

Privacy, Civil Rights, and Civil Liberties

Audit Guidance

for the State, Local, Tribal, and
Territorial Intelligence Component

September 2015

Privacy, Civil Rights, and Civil Liberties

Audit Guidance

for the State, Local, Tribal, and
Territorial Intelligence Component

September 2015

Supplemental materials and a digital copy
of this document are available at
<http://it.ojp.gov/PrivacyLiberty>
as part of the P/CRCL Officer Toolkit.

About the Global Advisory Committee

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment. GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

This project was supported by Grant No. 2014-DB-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice and the U.S. Department of Homeland Security.

Table of Contents

Overview	1
How to Use This Audit Guidance.....	4
Privacy, Civil Rights, and Civil Liberties (P/CRCL) Audit Procedure and Recommended Questions.....	6
Section 1: Sample P/CRCL Audit Questions for Review of Common Record Types.....	6
Part A—Criminal Intelligence (CI) Records and Products Containing Criminal Intelligence Information (CII)—28 CFR Part 23.....	6
Part B—Products (Situational Awareness, Analytic)*	8
Part C—Information Sharing Environment-Suspicious Activity Reports (ISE-SARs)	13
Part D—Other Records Subject to the Agency’s P/CRCL Audit	15
Section 2: Assessing Implementation of the P/CRCL Policy.....	16
Endnotes	19
Appendices **	
Appendix A: Pre-Audit Planning Checklist	22
Appendix B: Potentially Applicable Federal Statutes and Types of State Laws	27
Appendix C: General Principles for Developing Audit-Recommended Actions	29
Appendix D: Template for Internal Memorandum From the Audit Team	31

*Note: Products containing CII should be reviewed first using the questions under Part A and then using the relevant questions under Part B.

**Note: See <http://it.ojp.gov/PrivacyLiberty> for updates and additional Appendices developed for this document.

Document Source and Attribution

In order to safeguard the nation while respecting individuals' privacy, civil rights, and civil liberties (P/CRCL), the U.S. Department of Justice's Bureau of Justice Assistance—with support from the Global Justice Information Sharing Initiative's Criminal Intelligence Coordinating Council (CICC) and in partnership with the U.S. Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A), the DHS Office for Civil Rights and Civil Liberties (CRCL), the DHS Privacy Office (PRIV), and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—developed this *Privacy, Civil Rights, and Civil Liberties Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component*.

Overview

The *Privacy, Civil Rights, and Civil Liberties (P/CRCL) Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Component* (Audit Guidance) is designed to help state, local, tribal, and territorial (SLTT) agencies, including state and major urban area fusion centers, conduct a privacy, civil rights, and civil liberties (P/CRCL) audit of records within the agency's intelligence component. A P/CRCL audit will support agency leadership in ensuring the protection of community members' privacy, civil rights, and civil liberties in the agency's intelligence-related activities, including intelligence collection, analysis, and dissemination.

A P/CRCL audit is an essential component of effective intelligence function management:

- ◀ Through the audit process, personnel overseeing the agency's intelligence function will be able to identify compliant and noncompliant records and products and recommend appropriate next steps for remediation.
- ◀ The audit process also helps agency leadership assess the operational implementation of the agency's P/CRCL policy and implementing procedures.
- ◀ A P/CRCL audit reinforces mission effectiveness and may provide a measure of accountability to oversight bodies and the public.

The *National Criminal Intelligence Sharing Plan* (Global Justice Information Sharing Initiative [Global], October 2003) recommended that all law enforcement agencies develop an intelligence function to implement the intelligence process within their respective agencies. For purposes of this resource, an "intelligence function" or "law enforcement intelligence function" is an element within an agency charged with the collection, analysis, and dissemination of analyzed information that is tailored to the needs of law enforcement or homeland security decision makers or operators.

For this document, the use of "audit" refers to a process to determine whether an intelligence component is compliant with required policies and/or nationally recognized guidelines and to identify the causes of noncompliance and possible corrective actions. It does not mean a technical or financial audit using the standards identified in the Generally Accepted Government Auditing Standards or other professional standards.

The Bureau of Justice Assistance (BJA), in close collaboration with and leveraging the expertise of the U.S. Department of Homeland Security (DHS) Office for Civil Rights and Civil Liberties (CRCL) and the Privacy Office (PRIV), developed this resource through the support of the Criminal Intelligence Coordinating Council (CICC)—a group under the Global Initiative.

Document Format

This resource is separated into two sections:

- ◀ **Section 1** provides a series of questions to facilitate agency review of a sample of records and products for compliance with the agency's P/CRCL policy and applicable laws, regulations, guidance, and standards (see Appendix B for a list of *potentially* applicable federal and state laws).

Section 1 is subdivided by record type. These subsections include Criminal Intelligence (CI) Records and Products Containing Criminal Intelligence Information (CII) (i.e., 28 CFR Part 23); Products (Situational Awareness, Analytic); Information Sharing Environment (ISE)-Suspicious Activity Reports (SARs); and other records (such as responses to Requests for Information). ***It is important to note that not all questions will be relevant for a particular audit or a particular agency (see "Customizing a P/CRCL Audit" below).***

- ◀ **Section 2** includes questions to assess the extent to which the agency's daily operations align with its P/CRCL policy and implementing procedures.

This resource also includes various Appendices that may be helpful in facilitating a P/CRCL audit. Appendices include:

- a) Pre-Audit Planning Checklist
- b) Potentially Applicable Federal Statutes and Types of State Laws
- c) General Principles for Developing Audit-Recommended Actions
- d) Template for Internal Memorandum From the Audit Team

Customizing a P/CRCL Audit

Depending on an agency's intelligence-related activities and jurisdiction, the agency should customize its P/CRCL audit to address jurisdictional legal requirements and conform to the agency mission. An agency may also determine that some questions are not pertinent to the desired scope of its audit or relevant to its particular situation and therefore elect not to include those questions in the audit.

To help agencies customize their P/CRCL audit, this resource identifies potential sources of other legal requirements for the intelligence function (see Appendix B), as well as additional categories of records—beyond those addressed by name in Section 1 of this Audit Guidance—that agencies may wish to review.¹

P/CRCL Audit Period and Frequency Recommendations

Generally, an audit period covers the 12 months immediately prior to the actual audit. If agency personnel are not conducting audits on an annual basis or if this is the first audit, a longer audit period may be appropriate, especially if there are relatively few records. While an internal audit is appropriate for the initial cycle, agencies are encouraged to involve external participants in the audit process at least once every three or four years.

