TREASURY DIRECTIVE PUBLICATION

TD P 25-10

Information Sharing Environment (ISE) and Civil Liberties Policy: Implementation Plan

May 2013

1. Authority

The issuance of this Treasury Directive Publication has been authorized by Treasury Directive (TD) 25-10, "Information Sharing Environment Privacy and Civil Liberties Policy," dated 6/21/2013.

2. Policy

The Information Sharing Environment (ISE) provides a framework to facilitate the maximum sharing of terrorism information. It is the policy of the Department of the Treasury to share terrorism information with other agencies in the ISE to the maximum extent allowed under applicable law. The Department of the Treasury maintains high standards for the protection of protected information shared through the ISE. All covered Treasury entities and covered Treasury personnel shall comply with the Constitution, applicable laws, regulations, Executive Orders, Office of Management and Budget (OMB) requirements and guidance, and other relevant policies and guidelines relating to protected information, including the *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (the ISE Privacy Guidelines) and the *Key Issues Guidance* supporting the implementation of the ISE Privacy Guidelines. Compliance with such requirements is the responsibility of the component sharing information in the ISE.

3. Definitions

Collection, for Covered Treasury Entities outside the Intelligence Community, refers to the acquisition of or access to protected information by a Covered Treasury Entity or Covered Treasury Personnel in the course of their duties. For the Intelligence Community, collection is defined according to the authorities of the element involved.

Covered Treasury Entities are bureaus, offices, and other components in the Department of the Treasury, including the Offices of the Inspectors General, whose mission (e.g., law enforcement, intelligence, or foreign affairs) regularly requires them to maintain or have access to information (internally or externally) that meets the definition of protected information and shares that information in the ISE.

Covered Treasury Personnel are Treasury employees, detailees, interns, assignees, and contractors whose job functions (e.g., law enforcement, intelligence, or foreign affairs) authorize or regularly require them to have access to Treasury information (or external information) that meets the definition of protected information and share that information in the ISE.

An **Individual** is defined in the Privacy Act of 1974, 5 USC 552a (a) (2), as a citizen of the United States or an alien lawfully admitted for permanent residence. For members of the IC, "individual" means "United States Persons" as that term is defined in Executive Order 12333, entitled *United States Intelligence Activities*, as amended.

The **Information Sharing Environment (ISE)** is an approach to the sharing of information related to terrorism that is being implemented through a combination of policies, procedures, and technologies designed to facilitate the sharing of critical information by all relevant entities. The ISE serves the dual imperatives of enhanced information sharing to combat terrorism and protecting the information privacy and other legal rights of individuals in the course of increased information access and collaboration. The ISE is being developed by bringing together, aligning, and building upon existing information sharing policies and business processes and technologies (systems), and by promoting a culture of information sharing through greater collaboration. It is being developed pursuant to Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 ("the 9/11 Commission Act") and Executive Order 12333, as amended.

Information Sharing Environment Privacy Official is the Department of the Treasury's Assistant Secretary for Management.

Protected Information is certain information about U.S. citizens and lawful permanent residents that constitutes terrorism information, homeland security information, law enforcement information, or weapons of mass destruction information (all as defined below), which is subject to information privacy or other legal protections under the U.S. Constitution and federal laws of the United States, and is shared in the ISE. 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.

For elements of the intelligence community, "information about U.S. citizens and lawful permanent residents" means information about United States persons as defined in Executive Order 12333, as amended, and its implementing guidance, which provides that a U.S. person is "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments."

Information about U.S. citizens and lawful permanent residents (and U.S. persons as defined for elements of the intelligence community) is "protected information" as used in these Guidelines only if it is made available within the ISE and is homeland security information, law enforcement information, or terrorism information, including weapons of mass destruction information, which are defined by the ISE Privacy Guidelines as follows:

- ***Homeland Security Information***, for purposes of the ISE, as derived from the Homeland Security Act of 2002, Public Law 107-296, Section 892(f)(1) (codified at 6 USC 482(f)(1)), is defined as any information possessed by a state, local, tribal, or federal agency that:
    - Relates to a threat of terrorist activity;
    - Relates to the ability to prevent, interdict, or disrupt terrorist activity;
    - Relates to the identification or investigation of a suspected terrorist or terrorist organization; or
    - Relates to the response to a terrorist act.
- ***Law Enforcement Information***, for purposes of the ISE, is defined as any information obtained by or of interest to a law enforcement agency or official that is :
    - Related to terrorism or the security of our homeland, and
    - Relevant to a law enforcement mission, including but not limited to:
        - Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation;
        - Assessment of or response to criminal threats and vulnerabilities;
        - The existence, organization, capabilities, plans, intention, vulnerabilities, means, method, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct;
        - The existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law;
        - Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.
- ***Terrorism Information***, for purposes of the ISE, is defined in IRTPA Section 1016 (codified at 6 USC 485) as all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to:
    - The existence, organization, capabilities, plans, intentions, vulnerabilities, means of financial or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

- Threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
- Communications of or by such groups or individuals; or
- Groups of individuals reasonably believed to be assisting or associated with such groups or individuals.

