

Collection Limitation/Data Minimization

Fusion centers should only collect personally identifiable information ("PII"), that is directly relevant and necessary to accomplish the specified purpose(s) for collection, and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Implementing the Collection Limitation/Data Minimization Principle in the ISE – The following bullet points represent several ways in which fusion centers can implement the Collection Limitation/Data Minimization Principle. However, these action items are simply suggestions; they do not represent the universe of possible implementation approaches, nor do they ensure compliance with the Collection Limitation/Data Minimization Principle. The only way to ensure full compliance is individualized consideration of your center's practices to align all PII collection and retention standards with this Principle.

Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion. If not, share only activity-based information without PII;

Approaches to Implementation: *For instance, where a law enforcement officer seeks PII from Intelligence & Analysis, he or she must be able to demonstrate a reasonable suspicion of criminal activity that may lead to terrorism. Where that showing cannot be made, the Intelligence & Analysis analyst will only share activity-based information, stripped of PII.* DHS Privacy Impact Assessment: State, Local, and Regional Fusion Center Initiative (42pp | 319 KB | PDF).

Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged and then deleting the data;

Approaches to Implementation: *With respect to Custom and Border Protection's TECS system's (not an acronym) use of Information Sharing Environment Suspicious Activity Reports (ISE SARs) and Suspicious Activity Reports (SARs): "The main privacy risk presented by this sharing of [Memoranda of Information Received (MOIRs)] with the ISE-SAR server is that an MOIR may be mistakenly nominated as meeting the [National SAR Initiative] criteria. This privacy risk is mitigated in two ways: first, through the specialized training provided to the SAR nominating team from [The Office of Intelligence and Investigative Liaison] that submits MOIRs to become SARs; and secondly, through supervisory review of all nominated SARs."* DHS Privacy Impact Assessment: TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative (6 pp | 157KB | PDF).

Designing a data storage system to pull data for review and then, if appropriate, automatically purge data after the specified retention period has been reached;

Approaches to Implementation: *"Once a [FALCON-Search & Analysis system] source record or item of data is deleted from the system, because the retention period has expired, that data will also be deleted from the metadata, index, and any user-created visualizations and search queries."* DHS Privacy Impact Assessment: Falcon-SA (27pp | 322KB | PDF).

Limiting a system's data field elements to only those that are relevant;

Approaches to Implementation: *"In addition, FALCON-SA's access controls are highly customizable and can be set at the record or even data field level. This ensures that users without a need to know are technically barred from accessing that information."* DHS Privacy Impact Assessment: Falcon-SA (27pp | 322KB | PDF).

Requiring that justifications be entered, and logs maintained for all queries with sensitive PII, and that an internal review process of those logs takes place at specified intervals;

Approaches to Implementation: *"User activity is audited heavily, including actions such as: uploading records or data, extracting information from the system, resolving entities, searches, and viewing records. [U.S. Immigration and Customs Enforcement] has established controls that are based in policy and where possible enforced by technology, that provides clear instruction on what the authorize uses of the system are."* DHS Privacy Impact Assessment: Falcon-SA (27pp | 322KB | PDF).

Ensuring that all distributed reports and products (1) contain only the personal information that is needed; (2) do not contain information just because it is available; and (3) exclude all extraneous information;

Approaches to Implementation: *"The information DHS shares via the [Law Enforcement Information Sharing] Service is a filtered subset of data compiled by [ICE Pattern Analysis and Information Collection (ICEPIC) system], limited to only law enforcement data. Additionally, ICE has created filters on the law enforcement data to ensure that the system controls the amount and type of information being shared. Finally, DHS has limited member agencies' uses of the data to criminal law enforcement purposes, national and homeland security purposes, and background checks on applicants seeking employment with the member agency."* DHS Privacy Impact Assessment for the ICE Pattern Analysis and Information Collection (ICEPIC) (14 pp | 240 KB | PDF).

Enforcing a retention schedule that purges PII after it is no longer needed;

Approaches to Implementation: *Although there is always risk inherent in retaining PII for any length of time, the data retention period for the [National Operations Center (NOC)] Patriot Report Database is based on case type identified in the [the National Archives and Record Administration] retention schedule of [5 years] and is consistent with the concept of retaining PII for as long as necessary to support the agency's mission.* DHS Privacy Impact Assessment: NOC Patriot Report Database PIA (12 pp | 166 KB | PDF).

Data Minimization | Data Quality and Integrity | Purpose Specification | Use Limitation | Security | Transparency | Individual Participation | Accountability and Auditing

Source: The DHS Office for Civil Rights and Civil Liberties and the DHS Privacy Office.
Last date page updated: 3/3/21 (CRCL)