Anticipated P/CRCL Audit Outcomes and Recommendations

A P/CRCL audit is an opportunity to:

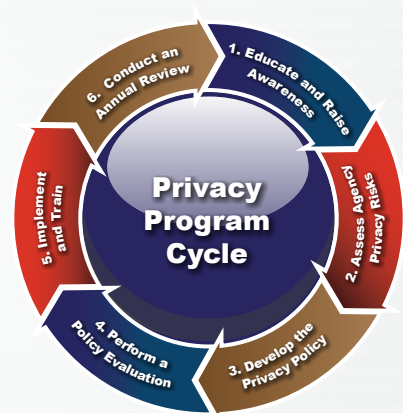
- ◀ Review activities of an intelligence function.
- ◀ Identify and discuss observed noncompliance issues.
- ◀ Incorporate findings and dispositions into a written plan, including any additional actions that need to be taken.
- ◀ Provide a measure of public accountability that will enhance confidence among policymakers and the citizenry that the intelligence component is complying with all legal requirements and operating in a professional manner.

The first audit cycle should be conducted as an informational exercise to identify initial findings and recommended actions. Subsequent annual audit findings, however, should be noted and reported.

It is recommended that appropriate elements of this audit process and key audit outcomes be compiled into a report and be provided to command staff and oversight entities or governance boards. The agency should also provide, at minimum, an overview to the public to enhance transparency with respect to P/CRCL protections built into agency intelligence operations.²

Privacy Program Cycle

This guidance document is part of a continual process designed to ensure that agencies incorporate comprehensive and effective P/CRCL protections into daily operations. Just as this guidance is designed to help agencies conduct a P/CRCL audit, each of the other steps in the process has guidance tools to help agencies meet their obligations.³



How to Use This Audit Guidance

This resource is designed to be scalable for different-sized agencies; agency personnel should use the sections best suited to their agency's intelligence function.

- ◀ For instance, a small law enforcement agency that does not participate in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) may decide to limit its audit to its P/CRCL implementation efforts and criminal intelligence records.
- ◀ A fusion center performing each of these intelligence functions, including the collection of ISE-SARs, might incorporate all sections of the document into its P/CRCL audit process.

The resource will be periodically updated and enhanced, as needed, to reflect the current operating environment.

Prior to the Audit

Prior to a P/CRCL audit, the audit team should review the entire Audit Guidance document, including appendices, to determine which records should be audited. In addition, the team should complete the Pre-Audit Planning Checklist (Appendix A). The checklist identifies suggested tasks that should be performed in advance of a P/CRCL audit, including a review of the guidance document, a review of legal requirements applicable to the intelligence function, identification of audit team members, and a review of other relevant documents. Completion of the checklist will significantly reduce the time required to complete the audit. Prior to the first audit, the team should identify and evaluate current processes, procedures, and use of data within the intelligence function. This may include a review of how personally identifiable information (PII) is collected, used, accessed, and disclosed; current P/CRCL standards, policies, and practices; and data retention policies and practices.

Conducting the Audit

This resource is designed to assist agencies in conducting a P/CRCL audit. For the purposes of the P/CRCL audit, the term "compliance" means that the intelligence function reviewed applicable records and determined that the records are maintained in accordance with the agency's P/CRCL policies and implementing procedures.

If a record or a practice is not in compliance with the agency's P/CRCL policy or requires further information or policy clarification, the audit team should consult with appropriate personnel to discuss preliminary findings. Such consultation would allow involved parties to respond to audit findings and to discuss possible corrective actions.

After the Audit

At the conclusion of the audit, a list of recommended actions should be developed, based on the audit findings. Agency leadership should work with appropriate personnel to identify time frames for implementing recommended actions.

In addition, the audit team should summarize and disseminate key audit outcomes through a memo to the commander or director of the intelligence component and/or oversight/governance board and the public, as appropriate (see Appendix D).



State and Major Urban Area Fusion Centers

The Audit Guidance supports the DHS Civil Rights and Civil Liberties Impact Assessment recommendation to develop P/CRCL audits “to fully implement the fusion center’s [Privacy] P/CRCL policy.” This resource also supports the Fusion Center Performance Program (FCPP), which includes an annual assessment process facilitated by the DHS Office of Intelligence and Analysis and is designed to capture objective, standardized data for the purpose of evaluating the value and impact of the National Network of Fusion Centers.

Specifically, the results of an agency’s audit can be used to inform two FCPP metrics, which are part of the federal interagency annual report to Congress:

- ◀ Percentage of fusion centers that conduct P/CRCL audits according to Global/DHS/U.S. Department of Justice (DOJ) guidance
- ◀ Percentage of P/CRCL audit findings for which fusion centers took remedial (corrective) actions

Fusion centers are encouraged to share this Audit Guidance with agency auditors, such as auditors in the agency’s Inspector General’s Office, and encourage them to use it when reviewing the centers’ records and products for compliance with applicable laws, policies, and sound practices. In addition, in the interests of public transparency and in order to demonstrate the commitment to comply with all relevant privacy, civil rights, and civil liberties laws, regulations, and policies in the conduct of the intelligence function, fusion centers are encouraged, at a minimum, to publicly share a summary of the audit methodology and key audit outcomes.⁴

The DHS/DOJ Fusion Process Technical Assistance Program also has technical assistance available to state and major urban area fusion centers, including peer-to-peer exchanges, to support the completion of the P/CRCL audit.

The National P/CRCL Fusion Center Training Program, supported by DOJ and DHS, offers materials, training, and technical assistance support for fusion center personnel and others with an intelligence function. For updated information and resource materials, visit <http://it.ojp.gov/PrivacyLiberty>.

