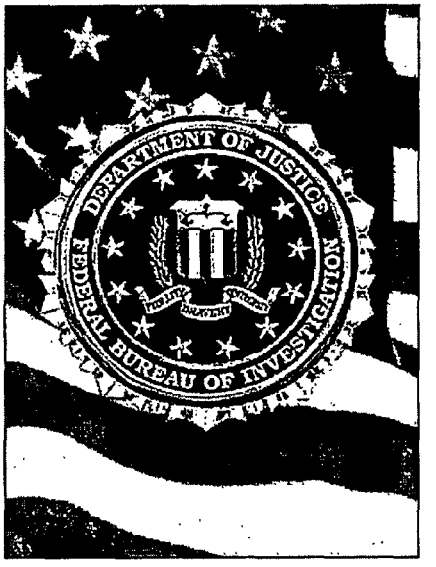
~~SECRET~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) Intelligence Information Report

Policy Implementation Guide



DATE: 05-24-2011
CLASSIFIED BY 65179 DMH/baw
REASON: 1.4 (C)
DECLASSIFY ON: 05-24-2036

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Federal Bureau of Investigation

0292PG

June 10, 2010

~~SECRET~~ ~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) GENERAL INFORMATION: Questions pertaining to this policy implementation guide (PG) may be directed to:

FBIHQ, Directorate of Intelligence/Division 19

(U) Division Point of Contact: DI/Division Policy Officer [redacted] b6 b7C

(U) NOTE: This document supersedes the following:

1) FBI Intelligence Information Report Handbook (last updated 5/14/2008);

2) Counterterrorism Division's Principles of Intelligence Information Report (IIR) Writing: A Reports Officer Guidebook (last updated 05/15/2006); and b7E

3) Recall/Revision Policy EC [redacted] (See Section 4.7.16.1.1.1).

(U) Table of Contents

[redacted] b7E

(U) List of Appendices

b7E

1. (U) Scope

1.1. (U) Purpose

(U) The FBI *Intelligence Information Report (IIR) Policy Implementation Guide (PG)* provides detailed guidance to assist FBI employees involved in writing and/or disseminating IIRs. The PG enhances the FBI's ability to provide raw intelligence information that is consistent with the content and format found throughout the United States Intelligence Community (USIC). It is not, however, intended to be an FBI IIR Dissemination System (FIDS) user guide, nor is it a training guide. For full comprehension, many of the concepts discussed in the IIR PG require training by experienced reports officers. This PG is intended primarily as a reference guide.

1.2. (U) Background

(U) The FBI is mandated by the President, Congress, the Attorney General, and the Office of the Director of National Intelligence (ODNI) to produce intelligence in support of its own investigative mission, national intelligence priorities, and the needs of other intelligence consumers. The IIR is a vehicle through which raw intelligence is shared within the FBI and throughout the intelligence and law enforcement communities, and it is currently the primary means by which the ODNI monitors and measures the FBI's intelligence reporting performance. All FBI Headquarters (FBIHQ) divisions and field offices (FO) must make collected raw intelligence information available in the IIR format.

1.3. (U) Intended Audience

(U) All FBIHQ divisions, FOs, and legal attaches (Legat) are to immediately adopt the FBI IIR PG for the reporting of raw intelligence. This PG is intended for IIR writers who have had a minimal level of training and, therefore, familiarity with the general concepts discussed herein.

Link to Policy: Intelligence Information Reports Policy Implementation Guide Corporate Policy Directive 0292D

2. (U) Roles and Functional Responsibilities

2.1. (U) IIR Authors

(U) All FBIHQ divisions and FOs will adhere to the process for the production of IIRs, as set forth in this PG. Intelligence analysts (IA), language analysts (LA), special agents (SA), task force officers (TFO), and any other individuals in a position that requires writing IIRs are required to use this PG as the source of policy information when drafting, coordinating, and disseminating IIRs.

