APPENDIX C

TYPE OF INFORMATION SENSITIVITY AND HOW ISSUES MAY ARISE IN THE ISE RESULTING FROM THE SHARING OF SUCH INFORMATION[3]

Type of Information Sensitivity	Nature of Protection	Examples	Stakeholder Considerations
Personally Identifiable Information (PII)	The term *PII* refers to "information that can be used to distinguish or trace an individual's identity, . . . alone, or when combined with other personal or identifying information is linked or linkable to a specific individual."[4]	Types of PII • Name • Social security number • Biometric records • Date of birth • Place of birth • Mother's maiden name, etc. Example • An individual's fingerprints are shared by the providing agency with an employee of another agency who does not have a need to know the information.	• Stakeholders should consult with P/CL officials to determine whether the information containing PII may be subject to statutory and regulatory restrictions on dissemination or disclosure of the information or subject to data quality restrictions/protections.[5] • Sensitivity of PII may vary depending upon the nature of the data element involved.[6] • PII requires safeguarding regardless of whether the individual is a U.S. citizen or a lawful permanent resident.

[3] The examples of rights and liberties listed below are not absolute and must be interpreted in conjunction with federal case law and any applicable statutes. These concepts are not explicitly or implicitly granting any cognizable legal remedies but are merely referenced when considering potential unintended consequences when developing ISAAs.

[4] See OMB M-07-16.

[5] See e.g., EO 12333; United States Intelligence Activities, December 4, 1981, *as amended*; the Privacy Act of 1974 (5 U.S.C. § 552a) (establishing a code of fair information practices that places restrictions on the federal government's collection, maintenance, use, and dissemination of information about individuals [i.e., PII] that is maintained).

[6] Some departments and agencies have issued departmental guidance that distinguishes between sensitive and non-sensitive PII. Stakeholders should inquire about the existence of such a policy and be familiar with it if one exists.

Type of Information Sensitivity	Nature of Protection	Examples	Stakeholder Considerations
The First Amendment to the U.S. Constitution	Information describing how an individual exercises rights guaranteed by the First Amendment is sensitive. The First Amendment prohibits Congress from passing any law that prohibits the free exercise of religion or abridges freedom of speech, freedom of the press, the right of the people to assemble peaceably, or the right to petition the government for redress of grievances.	Common First Amendment Activities • Possession of reading materials • Communication with lawmakers, the courts, or the press • Social media postings • Library activities • Protests • Association with political, religious, and other civil society organizations How the issue may arise in the ISE • An agency collects a membership list of a religious or political organization that poses no national security or criminal threat. If the agency shares that information, the affected organization could reasonably claim that its First Amendment rights had been violated when the public disclosure of the information results in public derision or leads to regulatory restrictions that result in a significant drop in membership.	The parties to the initiative: • Are required to have policies that prohibit the collection or sharing of information in the ISE based solely on the exercise of rights guaranteed by the First Amendment; and • Should have clear documentation of a valid mission purpose (for the sharer and receiver) whenever information pertaining to First Amendment activity is shared in the ISE (to comply with both ISE policy and, when applicable, Privacy Act 5 U.S.C. § 552a(e)(7)). Remember: some information may be valid for an agency with public safety mission to collect that may not be distributable through the wider ISE because it was not collected based on a law enforcement or national security predicate.
The Fourth Amendment to the U.S. Constitution	The Fourth Amendment protects against unreasonable searches and seizures and requires that warrants be judicially sanctioned and based on probable cause. The courts have generally held that dissemination of information from one federal agency to another does not implicate rights under the Fourth Amendment;[7]	How the issue may arise in the ISE • An agency inadvertently merges the information of two similarly named people and then shares the merged record. One of the individuals is detained in a traffic stop based on the derogatory information of the other individual, and the incident is not resolved until after the innocent individual is taken into custody and his car	• Agencies that share information should make reasonable efforts to ensure that the information is accurate, complete, timely, and relevant prior to dissemination. • Providing agencies should take care to fully inform receiving agencies of their assessment of the probable accuracy of the information before initiating an

[7] The rationale underlying this conclusion is that the dissemination itself is neither a "search" nor a "seizure." See e.g., *Jabara v. Webster*, 691 F.2d 272 (6th Cir. 1982), *cert. denied*, 464 U.S. 863 (1983).

Type of Information Sensitivity	Nature of Protection	Examples	Stakeholder Considerations
	however, sharing information about an individual that is subsequently determined to be materially inaccurate or misleading may indirectly implicate that individual's Fourth Amendment rights if he or she is seized or his or her property is searched as a consequence of the erroneous information.[8]	impounded. • Note: Information may be determined to be erroneous or deficient, either from the time collected or due to changing factual circumstances. If it is determined that information that has been shared was acquired in violation of an individual's rights under the Fourth Amendment, the information may become the subject of an expungement order.[9]	agreement; safeguards in the ISAA should reflect the accuracy of the information. • In those instances when it is later determined that the information is erroneous, agencies that share information should employ timely notice and corrective procedures. • ISAAs should contain provisions regarding how the parties will notify each other of corrected or updated information, and require that the parties adequately mark and track information so those corrections can be applied. They should also spell out which agency's individual redress procedures will be used.
The Fifth and Fourteenth Amendments to the U.S. Constitution – Due Process	The Fifth Amendment provides that no individual should "be deprived of life, liberty, or property, without due process of law" by the federal government. Similarly, the Fourteenth Amendment prohibits the states from making such a deprivation without due process. If erroneous information shared in the ISE leads to the denial of an individual's entitlements, benefits, status, privileges, or rights granted by statute, Fifth or Fourteenth Amendment rights may be infringed.	How the issue may arise in the ISE • A background check or other investigation is conducted prior to granting some benefit to the individual. Due process concerns may arise when the individual is not allowed to challenge the facts underlying the adverse action. The process that is due such an individual may include the right to access information that may be used to his or her detriment and the right to request correction of that information if the individual believes the information is not accurate, relevant, timely, or complete.	• Agencies that share information should make reasonable efforts to ensure that the information is accurate, complete, timely, and relevant prior to dissemination. • Federal agencies sharing information that could be used to deny constitutional rights should not rely on access and correction procedures as the only protective mechanism for minimizing the risk that action may be taken against persons based on inaccurate information. Redress should be part of the solution as a matter of policy—this is consistent with other rights, protections,

[8] This could occur, for example, when an individual is detained based on erroneous information or misidentification (e.g., at an airport or pulled over by a police officer on the public highways).