P/CRCL Audit Procedure and Recommended Questions

Section 1: Sample P/CRCL Audit Questions for Review of Common Record Types

Part A—Criminal Intelligence (CI) Records and Products Containing Criminal Intelligence Information (CII)—28 CFR Part 23

Part A focuses on a review of criminal intelligence information (CII).⁵ The recommended audit questions are based on the requirements of 28 CFR Part 23, the de facto national standard for agencies that collect, process, and share CII, as recommended in the *National Criminal Intelligence Sharing Plan*.⁶

Directions: Review a random selection of CII records in the criminal intelligence system, and for each record, answer the following questions.⁷

Reasonable suspicion is established when information exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

1. Information Collection

- a) Was the information in the record legally obtained?⁸
- b) Does the record include sufficient supporting information to determine that the individual or organization is reasonably suspected of involvement in an identifiable criminal activity or enterprise? If not, was the responsibility to determine reasonable suspicion delegated to the submitting agency?⁹
- c) Is the information in the record relevant to the identification of the criminal subject or the identified criminal conduct or activity?
- d) Does the record include information on political, religious, or social views, associations, or activities of individuals, businesses, or groups?¹⁰
If so:
 - i. Does the information directly relate to the criminal conduct or activity?
 - ii. Is there reasonable suspicion that the subject of the information is or may be involved in that criminal conduct or activity?
- e) Does the record contain any indication that the CII was entered in violation of any applicable local, state, or federal law or ordinance?¹¹
- f) Does the record include noncriminal identifying information?

If so:

- i. Is the noncriminal identifying information included to assist in identifying an individual who or organization that is reasonably suspected of involvement in an identifiable criminal activity or enterprise?
 - ii. Does the record include an appropriate disclaimer or designation of the individual or organization as noncriminal identifying information?
- g) Does the record include required source reliability and content validity (confidence) codes?

2. Validation/Retention/Destruction/Purge

- a) Were records (including backups of reports) purged from the system and/or destroyed (per project policy) in a timely manner?
- b) If the record was validated for a new retention period, did the reviewer provide an explanation for retention demonstrating continued compliance with system submission criteria?¹²

3. Sharing/Dissemination

Directions: Using the dissemination log or audit trail, review a random sampling of CII records that have been disseminated.

- a) Was the record disseminated only to those law enforcement authorities who have agreed to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with the 28 CFR Part 23 operating principles?¹³
- b) Were the recipients of the record or product authorized to request and receive CII records from the criminal intelligence system during the period covered by the audit?
- c) Did the record include required dissemination (sensitivity) codes (e.g., FOUO, LES, etc.)?
- d) Was there a clear law enforcement purpose to the dissemination? Was it documented?

Part B—Products (Situational Awareness, Analytic)¹⁴

Part B addresses a broad range of informational and analytic products—including situational awareness and analytic products—developed by the intelligence function.

Directions: Review a random selection of products, and for each product, answer the following questions:

1. Purpose and Creation of the Product

- a) Does the product address the agency's delineated customer needs (e.g., the agency analytic production plan or identified Standing Information Needs [SINs] or Priority Information Needs [PINs])?
If not:
 - i. Does the product fall within the agency's mission?
 - ii. If the product falls outside the agency's delineated customer needs, is there nonetheless a legitimate reason to create the product, such as a specific request from leadership?
- b) If the product originated from another source, did it undergo the same P/CRCL review for compliance with agency standards as internally produced products before the name/seal of the agency was affixed to the product?

2. Sources and Labels

Sources

- a) Are the sources for the information cited and rated for confidence (i.e., source reliability and content validity) using agency-established standards?¹⁵
If not:
 - i. Does the source meet one of the exceptions noted in agency policies (e.g., source's identity concealed to protect the source)?
- b) Are any limitations on the quality of the information or source reliability clearly identified and reflected in the confidence level assigned to the product?

Labels

- a) Is the information contained in the product labeled regarding any restrictions on access, use, or disclosure of the information to:
 - i. Indicate applicable legal restrictions for sharing and handling information based on the information's sensitivity or classification?

- ii. Protect confidential sources, police undercover operations, or pending criminal investigations?
- iii. Protect an individual's right of privacy or his or her civil rights and civil liberties?
- b) If the product was repurposed for a new audience or if new information was added, were any labels assigned to existing information reevaluated (e.g., for changes in access or disclosure limitations)?
- c) Are facts and opinions correctly labeled or identified as such?

3. PII and Data Quality Issues

- a) If the product contains personally identifiable information (PII), is the PII necessary to the usefulness of the product?
 - i. Is it possible to minimize the PII and still convey the essential points?
 - ii. Is there any extraneous PII (e.g., such as information about individuals who are not the subject of a record)?
- b) For any individual identified in the record, are there applicable laws providing greater privacy protections to that individual as a member of a special class (children, victims of sexual abuse, residents of substance abuse treatment programs, residents of mental health treatment programs, residents of domestic abuse shelters, etc.)?
- c) Was any of the data used in the product subsequently corrected or the subject of an agency data quality review and found to be in error, deficient, or otherwise problematic?

If so:

 - i. Was the product amended or invalidated in light of the erroneous data?
 - ii. If the product was disseminated, was a correction issued through the same dissemination channels and documented?

4. Conclusions and Individual Product Dissemination Considerations

Conclusions

- a) Are the conclusions stated in the product clearly related to analytical judgment?
- b) Does the factual information presented fully support the conclusions? (Are there sufficient derogatory facts to support any assessment of possible terrorism or other criminal behavior?)
- c) Does the product make clear what action(s) the reader is advised to take based on the information covered in the product (i.e., is it actionable)?

Individual Product Dissemination Considerations

- a) Is there documentation that the product was reviewed for P/CRCL considerations before dissemination?


If so:

- i. Was the reviewer the P/CRCL Officer or another official with specialized P/CRCL training?

- b) Is the product properly marked under agency policy or procedures (e.g., third-party dissemination, target audience, classification, expiration or discard date, and appropriate security), and are appropriate dissemination lists used?

If so:

- i. Was the restricted dissemination necessary?



5. CRCL “Red Flags”

Red flag questions: Included in this area are questions based on a “red flags” approach. A “red flag” is an area that requires closer scrutiny to certain elements of a product based on various constitutional or statutory considerations. It does not necessarily indicate an error or a problem, only the need for a review for potential P/CRCL implications.



Overall Impression of Neutrality

- a) Does the product include any statements conveying an implicit personal/institutional opinion about any belief system or group, especially if related to a controversial event?
 - i. Are references to religious, political, or social views, associations, or activities neutral in tone and without negative characterizations?
 - ii. Are the references to First Amendment activities documented in the record necessary to understand the law enforcement purpose the document is intended to convey?
 - iii. Does the agency refrain from editorializing or taking a position on the value of the belief systems/groups that were the subject of the report?



Use of Descriptors

Descriptive language used in products may raise civil liberties concerns in some instances when overly broad use of descriptors may negatively implicate an entire category of individuals who may then be subject to law enforcement action, search, or restraints based on this overly broad descriptive language.