2.2. (U) IIR Reviewers

(U) Individuals with the responsibility of reviewing IIRs must ensure all IIRs adhere to the policies set forth in this PG. Examples of IIR reviewers in FOs include the chief reports officers (CRO), associate chief reports officers (ACRO), field intelligence group (FIG) supervisors, and Intelligence Assistant Special Agents in Charge (ASAC). Examples of IIR reviewers at FBIHQ include supervisory intelligence analysts (SIA) and unit chiefs (UC).

2.3. (U) Legal Attaches (Legat)

(U) International Operations Division (IOD) is responsible for disseminating intelligence via IIR for Legats. Legats are encouraged to identify intelligence suitable for dissemination and forward it to IOD.

2.4. (U) SAs and TFOs Assigned to Investigative Squads and FIGs

(U) SAs and TFOs assigned to investigative squads and FIGs have an affirmative responsibility to collect and provide information that addresses FBI Collection Requirements, while carrying out their normal assessment and predicated investigation duties (referred to hereafter as "case-based investigations"). SAs and TFOs conducting case-based investigations have a significant opportunity to recognize and develop information of intelligence value, that is responsive to FBI Collection Requirements and should be shared with others who have a need for that intelligence. In addition, investigators may also acquire information that responds to requirements not levied by the FBI, which when disseminated to the USIC by IIR may prove of great value.

(U) It is critical for the FBI to continue to provide timely and accurate information to those who need it. Any FBI case-based investigation could potentially contain intelligence of actionable and/or analytical value. Therefore, investigators must become well versed in gleaning intelligence from their investigative efforts, even if such intelligence relates to another investigative program or has no direct impact on the specific assessment or predicated investigation conducted by the SA, TFO, or other FBI employee.

(U) All SAs and TFOs must determine if there is intelligence value to the information they collect, and if so, provide that information to the FIG for dissemination. It is the responsibility of every SA and TFO assigned to an investigative squad to work with the FIG and provide intelligence for dissemination, whether that dissemination would be internal to the FBI or external, via IIR, to the law enforcement community and/or USIC.

2.5. (U) Directorate of Intelligence

(U) The Directorate of Intelligence (DI) is responsible for program management, training, and policy regarding the dissemination of raw intelligence information collected by the FBI. Consistent with its mission, the DI establishes policy to ensure the FBI disseminates high-quality IIRs in a timely manner to the appropriate recipients.

3. (U) Policies

3.1. (U) FBI Intelligence Policy

(U//FOUO) The intelligence policy of the FBI is based on the United States Constitution; federal statutes; executive orders (EO) and Presidential directives (PD); Attorney General's guidelines (AGG) and Department of Justice (DOJ) orders; the *Domestic Operations and Investigations Guide (DIOG)*; Director of National Intelligence Directives (DNID) and Intelligence Community Directives (ICD); interagency memoranda; and other internal FBI policy implementation guides (PG).

3.2. (U) Other Relevant Authorities

(U) The policies set forth in the FBI IIR PG are intended to be consistent with the:

- *(U) The Attorney General's Guidelines for Domestic FBI Investigations* (AGG-Dom);
- *(U) Attorney General's Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons Memorandum;* and
- *(U) Domestic Investigations and Operations Guide* (DIOG).

3.2.1. (U) FBI IIR Dissemination System (FIDS) User Guide

(U//FOUO) FIDS is an automated tracking system that electronically connects FOs, Legats, and FBIHQ divisions to one another, transmits IIRs between participants in the IIR production process, and allows users to track the progress of IIRs during each stage of the process.

3.2.2. (U) Legal Review PG for IIRs

(U//FOUO) The Office of the General Counsel's (OGC) *Legal Review Policy Implementation Guide for IIRs* contains detailed guidance to assist FBI attorneys involved in reviewing IIRs. This PG provides attorneys with guidance concerning when pre-publication legal review of IIRs is required, and the standards to be applied by chief divison counsels (CDC), associate division counsels (ADC), or FBIHQ attorneys in performing the required legal review. FBI employees, task force personnel, detailees, contractors, and any other person engaged in the production of IIRs must adhere to the policies set forth in the *Legal Review PG for IIRs*, and use it as a central source of information when drafting, coordinating, or disseminating IIRs containing statutorily-restricted information or information concerning sensitive matters.