The definition of terrorism information includes weapons of mass destruction information.

- ***Weapons of Mass Destruction Information***, for purposes of the ISE, is defined in IRTPA Section 1016 (codified at 6 USC 485) as information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or terrorist organization against the United States, including information about the location of a stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or terrorist organization against the United States.

A **Record** is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

A **Routine Use** means, with respect to the disclosure of a Record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

A **System of Records** means 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.

System Owner is an official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

4. Responsibilities.

a. Collection (Acquisition and Access)

All protected information shall be collected lawfully and shall be limited to that information related to Treasury's missions, or otherwise in accordance with law. All protected information collected will only be used and shared for purposes authorized by law. Prior to beginning a new or modified information collection effort, all covered Treasury entities (unless otherwise exempted by law from one or more of these activities) shall assess their information collection practices to verify that:

1) Data collection is limited to that which is related to the Department's mission or otherwise authorized by law.
2) The Department has received approval from OMB for the collection, in compliance with the Paperwork Reduction Act (PRA), if applicable.
3) A copy of OMB's approval for a new collection that is subject to the PRA is sent to the Office of Privacy, Transparency, and Records for the purpose of determining whether the collection may be subject to the Department's ISE Policy and this Implementation Plan.
4) To the greatest extent practicable, information is collected directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs.
5) A privacy impact assessment (PIA) (as defined in OMB M-03-22) has been conducted if it is required for the information collection pursuant to Treasury Directive 25-07.
6) A system of records notice (SORN) has been published in the Federal Register if required by the Privacy Act of 1974.
7) Information about an individual is not collected based solely on his/her race, ethnicity, national origin, religion, or other classifications protected from discrimination by federal law.
8) No record is maintained describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained, unless pertinent to and within the scope of an authorized law enforcement or intelligence activity.

b. Use

The Privacy Act restricts use of protected information maintained in systems of records. Prior to using a record subject to the SORN requirement, system owners, with the assistance of their bureau or office's Privacy Point of Contact, shall verify that one of the following is true:

1) The intended activity is a routine use listed in the applicable SORN published in the Federal Register at least 30 days prior to the use;

2) The individual who is the subject of the records has provided consent to the use;

3) The use is subject to a Privacy Act general or specific exemption; or

4) The Privacy Act otherwise specifically allows the intended use.

Use as part of a non-exempt computer matching program must meet all requirements listed in the Computer Matching and Privacy Protection Act.

c. Notice

Covered Treasury entities will establish notice mechanisms (e.g., metadata, coversheets) for communicating the nature of the information to be made available in the ISE. These notice mechanisms will ensure that covered Treasury entities that receive protected information handle it in accordance with applicable legal and Departmental policy requirements. Notice mechanisms will, to the extent reasonably feasible, permit ISE participants to determine whether the information pertains to a U.S. citizen or lawful permanent resident, is subject to specific disclosure or information privacy or civil rights or civil liberties requirements or limitations (including restrictions on further dissemination), and whether there are known limitations on the reliability or accuracy of the information.

d. Data Quality and Integrity

Treasury has procedures in place, as appropriate, to facilitate the prevention, identification, and correction of inaccuracies in protected information. For these purposes, "accurate" means that the protected information is accurate for the purposes for which it is retained and has not mistakenly been shared through the ISE. In addition to other data quality and integrity efforts outlined in this implementation plan, the Department will take the following steps to ensure data quality and integrity, except that elements of the intelligence community (as defined in Executive Order 12333, as amended) will follow intelligence community requirements to identify, report, notify, or correct intelligence information:

1) The Department's ISE Privacy Official or the appropriate bureau, office, or other component will investigate in a timely manner alleged inaccuracies in the bureau, office, or component's information and correct, delete, or refrain from using protected information found to be inaccurate.
2) Upon receiving information from an ISE participant that the Department determines may be inaccurate, the Department's ISE Privacy Official or the appropriate bureau, office, or other component (with notice to the ISE Privacy Official) will, consistent with applicable legal authorities and mission requirements, ensure that the contributing agency's ISE Privacy Official is notified in writing.
3) If the Department determines that its protected information, which has been disseminated in the ISE, is inaccurate, the Department's ISE Privacy Official or the appropriate component (with notice to the ISE Privacy Official) will provide written notice to ISE participants who received the information and request corrective measures with respect to the inaccurate data.
4) The Department will have mechanisms in place whereby, subject to applicable and appropriate exemptions claimed for Departmental systems of records under the Privacy Act, individuals may request correction of their data that is contained in a system of records. For more information, please refer to Section 8 on Administrative Redress, Access and Correction.
5) When merging protected information (including partial matches) from two or more sources, the Department will take steps reasonably designed to ensure that the information is about the same individual.