- a) Does the product avoid the use of broad, vague terms that can be interpreted to include constitutionally protected activities (e.g., extremist, radical, far right, far left)?

- b) Are specific demographic descriptors properly used (i.e., *descriptors are used to aid law enforcement in identifying a known criminal suspect*)?

Note: Under the ISE-SAR Functional Standard,¹⁶ reference to factors such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).

- i. Is the inclusion of sensitive descriptors necessary to serve the law enforcement or homeland security purpose?
 - ii. Does the product refer to an individual's race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in a manner that unfairly imputes the individual's alleged bad actions to all members of a group to which the individual belongs?¹⁷
 - iii. Does the product describe an individual in a manner that unfairly imputes the individual's alleged bad actions to a larger group to which the individual belongs (e.g., protestors, veterans, militias, or environmental activists)?
- d) Is the product based on individual behavior and not on stereotypes, assumptions, or generalizations about an individual (i.e., race, ethnicity, national origin, religion, gender, sexual orientation, or gender identity)?¹⁸



Use of Religious Terminology

- a) Does the product use religious terms that are not quotes from another source?
- b) Does the product avoid an implied government endorsement or disapproval of a particular interpretation of a religious term, even if the term is used in the media or the group itself?
- c) Does the product avoid using terms such as “moderate” or “extremist” to describe individuals engaged in religious debate, as their use may imply government endorsement or disapproval of a particular religious expression or interpretation?



For Products Covering Violence, Terrorism, or Other Illegal Activity

- a) Does the product clearly demonstrate a link between the individual or group and the prior, current, or planned terrorist or other criminal activity before concluding that the individual or group is involved in criminal activity?
 - **Note:** In some instances, a description of individuals or groups who are victims or targets of violence must be included to provide a necessary context for investigation of an illegal act. These persons or groups should be marked as victims, witnesses, etc.
 - **Note:** In other instances, public safety concerns may require the inclusion of additional persons or groups, although these products are likely to have more local distribution.

- b) Is the “nexus” with violent or other criminal activity supported by clearly articulated, factual information?
- c) Is the product driven by behavioral facts relating to what the individual did or planned to do?
- d) Does the product avoid citing the subject’s previous expressions, including those found on open source forums such as social media, which are not directly relevant to the potential criminal activity or which do not constitute a direct incitement to imminent violence or terrorism?

If the subject’s expressions are included:

- i. Review the context to ensure that the inclusion of the opinions in the report was essential to the purpose of the product.
 - ii. Verify that the product does not infringe on the First Amendment right to petition government for a redress of grievances (e.g., communicate support or opposition to public policies), regardless of the controversy of the statement.
- e) Does the product avoid attributing the violent or other criminal actions of an individual to any group or affiliation associated with that individual, unless it is known for certain that the larger group had publicly endorsed or undertaken similar actions?
 - **Note:** When a group spokesperson has specifically disavowed the individual’s action, it is problematic to cite the affiliation, unless there is specific and credible information indicating that the group is in fact supportive of the individual’s actions.
 - **Note:** Terrorist groups will often claim responsibility for an act when they, in fact, were not involved.
 - **Note:** If there is sufficient evidence that a group actively advocates or uses violence, it is reasonable to attribute an individual member’s violence or other criminality to the larger group when an individual was acting under directions from the group or from leadership of the group or was clearly advancing the group’s aims using methods approved or endorsed by the group.
 - **Note:** The intelligence component should validate that a particular individual is serving as the affiliated or known spokesperson for the group or as the event organizer before including such information in a product.¹⁹
 - f) Does the product properly describe the individual’s most current status in any legal proceedings (e.g., arrested, charged, indicted, arraigned, pending trial, convicted, sentenced, on probation, or paroled) and avoid attributing guilt to an individual prior to adjudication?
 - g) If the product includes statements that an individual has been implicated in a crime, does the product clearly cite to a legal document, such as a complaint, a warrant, or an indictment?²⁰



Other Constitutional Considerations

- a) Does the product address First Amendment-protected activities (e.g., protests, conferences, reading materials, religious practices, published or spoken political opinions, lobbying)?
If so:
 - i. Do those reported activities involve violence or other criminal behavior, a public or officer safety concern, or a lawful criminal predicate that permits such reporting?
 - ii. Is the product and inquiry into the First Amendment-protected event proportional (in length, content, amount of PII included, etc.) to the threat posed?
- b) Does the product include extraneous constitutionally protected biographic information and activities (i.e., not necessary for specific suspect descriptions for identification purposes), such as:
 - i. The subject's race, ethnicity, religion, national origin, gender, gender identity, or sexual orientation?
 - ii. The subject's religious, political, or social views, associations, or activities?
- c) If information detailing subjects' constitutionally protected activity, speech, or characteristics appears in the product,²¹ are there any patterns indicating that one group is over- or underrepresented for impermissible reasons (e.g., bias, animus)?

Part C—Information Sharing Environment-Suspicious Activity Reports (ISE-SARs)²²

This section identifies questions related to the audit of ISE-SARs, including their adherence to the ISE-SAR Functional Standard 1.5.5 (ISE-SAR FS).²³ The standardized and consistent vetting of SARs within an intelligence function and the appropriate sharing of ISE-SARs are vital to assessing, deterring, preventing, or prosecuting those involved in terrorism-related criminal activities.

Directions: Review a random selection of ISE-SAR submissions, and for each submission, answer the following questions:

1. Information

- a) Does the ISE-SAR comply with the agency's P/CRCL policy and applicable procedures?
- b) Was the information collected in a lawful manner?²⁴

An ISE-SAR is official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity.

2. Acquiring and Receiving Information

- a) Was the ISE-SAR assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value?

Ways to accomplish this include:

- Determining source reliability.
- Assigning the record a disposition label (e.g., undetermined or unresolved, cleared or unfounded, verified, or under active investigation).
- Determining content validity (i.e., reliable, unreliable, unknown).
- Attempting to validate or refute the information.
- Requiring ISE-SARs to employ a standard reporting format and data collection codes.