4. (U) Procedures and Processes

4.1. (U) Introduction

(U) The FBI is mandated by the President, Congress, the Attorney General, and the ODNI to produce intelligence in support of its own investigative mission, national intelligence priorities, and the needs of other intelligence consumers. The IIR is the primary vehicle through which raw intelligence is shared within the FBI and throughout the intelligence and law enforcement communities, and it is one of the primary means by which the ODNI monitors and measures the FBI's intelligence reporting performance. All FBIHQ divisions and FOs must make collected raw intelligence information available in the IIR format.

4.1.1. (U) Definition of an IIR

(U) The IIR is the FBI's primary document sharing mechanism for raw intelligence information. IIRs are transmitted electronically to recipients within the USIC and law enforcement communities, with redacted tearlines occasionally being transmitted to foreign government partners. The IIR is composed of raw intelligence gathered by FBI intelligence collectors, including SAs, TFOs, surveillance specialists, language analysts, and other personnel. IIRs generally consist of raw intelligence that has not been fully evaluated from a single source, and they include minimal interpretation and analysis. An IIR is not a tasking document and it cannot be used to solicit further information or request operational activities. An IIR is not intended solely as a means to communicate internally within the FBI, though every FO is a recipient of each IIR disseminated.

4.1.2. (U) IIR Audience

(U) IIR consumers range from the President at the national level, to an on-scene commander at the tactical level. Common IIR consumers include the following:

- USIC;
- White House;
- Senior national decision-makers;
- FBI FOs and other FBIHQ divisions;
- DOJ;
- Other federal authorities;
- State, tribal, and local law enforcement organizations; and
- Foreign governments and international organizations.

(U//FOUO) The FBI's policy is to share FBI intelligence whenever dissemination has the potential to protect the United States against threats to national security and/or improve the effectiveness of law enforcement.

4.1.3.

b7E

b1
b7E

4.2. (U) Requirements

(S)

(S) [redacted] b7E

(S) [redacted]

(U//FOUO) FBI intelligence needs may or may not correspond with other requirements issued under the authority of the Director of National Intelligence (DNI) [redacted]

(U//FOUO) In addition, the FBI may disseminate information that does not meet the definitions in (i) and (ii), if the information was collected incidentally, either from a case-based investigation, or against requirements that meet definition (i) or (ii). The DIOG does not discriminate between the two definitions for purposes of dissemination.

4.2.1. (U) FBI National Standing Collection Requirements

b7E

(U//FOUO) There are two types of FBI national collection requirements [redacted] A National Standing Collection Requirement is a continuing information need that will either expire or be renewed after one year. Because of their long duration, national standing collection requirements are periodically reviewed to ensure they are viable for collection. An FBI National Standing Collection Requirements Set is a document that contains consolidated collection and production requirements regarding criminal, cyber, or national security issues.

(U) National Standing Requirements Sets may be found on the [redacted] under FBI Standing Collection Requirements.

[redacted] b7E

b7E

on the

(S) 4.2.3. (U) Other Requirements

b1
b7E

b7E

4.3.1. (U) New

b6
b7C
b7E

(U//FOUO) For example,

b7E

4.3.2. (U) Detailed

(U//FOUO) All IIRs must contain information that is detailed enough to be of investigative or analytic value to the IIR consumer. Ideally, each IIR should address six major questions: who, what, when, where, how, and why. However, intelligence that does not include answers to all six questions can still be useful. For example, IIRs that contain fragmentary intelligence often serve as valuable building blocks that contribute to the FBI's, USIC's, and/or law enforcement community's understanding of a particular threat or issue. Based upon the wording of the requirement(s) to which the report responds, the level of detail required to meet the detailed threshold may vary.

