et seq.* (requiring civilian Federal information systems to follow computer security guidance issued by the National Institute of Standards and Technology [NIST]).
http://www4.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003541----000-.html

Clinger-Cohen Act of 1996, 40 U.S.C. § 1401 *et seq.*, Public Law 104-106, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104 as amended by Public Law 104-208, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ208.104.pdf, which amended Public Law 104-106.

Regulations

Health Insurance Reform: Security Standards; Final Rule (a.k.a. the HIPAA Security Rule), 45 CFR Parts 160, 162, and 164 ("standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers").
http://www.hipaadvisory.com/regs/finalsecurity/finalsecurity.txt

Gramm-Leach Bliley *Standards for Safeguarding Customer Information; Final Rule*, 16 CFR Part 314, (establishing "standards relating to administrative, technical, and physical information safeguards for financial institutions subject to" Federal Trade Commission jurisdiction).
http://www.ftc.gov/os/2002/05/67fr36585.pdf

28 CFR § 23.20(g) (imposing security requirements on criminal intelligence systems).
http://www.it.ojp.gov/documents/28CFR_Part_23.PDF

Policy Guidance and Standards

NIST Publications.
http://www.nist.gov/public_affairs/pubs.htm

OMB Circular A-130 *Management of Federal Information Resources*, http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf, and OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security*

Management Act and Agency Privacy Management.
http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf

DoD Instruction Number 5200.40.
http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/i520040p.pdf

National Information Assurance Certification and Accreditation Process (NIACAP).
http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf

Director of Central Intelligence Directive 6/3: *Protecting Sensitive Compartmented Information Within Information Systems.*
http://ftp.fas.org/irp/offdocs/DCID_6-3_20Manual.htm

National Information Assurance Acquisition Policy (NSTISSP No. 11).
http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf

National Security Directive No. 42.
http://www.cnss.gov/Assets/pdf/CNSSD-900.pdf

RESOURCES AND TOOLS

The following information may assist agencies in reviewing their policy issuances and compliance directives regarding the data security requirements appropriate to their operating environments:

Definition of National Security System (NSS):

1. Federal Information Security Management Act (FISMA) of 2002 (Title III of the E-Government Act of 2002), 44 U.S.C. § 3542(b)(2):
   a. Definition—In this subtitle, the term *national security system* means any telecommunications or information system operated by the United States government,
      (i) The function, operation, or use of which—
         (a) Involves intelligence activities;
         (b) Involves cryptologic activities related to national security;
         (c) Involves command and control of military forces;
         (d) Involves equipment that is an integral part of a weapon or weapons system; or
         (e) Subject to Subsection (b), is critical to the direct fulfillment of military or intelligence missions.
      (ii) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
   b. Limitation—Subsection (b)(2)(i)(e) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

2. DIACAP
   a. Applies to unclassified, as well as to classified DoD information systems.
   b. Civilian agencies often apply DIACAP principles to certification and accreditation processes when not inconsistent with NIST guidance.

3. NIACAP
   a. Agencies following NIACAP to certify and accredit NSSs include but are not limited to:
      i. U.S. Department of State (blended with NIST guidance)
      ii. U.S. Department of the Treasury
      iii. U.S. Department of Energy
      iv. U.S. Department of Justice

b. NIACAP is not appropriate for application to systems administering Sensitive Compartmentalized Information (SCI), such as those residing within DoD or at the various Intelligence Community agencies.

4. DCID 6/3
   - Applicable to information systems administering Sensitive Compartmentalized Information (SCI) and information used in Special Access Programs (SAPS).

5. NSTISSP-11
   - Applicable to the acquisition of information technology products for all systems entering, processing, storing, displaying, or transmitting national security information.

ACCOUNTABILITY, ENFORCEMENT, AND AUDIT

GUIDANCE

Requirement

The Information Sharing Environment (ISE) Privacy Guidelines, at Section 7, provide the following Accountability, Enforcement, and Audit requirements:

a. *Procedures.* Each agency shall modify existing policies and procedures or adopt new ones, as appropriate, requiring the agency to:

   (i) Have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;
   (ii) Provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information and, as appropriate, for reporting violations of agency privacy-protection policies;
   (iii) Cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and
   (iv) Designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

b. *Audit*. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

Purpose

This document does not create new or modify existing policy but rather provides guidance interpreting the above ISE Privacy Guidelines requirement and outlines possible methods or "best practices" to assist agencies in implementing this requirement. This guidance will be supplemented as the ISE matures and other technological recommendations are implemented.