3. Vetting

- a) Was the ISE-SAR vetted using a human review to identify it as an ISE-SAR?
- b) Does the ISE-SAR include information regarding observed behavior that has a potential nexus to terrorism (i.e., *Is it reasonably indicative of criminal activity associated with terrorism?*) based on the available context, facts, and circumstances?
- c) Does the ISE-SAR include one or more of the 16 behaviors associated with preoperational planning that may be associated with terrorism, as enumerated in Part B of the ISE-SAR FS?
- d) If the ISE-SAR includes PII²⁵ and the identified behavior(s) are not inherently criminal, are there additional facts or circumstances articulated that clearly support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism?²⁶
- e) Does the ISE-SAR include race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity as *factors* creating suspicion?²⁷

If so,

- i. Are the attributes documented in specific suspect descriptions for identification purposes only?

4. Validating/Retention/Destruction/Purge

- a) Was the ISE-SAR stored as appropriate, per agency policy?
- b) Was the ISE-SAR validated and retained for a defined retention period in accordance with the agency's P/CRCL policy provision?

5. Sharing/Dissemination

- a) Was access to or dissemination of the ISE-SAR based on an individual's "need to know" and "right to know" the information in the performance of a law enforcement activity?

Part D—Other Records Subject to the Agency's P/CRCL Audit

This section addresses other types of information and criminal intelligence products and records that may raise P/CRCL considerations. Agency personnel should consider soliciting input from agency governance and oversight entities to determine whether other types of records or policy implementation questions should be included in this audit plan.

Examples of information and criminal intelligence products and records that generate records and products potentially raising P/CRCL issues include:

- Responses to Requests for Information (RFIs).
- Acquisition and use of open source information, including information derived from social media Web sites.
- Open source research practices.
- Acquisition and use of technology (e.g., license plate readers) to assess and mitigate the risks associated with the acquisition and use of the technology during the audit period.
- Use of commercial databases.
- Tips and leads, including suspicious activity reports (non-ISE-SARs).
- Information in the intelligence component's records management system (RMS) or computer-aided dispatch (CAD) system, if repurposed and included in records subject to the agency's P/CRCL policy.

Section 2: Assessing Implementation of the P/CRCL Policy

This section builds upon three documents: *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*,²⁸ originally designed for the National Network of Fusion Centers; *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*;²⁹ and *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*.³⁰ The suggested questions will help any agency with an intelligence function gather and share information in a manner that protects P/CRCL.

1. Governance and Oversight

- a) Was the P/CRCL policy updated as required?
- b) Have all personnel,³¹ including external personnel (e.g., liaison officers), received and signed/acknowledged agreements to comply with the P/CRCL policy?

2. Information Quality Assurance

- a) If there were any alleged data errors or deficiencies during the audit period, did the agency conduct a timely review (or notify the source agency of alleged errors or deficiencies), correct or delete any actual errors, and refrain from subsequent use of the defective information?
- b) During the audit period, did the agency conduct periodic data quality reviews of information it originated to ensure that (i) it is accurate and reliable, (ii) the agency has authority to gather it and to share it (if applicable), and (iii) the information was gathered in accordance with agency policy and applicable laws?

3. P/CRCL Policy Training

- a) If required, was training provided to agency personnel on:
 - i. The P/CRCL policy?
 - ii. Responsibilities related to the submission, maintenance, or dissemination of CII in accordance with 28 CFR Part 23 and the agency's P/CRCL policy?
- b) If the agency vets and submits ISE-SARs to the eGuardian NSI SAR Data Repository (SDR), is there at least one analyst or investigator who has completed the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) training?

4. Sharing and Dissemination

- a) Have all members or participating agencies signed the user agreements or memoranda of understanding (MOUs), accepting and agreeing to follow procedures regarding the receipt, maintenance, security, and dissemination of CII that are consistent with the operating principles set forth in 28 CFR Part 23?
- b) Based on the random sample of CII related to terrorism, has the agency implemented the ISE Privacy Guidelines requirement to limit the sharing of information through the Information Sharing Environment (ISE)³² to terrorism, homeland security, and law enforcement (terrorism-related) information?
- c) Did the agency maintain an audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed?

5. Information Sharing/Dissemination

- a) If the intelligence function delegated the responsibility to determine need and right to know to recipient agencies/personnel/others, was the recipient properly trained in making such determinations?³³

6. Records Retention Policy Implementation

- a) Were appropriate personnel trained on the agency's records retention policy and provided a copy of the policy?

7. Records Purge Policy Implementation

- a) Were all validation/purge/retention policies and business practices consistently enforced in a timely manner during the audit period?
- b) Was a record kept to document all purged information?

8. P/CRCL Policy Violations and Data Breaches

- a) Is there a designated point of contact to whom agency personnel are required to report violations of the P/CRCL policy?
If yes,
 - i. Is the agency's point(s) of contact trained on the process for investigating and documenting violations of the P/CRCL policy?
- b) If any P/CRCL policy violations were reported during the audit period, was the policy for handling violations followed?

- c) If there were any data breaches involving PII (including PII contained in a CII record) during the audit period, were agency procedures for handling breaches followed?
- d) Is the agency subject to external reporting of data breaches (e.g., to a state or city attorney general's office)? If so, what is the reporting responsibility and to whom? How frequently does external reporting occur?

9. Redress Policy Implementation

- a) If there were any public records requests during the audit period, did the agency's decision to disclose or withhold the requested record(s) comport with relevant laws, standards, and agency policy?
- b) If there were any requests for records corrections or complaints regarding information on individuals in disclosed records during the audit period, was the agency policy for handling such requests/complaints followed?

10. Security Safeguards

- a) Has the agency implemented administrative, technical, and physical safeguards (including audit trails) to ensure against unauthorized access and against intentional or unintentional damage to the information gathered or collected by the agency?

11. P/CRCL Policy Public Outreach and Transparency of Operations

- a) If required by policy, was the agency's P/CRCL policy available to the public during the period of the audit?