[9] Depending on the jurisdiction of the court issuing the order and the contents of the order, the expungement order could apply broadly throughout the ISE. Such a determination could result from a suppression hearing in a criminal trial or an agency's internal response to a complaint from the affected party.

Type of Information Sensitivity	Nature of Protection	Examples	Stakeholder Considerations
			and strategies that reduce agency liability. • ISAAs should contain provisions regarding how the parties will notify each other of corrected or updated information and require that the parties adequately mark and track information so those corrections can be applied. They should also spell out which agency's individual redress procedures will be used. • The aggrieved party may obtain an order to have the information expunged from agency records; agencies may be under a legal or policy-driven obligation to provide notice of this consequence to other agencies with which the information has been shared. Agencies are encouraged to have in place robust data quality measures to facilitate compliance with court orders and to correct data errors when detected.
The Fourteenth Amendment to the U.S. Constitution – Equal Protection	The Fourteenth Amendment provides that no state shall "deny to any person within its jurisdiction the equal protection of the laws." While the Fourteenth Amendment's equal protection clause applies only to the states, the concepts and rights embodied in it align to great extent with the Fifth Amendment's due process clause, which applies to the U.S. government.	How the issue may arise in the ISE • An agency receives a suspicious activity report from an officer who, during the course of a traffic stop, noticed the driver had what appeared to be Arabic language books and CDs on the passenger seat. The officer reports the stop, including a description of the driver as "Muslim-appearing." The agency adds information from its records indicating the individual is a naturalized U.S. citizen born in Pakistan, and enters the report into the Shared Data Repository. In the ISE context, sharing information about	• Agencies should have robust training initiatives to ensure that information is collected and shared appropriately within the ISE, including specific guidance regarding use of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in investigative or intelligence contexts. • If an agency discovers that information it has shared was collected and retained solely on a prohibited basis, it should make reasonable efforts to ensure that recipients of the information are notified of the improper collection and delete or refrain from using the information. • Given the complexity of equal protection

Type of Information Sensitivity	Nature of Protection	Examples	Stakeholder Considerations
		an individual solely because he or she is of a certain race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity would violate that individual's constitutional right to equal protection. The equal protection standard is further reflected and implemented for federal law enforcement in the U.S. DOJ's *Guidance Regarding Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (December 2014).	law, agency personnel should seek legal guidance when questions relating to race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, or related practices arise, especially when a sharing initiative seeks to aggregate or display information based on these categories. Even where the information is lawfully collected, organizing and displaying information on this basis can have equal protection implications.
Unenumerated Rights, Federal Statutory Rights, Common Law, and State Law	The concept of civil liberties is much broader than those freedoms specifically enumerated in the Constitution. It includes the general presumption of freedom of action and the commonly recognized rights protected by federal statutory law, common law, and state law. In addition, the Ninth Amendment specifically notes that individual rights and liberties are not limited to those enunciated by the preceding amendments.	Examples • Right to travel • Right to privacy • Commonly recognized rights protected by federal statutory law, common law, and state law, such as the right to seek and retain employment How the issue may arise in the ISE • Even when the inconvenience or constraint imposed on a person's activities does not amount to an infringement of constitutional rights, the sharing of inappropriate or inaccurate information in the ISE can have a consequential effect on an individual's unenumerated rights. For instance, when erroneous information is shared and subsequently relied on by end users, an individual's ability to travel or conduct lawful business may be impaired.	• Agencies participating in the ISE are urged to consider the potential unintended consequences to innocent individuals and to develop and implement ISAAs that minimize those consequences (e.g., redress procedures documented in the ISAA should be commensurate with the potential impact to an individual from use of incorrect or out-of-date information).

Type of Information Sensitivity	Nature of Protection	Examples	Stakeholder Considerations
Statutory Rights – PII Held by Third Parties	Stakeholders should be aware that certain types of information are lawfully retained by third parties and are regulated by statutory schemes that prohibit unauthorized disclosure. Federal law restricts the U.S. government's and some other governmental and private entities' access to and use and disclosure of such information.	Examples • Financial records subject to the Right to Financial Privacy Act[10] • Credit information subject to the Fair Credit Reporting Act[11] • Tax information subject to the Internal Revenue Code [12] • Telephone and Internet service records subject to the Electronic Communications Privacy Act[13] • School records subject to the Family Educational Rights and Privacy Act[14] • Medical records subject to federal regulations issued pursuant to the Health Insurance Portability and Accountability Act[15]	• ISE participating agencies are encouraged to develop policies that treat this information as sensitive and to protect it from unlawful disclosure. Practices commonly used to safeguard sensitive information include physically or electronically securing sensitive information, limiting physical access to such information to those with a need to know the information, sound personnel security practices, and audit capability and implementation.

[10] 12 U.S.C. § 3401.
[11] 15 U.S.C. § 1681.
[12] 26 U.S.C. § 6100.
[13] 18 U.S.C. § 2701.
[14] 20 U.S.C. § 1232g.
[15] 45 CFR Parts 160, 164.