General

The policies, procedures, and mechanisms governing the ISE are designed to protect the privacy and other legal rights of Americans and to ensure the timely availability and utility of protected information. To ensure these ends are achieved, agencies are encouraged to integrate enhanced accountability, enforcement, and audit policies and practices for protected information (PI)[44] in the ISE with existing agency compliance verification mechanisms. Where necessary, agencies should develop compliance verification mechanisms specific to their ISE activities. In either case, to ensure an adequate compliance policy/program, agencies should consider incorporating the following core elements:

Core Elements

1. Policy framework that addresses:
   a. Training of personnel authorized to handle PI in the ISE.
   b. Reporting of violations of agency privacy protection policies.
   c. Investigating identified/reported violations of agency privacy protection policies.
   d. Responding to identified/reported violations of agency privacy protection policies.
   e. Cooperating with audits and reviews by appropriate internal and external audit and oversight authorities.
   f. Measures ensuring that the agency ISE privacy official receives copies of all reports/notices regarding alleged errors in PI content that the agency has disseminated in the ISE.

2. Audit:
   Program review framework/inspection process for examining compliance with the ISE Privacy Guidelines in the following areas (ISE Privacy Guidelines section identified):
   a. Compliance with laws [Section 2]
      (Compliance with general and specific laws applicable to the agency)
   b. Purpose limitation (terrorism-related) [Section 3]
   c. Identification of PI [Section 4(a)]
   d. Notice mechanisms [Section 4(b)]
   e. Data quality [Section 5]
   f. Data security [Section 6]
   g. Accountability, enforcement, and audit [Section 7]

[44] Section 1(b) of the ISE Privacy Guidelines defines *protected information* as "information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States. For the intelligence community, protected information includes information about 'United States persons' as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines."

h.	Redress	[Section 8]
i.	Execution, training, and technology	[Section 9]
j.	Public awareness of agency policies and Procedures	[Section 10]

BACKGROUND AND COMMENTARY[45]

Purpose

The purpose of this document is to identify and discuss potential methods and tools that will enable agencies to comply with the accountability, enforcement, and audit requirements set forth in Section 7 of the ISE Privacy Guidelines. There are many existing Federal requirements and processes that agencies can use to conduct effective audit and oversight of compliance with the ISE Privacy Guidelines:

1. Identify the Persons Assigned to Privacy and Civil Liberties Roles:
   a. Section 12(a) of the ISE Privacy Guidelines requires that "[e]ach agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or Executive Order, or as otherwise identified in response to the Office of Management and Budget (OMB) Memorandum M-05-08[46] dated February 11, 2005), shall [unless another official is better situated to perform this role] directly oversee the agency's implementation of and compliance with these Guidelines (ISE Privacy Official)."[47]
   b. The ISE Privacy Guidelines further state that the ISE Privacy Official shall be responsible for ensuring that "(i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these guidelines, and (ii) changes are made as necessary."[48]
   c. In most instances, the ISE Privacy Official's duties will be handled by each agency's statutory privacy officer or the person appointed as the Senior Agency Official for Privacy (SAOP) under OMB M-05-08. Some agencies, however, also have separate

[45] The Background and Commentary section is provided as a resource concerning the general principles applicable to each ISE Privacy Guidelines requirement addressed. It is not a binding interpretation of law, regulation, or policy.

[46] OMB Memorandum 05-08 (M-05-08), *Designation of Senior Agency Official for Privacy*, requires that each executive department and agency appoint a Senior Agency Official for Privacy to oversee privacy development and implementation. OMB guidance specifically requires that the Official's role "include reviewing the agency's information privacy procedures to ensure that they are comprehensive and up-to-date, and where additional or revised procedures may be called for, working with the relevant agency offices in the consideration, adoption, and implementation of such procedures." OMB M-05-08 also requires that this official review existing departmental and component-level privacy policies and procedures to*:* "ensure the agency's full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act."

[47] ISE Privacy Guidelines, Section 12(a).

[48] "The ISE Privacy Official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's [senior ISE official]." ISE Privacy Guidelines, Section 12(a).

components (e.g., the U.S. Department of Homeland Security [DHS] Office for Civil Rights and Civil Liberties) that handle civil rights and civil liberties issues (e.g., racial profiling) that are beyond the scope of the duties of statutory and OMB-required privacy officials. In addition to appointing an ISE Privacy Official, these agencies may want to consider appointing an ISE point person from civil rights and civil liberties offices where those functions are separate from the SAOP or the statutory privacy officer duties.