Endnotes

1. See Section 1 (D), “Other Records Subject to the Agency’s P/CRCL Audit,” for additional questions.
2. Agencies may also release the full audit, with redactions as necessary to protect the privacy of any individual or group, if appropriate and consistent with jurisdictional requirements.
3. See <http://it.ojp.gov/privacy> for additional information on Global Privacy Resources.
4. Fusion centers may also release the full audit, with redactions as necessary to protect the privacy of any individual or group, if appropriate and in compliance with policies, laws, and regulations.
5. As stated in 28 CFR Part 23, “Criminal Intelligence Information (CII) means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria.”
6. The *National Criminal Intelligence Sharing Plan* is available at <https://it.ojp.gov/gist/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>.
7. Note that products containing CII should be reviewed first using the questions in this section and then using the relevant questions under Section 1, Part C.
8. See 28 CFR §23.20(d), “A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance.”
9. 28 CFR §23.20(c) states, “Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.”
10. 28 CFR §23.20(b) states that “a project shall not collect or maintain criminal intelligence information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.”
11. 28 CFR §23.20(d) states that “a project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance.”
12. 28 CFR Part 23 states, “Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.” The standard for retention cycles is up to 5 years.
13. There is an exception for dissemination of an assessment of CII if necessary to avoid imminent danger to life or property. See 28 CFR §23.20.
14. The intelligence component of many entities, including fusion centers, describes products by a host of names: some are focused on various sectors (e.g., Emergency Services Chronicle); others target specific issues (e.g., a Human Trafficking Report). Other descriptive names include Intelligence Bulletin, Product, or Assessment; Information Report; Monthly Information Sharing Bulletin; Officer Safety Information; Situational Awareness Bulletin; Special Advisory; Major Event Threat or Risk Assessment; and Security Brief. Note that the products containing CII should be reviewed first using the questions under Part B and then under Part C.
15. See LEIU’s *Criminal Intelligence File Guidelines* for additional information regarding confidence codes (i.e., source reliability and content validity), https://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.
16. ISE-SAR Functional Standard 1.5.5—Section IIB, page 10: “It is important to stress that this behavior-focused approach to identifying suspicious activity requires that factors such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).”

17. For more information about commonly used standards, including Title VI, see the supplemental Audit Guidance Web resources. <http://it.ojp.gov/privacyliberty>.
18. See *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* for additional information, <http://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf>.
19. See *Recommendations for First Amendment-Protected Events for State and Local Law Enforcement*, <http://it.ojp.gov/GIST/35/Recommendations-for-First-Amendment-Protected-Events-for-State-and-Local-Law-Enforcement-Agencies>.
20. In certain instances, reviewers will have access to or may wish to gain access to the source material documentation for a particular product. This may arise if (1) a supervisory analyst is part of the audit team, (2) there is a particular audit goal of reviewing the products of new analysts or a new line of products, or (3) there have been problems in the past. In other circumstances, this is likely to be outside the scope of the audit review of products. Source review for reliability is part of the analytic development process.
21. In the context of intelligence products, there is likely a legitimate reason for such disproportionality, such as a discrete, violent/criminal event that involved suspects of only one race, ethnicity, national origin, religion, sexual orientation, gender, or ideology. However, because the characteristics, associations, and expressive behavior cited above are protected by the Constitution, a deeper review as a part of the audit may be needed to determine whether any disproportionality is reasonable (e.g., whether each record affected by the constitutionally protected attribute or activity at issue is supported by a potential nexus to criminal activity of the individual or group).
22. An ISE-SAR is a SAR that has been determined by a trained analyst or investigator, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of preoperational planning associated with terrorism). The ISE-SAR FS highlights the importance of having a trained analyst or investigator take into account the context, facts, and circumstances in reviewing suspicious behaviors to identify those SARs with a potential nexus to terrorism.
23. http://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf.
24. The ISE-SAR Functional Standard (p. 10) states, “The same constitutional standards that apply when conducting ordinary criminal investigations also apply to Federal and SLTT law enforcement and homeland security officers collecting information about suspicious activity. The ISE-SAR Functional Standard does not alter law enforcement officers’ constitutional obligations when interacting with the public.” http://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf.
25. Auditors and other personnel may determine the presence of PII by determining whether the ISE-SAR submission includes data in the identified “privacy fields” (Ibid., § 5(o)).
26. ISE-SAR Functional Standard (p. 41, part 4) states that if the identified behavior(s) are not inherently criminal, it may not be documented as an ISE-SAR that contains PII “unless there are articulable facts or circumstances that clearly support the determination that the behavior observed is not innocent, but rather reasonably indicative of pre-operational planning associated with terrorism.
27. See the Fusion Center Privacy Policy Template, pp. 10 and 41. It is important to note that these attributes must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes). Consideration and documentation of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity shall be consistent with applicable guidance, including for federal law enforcement officers. See ISE-SAR Functional Standard 1.5.5, p. 10, n. 9, citing *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (December 2014).
28. See Fusion Center Privacy Policy Template at <http://www.it.ojp.gov/GIST/48/Fusion-Center-Privacy-Policy-Development--Privacy--Civil-Rights--and-Civil-Liberties-Policy-Template>.
29. See <http://www.it.ojp.gov/GIST/31/Privacy--Civil-Rights--and-Civil-Liberties-Policy-Development-Guide-for-State--Local--and-Tribal-Justice-Entities--Privacy-Guide>.

30. Global and DHS/DOJ Fusion Process Technical Assistance Program and Services, *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* (June 2010).

31. Personnel—includes employees, detailees, interns, assignees, contractors (e.g., personnel providing information technology services to the agency), and others whose job functions require them to have access to protected information (e.g., personnel from other agencies who are colocated in the intelligence component).

32. The ISE was established by the Intelligence Reform and Terrorism Prevention Act of 2004 as amended. See Section 1016(a) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended and codified at 6 U.S.C. § 485(a). The ISE broadly refers to the people, projects, systems, and agencies that enable the responsible sharing of terrorism-related information. In the ISE, “terrorism-related information” includes terrorism information, homeland security information (including weapons of mass destruction information), and law enforcement information related to terrorism.

33. *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*, p. 17.

34. Including the Intelligence Reform and Terrorism Prevention Act of 2002 and Executive Order 12333.

Appendix A—Pre-Audit Planning Checklist

9-Step Pre-Audit Checklist														
Completed	Step to Be Completed													
<input type="checkbox"/>	<p>1. Determine whether the P/CRCL Policy has been reviewed since the last audit or within the past year.</p> <p>After reviewing the P/CRCL policy, note the date of the review and reviewers involved and, if applicable, the date of the last audit.</p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="text-align: center;">Date the policy was created</th> <th style="text-align: center;">Last date policy reviewed</th> <th style="text-align: center;">Reviewers</th> </tr> </thead> <tbody> <tr> <td style="height: 40px;"></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1" style="width: 100%;"> <thead> <tr> <th style="text-align: center;">Related policies</th> <th style="text-align: center;">Last date audit conducted</th> <th style="text-align: center;">Reviewers</th> </tr> </thead> <tbody> <tr> <td style="height: 40px;"></td> <td></td> <td></td> </tr> </tbody> </table> <ul style="list-style-type: none"> ◀ A review should include: <ul style="list-style-type: none"> • Consultation with applicable legal advisors to determine whether the P/CRCL policy meets all applicable legal requirements (see #3 below). • Consideration of whether the policy fully reflects current processes and practice. ◀ The intelligence function may not have a single, stand-alone policy but be subject to various agency policies that include elements of P/CRCL protections. ◀ If the P/CRCL policy has not been reviewed since its creation, consider consulting the <i>Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise</i> for the capabilities needed to ensure P/CRCL protections. <p>NOTE: Consider interviewing key staff members on the operational implementation of the current policy to determine potential changes or gaps.</p>		Date the policy was created	Last date policy reviewed	Reviewers				Related policies	Last date audit conducted	Reviewers			
Date the policy was created	Last date policy reviewed	Reviewers												
Related policies	Last date audit conducted	Reviewers												