6) The Department will retain protected information only so long as appropriate.
7) The Department will take necessary remedial action when it is determined that protected information is outdated, not related to Treasury's mission, or as otherwise authorized by law.

e. Sharing and Dissemination

Lawfully obtained information may be shared and disseminated through the ISE. All covered Treasury entities must:

1) Share protected information in the ISE provided it is terrorism-related information (homeland security, law enforcement information, terrorism, and weapons of mass destruction information as defined in section 15 of this Publication).
2) Ensure that protected information is shared in the ISE in compliance with TD 25-10 and this implementation plan.
3) Put in place a mechanism to enable Treasury employees and other ISE participants to determine the nature of the protected information, so it can be handled in accordance with applicable legal requirements.

f. Administrative Redress, Access, and Correction

Treasury has multiple mechanisms in place that provide individuals (as defined in section 15 of this Publication) with opportunities to request access to their record(s), request correction of their record(s), and file a privacy or civil rights/civil liberties complaint (subject to applicable and appropriate exemptions claimed for certain systems of records under the Privacy Act). These mechanisms are:

- The Department's procedures by which certain individuals may obtain correction of records under the Privacy Act of 1974 are published at 31 CFR 1.27 and the Appendices to Part 1. These procedures allow for the amendment of records pertaining to individuals, including agency review and appeal from initial adverse agency determinations.
- Treasury Directive (TD) 25-09 is Treasury's policy addressing the activities of Chief Privacy and Civil Liberties Officer (CPCLO) as directed by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53. This directive requires that the CPCLO receive, investigate, and respond to complaints from individuals who allege violation of their privacy or civil liberties, and develop a process to protect employees who make a complaint from reprisal or threats of reprisal.

g. Security

The Department shall provide adequate and effective security protection for all protected information, including protected information shared through the ISE, in records stored and accessed in Departmental systems to ensure their protection from unauthorized access, use, modification, or destruction. Covered Treasury entities

shall develop policies and procedures that seek to ensure the following with respect to protected information maintained by Treasury and shared in the ISE:

1) Administrative, technical, and physical safeguards are in place to protect the security, integrity, confidentiality and availability of protected information and all protected information.
2) All safeguards for protected information and other sensitive information comply, where required, with the Federal Information Security Management Act of 2002 (FISMA), OMB Circular A-130, Appendix III, applicable National Institute of Standards and Technology (NIST) security guidance, and Treasury security policies and procedures.
3) Records are securely maintained and destroyed in accordance with applicable records retention schedules.
4) Security protection shall be commensurate with the risk level and magnitude of harm Treasury and/or the record subject would face in the event of a data security breach.
5) ISE recipients of Treasury's protected information are required to indicate that they are in compliance with FISMA or other comparable, applicable security requirements that govern the information shared.
6) Where appropriate and feasible, available privacy enhancing technologies are considered.
7) Additional information security requirements are included in the information sharing access agreement.

h. Accountability, Enforcement, and Audit

To ensure the accountability and protection of protected information shared in the ISE, Treasury employs the following enforcement and audit procedures:

1) All personnel must report violations of Departmental policies relating to protected information, as required in relevant Departmental directives, policies, and guidelines.
2) All covered Treasury personnel must cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE.
3) The Department has designated its Assistant Secretary for Management (ASM) to receive reports (or copies, as appropriate) regarding alleged errors that may exist in protected information originating from or received or used by Treasury.
4) The Department has established mechanisms to enable Departmental officials to verify that covered Treasury entities and covered Treasury personnel are complying with the ISE Privacy Guidelines as required by TD 25-10 and this implementation plan.

i. Training

Treasury's ISE Privacy Official (the ASM) shall ensure that training is provided to covered Treasury personnel regarding Departmental requirements and policies for the collection, use, and disclosure of protected information and, as appropriate, for reporting violations of TD 25-10 and related Departmental policies. All Departmental employees are provided annual privacy awareness training. In addition to this annual privacy awareness training, covered Treasury personnel will receive additional, annual training covering the requirements of the Department's ISE Policy, this Implementation Plan, and any additional guidance provided to ensure its proper implementation.

j. Awareness

The Department of the Treasury will take steps to facilitate appropriate public awareness of its policies and procedures for implementing TD 25-10 and this implementation plan and by making both publicly available on its web site.

k. Required Procedures

Covered Treasury entities may customize the Departmental procedures or develop their own, as needed, to meet their specific mission needs, provided they are consistent with TD 25-10, this implementation plan, and all applicable legal requirements and developed in consultation with the Deputy Assistant Secretary for Privacy, Transparency & Records (DASPTR). Covered Treasury entities may only develop procedures that deviate from TD 25-10 and this implementation plan if approved in advance by the DASPTR. Covered Treasury entities that choose to customize the Departmental procedures must also develop or modify Departmental training developed in coordination with the DASPTR in a manner that is approved by the DASPTR.

l. Assessment of Policies and Update of TD 25-10 and Implementation Plan

The Department of the Treasury will continue to identify and assess evolving laws, Executive Orders, policies, and procedures applicable to protected information that it will make available or accessible through the ISE and will comply with any legal restrictions applicable to such information. This may require updating the ISE Policy and the implementation plan as necessary.