2. Leverage Existing Agency Training Programs:
   a. OMB M-05-08 privacy officials (who have assumed the role of ISE Privacy Official in most agencies) are also required to "ensure the agency's employees and contractors receive appropriate training and education regarding the information privacy laws, regulations, policies, and procedures governing the agency's handling of personal information."
   b. Agencies generally provide specialized training with respect to one or more of the following: Privacy Act, Freedom of Information Act, E-Government Act, the handling of Sensitive but Unclassified (proposed as Controlled Unclassified Information [CUI]) and classified information, and/or computer security requirements.
   c. These existing training procedures could be enhanced, where necessary, to do the following:
      i. Ensure employee awareness of proper access, use, and disclosure of PI in the ISE.
      ii. Provide training for personnel in agency policies for reporting noncompliance with agency-developed ISE policies and procedures.
      iii. Ensure that employees are aware of penalties for misuse of information in the ISE.
      iv. Use existing or develop modified agency policies for reporting violations of agency ISE privacy and other civil liberties protection policies to designated authorities within the agency.

3. Leverage Existing Internal Agency Processes, Policies and Procedures, and Oversight Resources:
   a. Processes. Existing privacy and other review processes and resources could be leveraged as part of ISE oversight, such as:
      i. Information sharing review boards or councils.
      ii. Privacy Impact Assessment processes.
      iii. Civil rights and civil liberties office review (where separate from the M-05-08 or Privacy Officer functions).
      iv. Data integrity boards.

v. National Security Systems participating in the ISE can leverage the security controls, safeguards, standards, and countermeasures being defined by both the Committee on National Security Systems (CNSS) and the Director of National Intelligence (DNI) Certification and Accreditation (C&A) Transformation initiatives. These initiatives embrace the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) as outlined in Special Publication 800.53.

b. Policies and Procedures. Existing policies and procedures regarding the handling, sharing, and use of sensitive information may provide for oversight, audit, and accountability for PI, but if they do not, they should be amended to provide needed policies and procedures. Where necessary and as appropriate, these amendments could provide for the following with respect to information used and shared in the ISE:

i. Maintenance of records that are available for reasonable audit and inspection by appropriate officials or entities.[49]

ii. "[I]nspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency criminal intelligence information."[50]

iii. Encouragement of active agency employee participation in oversight, enforcement, auditing, and compliance.

iv. Periodic reviews of the content of PI disseminated and received in the ISE in order to ensure compliance with the ISE Privacy Guidelines.

v. Random auditing of audit trails and other information maintained regarding the agency's use and dissemination of PI in the ISE.[51]

c. Oversight Resources. Agency Inspectors General—In addition to ISE privacy officials (who will generally have oversight but not

---

[49] Agency-specific authorities and mission may determine the information to be captured in transaction logs; i.e., the operations, recipients, or communications about which the agency will maintain auditable records. For example, U.S. Department of Justice-funded systems maintaining "criminal intelligence information" must maintain records indicating "who has been given information, the reason for release of the information, and the date of each dissemination." See 28 CFR § 23.20(g).

[50] See U.S Department of Justice, 28 CFR § 23.20(n), which states that:

> A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

[51] Institute for Intergovernmental Research, *28 CFR Part 23 Sample Operating Policies and Procedures*, http://www.iir.com/28cfr/SampleOperatingPolicies.pdf.

auditing functions), most of the Federal participants in the ISE have their own Inspector General's Office. The Inspectors General conduct and supervise audits and investigations relating to the programs and operations of the organizations for which they are responsible. They also recommend policies for activities designed to promote economy, efficiency, and effectiveness in the administration of the programs they oversee.[52]

i. Inspectors General can help to ensure that their agencies comply with the ISE Privacy Guidelines.

ii. Investigations of suspected violations should "focus principally on systemic measures to avoid future violations."[53]

4. Use Existing Tools Available for Implementing Audit and Review Mechanisms to Ensure Accountability, Enforcement, and Audit, such as strong audit trails.[54] As emphasized in the Markle Foundation report, strong audit trails (or logs) are needed to ensure protection of privacy and civil liberties in the ISE.[55] An audit trail is "a record showing who has accessed an IT system and what operations the user has performed during a given period."[56] The audit trail, primarily established for security purposes, allows the project [agency] to track the file, maintain compliance, and notify a recipient if it turns out there is invalid information in a file."[57]

5. Consider Using Emerging Tools and Technologies:
There are many emerging technologies to assist agencies in tracking the ISE in order to ensure accountability, provide enforcement, and

---

[52] 5 U.S.C. § 1 *et seq*. http://www.law.cornell.edu/uscode/uscode05a/usc_sec_05a_01000001----000-.html

[53] *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*, at p. 33. http://www.markle.org/downloadable_assets/nstf_part_1.pdf

[54] OMB M-07-16, May 22, 2007, Attachment 1 C, provides the following "Log and Verify" security requirement to prevent and identify breaches of sensitive Federal information: "Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required."