9-Step Pre-Audit Checklist

Completed	Step to Be Completed
<input type="checkbox"/>	<p>2. Form an audit “team.”</p> <ul style="list-style-type: none"> ◀ Depending on the structure of the intelligence function, team members may include: <ul style="list-style-type: none"> • Intelligence function director • P/CRCL Officer • Supervisors of various offices or work units • Intelligence enterprise director or deputy • State/city Attorney General representative • Parent-agency representative • Legal advisor for the enterprise • Neighboring-agency intelligence enterprise director or P/CRCL Officer • Chief Information Officer representative or director of the agency’s IT department • Analyst or Supervisory Analyst ◀ The P/CRCL Officer should have primary responsibility for coordination of the various aspects of the privacy and civil liberties function within the intelligence function and should be an integral part of the audit process. ◀ Skills and knowledge of at least one team member should include: <ul style="list-style-type: none"> • Authority to ensure that the audit results will be acted upon • Knowledge of 28 CFR Part 23 implementation in the context of an intelligence function or fusion center serving as an intelligence project or participating in an intelligence project • Legal expertise • Intelligence records management • Operational knowledge to ensure that informal or outlier record-keeping practices are addressed • IT professional who can address issues related to technological systems, record storage, access limitations, purge, etc., and has knowledge of all of the relevant IT standards ◀ The Security Officer and an IT professional may also be involved team members for the entire process or for any part of the process when their expertise is helpful. ◀ Fusion centers may wish to use the DHS peer-to-peer exchange to identify external fusion center staff to join or advise the audit team.

9-Step Pre-Audit Checklist

Completed	Step to Be Completed
<input type="checkbox"/>	<p>3. Conduct a legal framework review—See Appendix B.</p> <ul style="list-style-type: none"> ◀ Assess whether any relevant changes have occurred since the P/CRCL policy was last updated by reviewing: <ul style="list-style-type: none"> • Federal law, regulations, or policy • Applicable federal funding requirements • State laws, case law, regulations, or policies ◀ This step will help determine any necessary changes to the intelligence function's P/CRCL policy and procedures and may be used to inform the P/CRCL audit. <p>Any issues identified in this area should be part of the post-audit recommended actions plan. (See #8 below.)</p>
<input type="checkbox"/>	<p>4. Identify the standards against which the audited records will be compared.</p> <ul style="list-style-type: none"> ◀ The most commonly used frameworks are: <ul style="list-style-type: none"> • The ISE Privacy Guidelines as they apply to fusion centers via DHS-reviewed P/CRCL policies and DHS grant requirements. • The ISE-SAR Functional Standard 1.5.5 (February 2015) for review of suspicious activity reports submitted to the SAR Data Repository. • 28 CFR Part 23: Criminal Intelligence Systems Operating Policies, which apply to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Also often used as the “de facto standard” for other criminal intelligence systems. • Title VI of the Civil Rights Act of 1964, which prohibits discrimination based on race, color, or national origin in any activities or programs receiving federal funds. • Privacy Act of 1974 • E-Government Act of 2002 • Federal Information Security Management Act (FISMA) <p>Note that the applicable guidance/standards against which the audit team will be examining the various types of records (e.g., intelligence products and ISE-SARs) will vary by type of record.</p>

9-Step Pre-Audit Checklist

Completed	Step to Be Completed
<input type="checkbox"/>	<p>5. Gather foundational documents.</p> <ul style="list-style-type: none"> ◀ Foundational documents that may be needed to consult while conducting the audit include but are not limited to: <ul style="list-style-type: none"> • <i>Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template</i> • <i>Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities: SLT Policy Development Template</i> • A current personnel list, including on-site personnel employed by other entities • Information sharing MOUs with partners (for data access procedures) • Other agency policies with P/CRCL components, such as “Use of Social Media” • Description of analytic product dissemination lists ◀ Also see audit-related resources available as part of the P/CRCL Officer Toolkit, which is part of the www.it.ojp.gov/PrivacyLiberty Web portal noted above.
<input type="checkbox"/>	<p>6. Gather a random sampling of the classes of records that will be subject to the audit.</p> <ul style="list-style-type: none"> ◀ Identify the information technology systems and any other record-keeping storage management systems and/or physical repositories that hold records/information to be audited. ◀ Review the agency’s records sampling methodology—determine sample size and how to select a representative, random sample. ◀ Note that the audit team may include a greater number of certain record types that are more likely to contain possible P/CRCL issues (such as analytic products).

9-Step Pre-Audit Checklist

Completed	Step to Be Completed
<input type="checkbox"/>	<p>7. Customize this P/CRCL Pre-Audit Checklist to the needs of the intelligence function.</p> <ul style="list-style-type: none"> Consider programs and processes that are unique to the intelligence function as well as new initiatives. A “Use of Social Media” policy is an example of an additional policy against which the audit team may wish to conduct a portion of the audit. This policy should contain privacy and civil liberties protections.
<input type="checkbox"/>	<p>8. Determine whether, based on the result of the pre-audit checklist, P/CRCL policy changes are needed.</p> <ul style="list-style-type: none"> If changes are needed to comport with current laws,³⁴ regulations, or policy or are based on an assessment of current operations, consider creating a post-audit plan to: <ul style="list-style-type: none"> Update the P/CRCL policy and train personnel on the updated policy. Distribute the updated P/CRCL policy to relevant stakeholders and post it to the enterprise and/or host agency’s Web site(s).
<input type="checkbox"/>	<p>9. Set a date and location for the audit. In addition to the pre-audit work, plan on setting aside at least a full day for the audit.</p>

Appendix B—Potentially Applicable Federal Statutes and Types of State Laws

The state, local (including ordinances), tribal, or territorial laws that may be relevant to the intelligence function records audit include:

- State constitutional provisions: privacy, civil rights, and civil liberties clauses
- Statutory civil rights laws
- At-risk adults laws
- State freedom of information or “sunshine” laws
- Open records laws
- Financial information privacy laws
- Consumer fraud protection laws
- Communication protection laws
- Health care and communicable disease information privacy laws
- Juvenile or victim/witness identification restrictions
- Privacy laws defining protected information and prohibiting its authorized collection or disclosure
- Education information privacy laws
- Laws regulating the use of data obtained via unmanned aerial surveillance, license plate reader technology, or biometric information
- Law enforcement or intelligence use of data obtained from social media
- Statutes related to sharing or handling of data sets or subsets of information within the data set
- Juvenile privacy protection and parental empowerment laws
- Laws dictating a records retention schedule
- Laws conferring authorization to record communications, such as anti-money laundering and/or organized crime laws
- Laws prohibiting unauthorized interception, recording, disclosure, alteration, or use of communications
- Laws prohibiting the unauthorized intrusion upon personal privacy/tranquility/seclusion
- Anti-wire fraud laws
- Laws prohibiting the unauthorized tampering with or access to communication equipment or computers
- State emergency management acts
- Laws dictating data breach response measures, including incident reporting

The federal laws that might be relevant to an intelligence function records audit include:

Following is a partial list of federal laws that should be reviewed when conducting a records audit. The list is arranged in alphabetical order by popular name. Short descriptions of the laws and their potential relevance to state, local, tribal, or territorial intelligence enterprises can be found at www.it.ojp.gov/PrivacyLiberty portal under the “Authorities” tab.

- **Brady Handgun Violence Prevention Act**, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A.
- **Computer Matching and Privacy Protection Act of 1988**, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, “Guidance on Interagency Sharing of Personal Data—Protecting Personal Privacy,” December 20, 2000.
- **Confidentiality of Identifiable Research and Statistical Information**, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22.
- **Criminal History Records Exchanged for Noncriminal Justice Purposes**, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611.
- **Criminal Intelligence Systems Operating Policies**, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23.
- **Criminal Justice Information Systems**, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20.
- **Electronic Communications Privacy Act of 1986**, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508.
- **Federal Civil Rights laws**, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983.
- **Indian Civil Rights Act of 1968**, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301.
- **National Crime Prevention and Privacy Compact**, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616.
- **U.S. Constitution.**
- **USA PATRIOT Act**, Public Law 107-56 (October 26, 2001), 115 Stat. 272.

Appendix C—General Principles for Developing Audit-Recommended Actions

Recommended actions for the vast majority of the issues identified in an agency's P/CRCL audit will fall into one of the following **four general categories**. In addition to the four general categories, there are **recommended actions tailored** to responses for RFIs, products, and P/CRCL policy implementation issues. If the errors discovered in the audit appear to be a pattern, consider pulling additional records to verify and then determine the best approach.

General Recommended Actions

For each instance of noncompliance or other issue discovered in an audit, decide whether the problem stems from one or more of the following:

1. Training issue
 2. Policy gap
 3. Technology interface issue
 4. Deliberate misuse issue
1. **Training Issue:** Training can be preventive or remedial, individualized, or generalizable for all personnel. In some instances, individualized remedial training may be transformed into more general preventive training for agency personnel. Training gaps can be addressed through a variety of approaches, including:
 - Creating a job aid/worksheet/checklist.
 - Changing a form or software field to prompt the user.
 - Providing individualized coaching/feedback.
 - Developing issue- or job function-specific training for relevant staff.
 - Modifying the orientation for staff or liaison officers to include missing information.
 - Updating the annual P/CRCL policy training to address the gap.
 2. **Policy Gap:** Determine whether the P/CRCL policy needs to be updated to explicitly address the problems associated with the noncompliant behavior. This may mean clarifying policy language to address a gap or updating the policy to meet applicable legal authority (consult legal counsel). Alternatively, consider whether the noncompliant behavior demonstrates a need to update the P/CRCL policy to conform to existing operations. (Be sure any change does not undermine required P/CRCL protections, including those required for grant recipients.) Finally, consider adding additional P/CRCL protections to other agency policies or procedures.
 3. **Technology Interface Issue:** In many instances, there will be a technology element associated with the access, storage, retrieval, retention schedule, and purging of agency records. When identifying the root cause(s) of P/CRCL-related issues, consider whether technical changes are warranted (e.g., access protocols, pull-down menus, software or programming, automation of retention schedule reminders, the addition of prompts next to certain data fields, or other technology-based solutions). In addition, the audit team

should test to ensure that electronic alerts for identifying retention deadlines are operational and tested periodically.

4. **Deliberate Misuse Issue:** If deliberate misuse is suspected, the audit team, in consultation with agency leadership, should prepare to pull additional records to support an investigation (in the event that one is opened).

Appendix D—Template for Internal Memorandum From the Audit Team

MEMORANDUM

TO: *Director*

FROM: *Privacy, Civil Rights, and Civil Liberties Officer*

DATE: [Date]

RE: [Year] P/CRCL Audit

On [date], an audit team conducted a privacy, civil rights, and civil liberties (P/CRCL) protections audit of the intelligence component of [name of entity]. The audit was conducted using the following documents: *Privacy, Civil Rights, and Civil Liberties (P/CRCL) Audit Guidance for the State, Local, Tribal, and Territorial Intelligence Enterprise* and the [entity P/CRCL policy]. A sampling of records and products was reviewed for compliance with relevant standards. In addition, the audit team included a review of the following agency policy(ies): [name(s) of policy audited]

I have attached the following documents regarding the audit:

Exhibit A: *Audit Guidance cited above*

Exhibit B: *P/CRCL Policy*

Exhibit C: *P/CRCL Audit Summary: Methodology, Findings, and Dispositions*

Based upon this audit, it is my opinion that the intelligence function within our agency is in [compliance/noncompliance] with the law and the P/CRCL policy.

In the interests of public transparency and to demonstrate the commitment of [agency name or abbreviation] to comply with all relevant privacy, civil rights, and civil liberties laws, regulations, and policies in the conduct of the intelligence component, a summary of the audit methodology and certain key audit outcomes will be posted on the agency Web site at [insert URL].

[Signature]