[55] "Consistent with a vigorous defense against terrorism, these guidelines envision tools that create audit trails of parties who carry out searches, that anonymize and minimize information to the greatest extent possible, and that prevent both the intentional and unintentional dissemination of irrelevant information to unauthorized persons or entities." *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*, at p. 33. http://www.markle.org/downloadable_assets/nstf_part_1.pdf

[56] NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002, at D-1. http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[57] Institute for Intergovernmental Research, *Frequently Asked Questions Regarding 28 CFR Part 23*, FAQ Number 20. http://www.iir.com/28cfr/FAQ.htm#q20

enhance auditing capabilities. Technologies that ISE participants may consider include, but are not limited to:

a. Permissioning systems
b. Hashing
c. Data anonymization
d. Immutable Audit logs[58]
e. Authentication[59]

These tools and technologies may be considered when conducting system development and in the development or modification of agency policies designed to ensure compliance with the ISE Privacy Guidelines.

The following is a list of authorities that may assist ISE participants in developing their accountability, enforcement, and audit policies and procedures for PI in the ISE:

Statutes

Inspector General Act of 1978, 5 U.S.C. § 1 *et seq*.
http://www.law.cornell.edu/uscode/uscode05a/usc_sec_05a_01000001----000-.html

Regulations

28 CFR § 23.20 (requiring that projects maintaining criminal intelligence information ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to ensure against unauthorized access and against intentional or unintentional damage). http://www.it.ojp.gov/documents/28CFR_Part_23.PDF

Policy Guidance and Standards

OMB Memorandum M-05-08 (February 11, 2005), *Designation of Senior Agency Officials for Privacy*, http://whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf (requiring that every Federal agency appoint a Senior Agency Official for Privacy to oversee privacy development, implementation, and oversight).

OMB Memorandum M-07-16 (May 22, 2007), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*,
http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

---

[58]Markle Foundation, *Implementing a Trusted Information Sharing Environment, Using Immutable Logs to Increase Security, Trust, and Accountability* (2006). "Immutable logs are tamper resistant logs of user activity in the information sharing environment. Audit of immutable logs would allow authorized officials to trace the origin of a piece of information, who has accessed it, under what circumstances, pursuant to what authority, and how it actually has been used, thus providing a mechanism to oversee or measure compliance with privacy and security rules. As a mechanism for oversight and review of system usage, immutable logs are a key component of accountability." *Id.* at p, 70.
http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf

[59] ISE Privacy Guidelines, Section 9(c), Technology.

28 CFR Part 23, Sample Operating Policies and Procedures.
http://www.iir.com/28cfr/SampleOperatingPolicies.pdf

Commentators

Markle Foundation, *Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force*, at p. 33.
http://www.markle.org/downloadable_assets/nstf_part_1.pdf (discussing accountability in the Information Sharing Environment).

Markle Foundation, *Implementing a Trusted Information Sharing Environment, Using Immutable Logs to Increase Security, Trust and Accountability* (2006) (discussing use of immutable audit logs to ensure accountability).
http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf

J. Dempsey and P. Rosenzweig, *Technologies That Can Protect Privacy as Information Is Shared to Combat Terrorism* (May 26, 2004).
http://www.heritage.org/research/homelandsecurity/upload/63976_1.pdf

American Statistical Association, *Frequently Asked Questions Regarding the Privacy Implications of Data Mining* (includes discussion of permissioning systems).
http://www.amstat.org/profession/index.cfm?fuseaction=dataminingfaq#4

RESOURCES AND TOOLS

In developing a program review framework, agencies may find it expedient to add oversight of ISE-specific processes involving protected information (PI) in the ISE to the portfolios of agency offices/officials already responsible for maintaining and handling personally identifiable information (PII). ISE-specific processes that may be merged into existing PII handling functions include:

1. Access, use, and disclosure of PI.
2. Training regarding the access, use, and disclosure of PI.
3. Maintenance of records/logs regarding access to/disclosure of/receipt of PI.
4. Review of compliance with PI handling policies and practices.
5. Investigation of reported/identified violations of PI handling practices.
6. Procurement/development of information technology for administering PI.
7. Audit, inspection, and investigation of agency programs.

The Office of the Director of National Intelligence has undertaken studies of existing and emerging privacy-enhancing technologies and will make the results available to agencies when completed.