(U//FOUO)

b7E

4.3.3. (U) Authoritative

b7E

(U//FOUO)

The first two are examples of sources who are sufficiently authoritative, and the third example is of a source who is not.

b7E

b7E

b7E

4.3.4. (U) Of Interest

(U) Intelligence reporting must be requirements-driven, to ensure the FBI is responsive to satisfying its own intelligence needs and those of its external customers. Information is considered "of interest," with respect to dissemination in an IIR, if it meets an intelligence requirement or addresses a new information need.

(U//FOUO)

b7D
b7E

b7E

4.3.5. (U) Respect the Rights of US Persons

(U//FOUO) In order to ensure compliance with the *Privacy Act of 1974 (5 U.S.C. §552a)* and to protect the privacy, reputation, and other interests of USPERs,

b7E

b7E

(U//FOUO) The term "United States person" or "USPER" is defined in EO 12333 and in the AGG-Dom. The definition includes an individual who is a U.S. citizen or an alien lawfully admitted for permanent residence; an unincorporated association substantially composed of individuals who are United States persons; or a corporation incorporated in the United States. EO 12333 authorizes elements of the USIC (including the intelligence elements of the FBI) to collect, retain, and disseminate information concerning USPERs. The FBI does so in accordance with the AGG-Dom and the DIOG.

(U//FOUO) The previous version of the required that

b7E

b7E

4.3.5.1. (U) Legal Authorities Governing Dissemination of USPER Information

4.3.5.1.1. (U) Executive Order 12333

(U//FOUO) According to Section 2.3 of EO 12333, the FBI may disseminate USPER information in accordance with the AGG. Section IV.B.1. of the AGG-Dom, and Section 14.3.A. of the DIOG permit the sharing of USPER information if:

- the information is publicly available;
- the USPER's consent is obtained;
- it is necessary to protect persons or property, prevent a crime or threat to national security, or to obtain information for the conduct of an authorized FBI investigation; or
- the Privacy Act permits the dissemination.

(U//FOUO) The AGG-Dom sections further state that if the dissemination is to a foreign government, USPER information may be included if the FBI has considered the reasonably expected effect of the dissemination on any identifiable USPER. The DIOG also requires that any of the above-noted disseminations be done in accordance with

b7E

(U//FOUO) For additional information, see Section 4.4.1 of the

4.3.5.1.2. (U) The Privacy Act

(U//FOUO) *The Privacy Act of 1974 (5 U.S.C. §552a)* places restrictions on the collection, maintenance, use, and dissemination by federal agencies of records containing personal information on individuals (defined as U.S. citizens and aliens lawfully admitted for permanent residency [LPR]). *The Privacy Act* prohibits federal agencies from disclosing any "record" contained in a "system of records" to any person or to another agency, except with the consent of the subject of the record or, in the absence of consent, under certain prescribed circumstances. One of these circumstances is for a "routine use" that has been published by the agency in the Federal Register. The FBI has established several routine uses that would permit disclosure, without consent, of a record about an USPER (an IIR likely would be considered a record for purposes of the Privacy Act). One of the most pertinent routine uses is as follows:

> "Personal information . . . may be disclosed as a routine use to any federal agency where the purpose in making the disclosure is compatible with the law enforcement purpose for which it was collected, e.g., to assist the recipient agency in conducting a lawful criminal or intelligence investigation, to assist the recipient agency in making a determination concerning an individual's suitability for employment and/or trustworthiness for

employment and/or trustworthiness for access clearance purposes, or to assist the recipient agency in the performance of any authorized function where access to records in this system is declared by the recipient agency to be relevant to that function." 63 Fed.Reg.8659, 8682 (February 20, 1998)

(U//FOUO) Other routine uses allow disclosure when a record, on its face or in conjunction with other information, indicates a violation or potential violation of law (whether civil or criminal), regulation, rule, order, or contract. In that event, the pertinent record may be disclosed to the appropriate entity (whether federal, state, local, joint, tribal, foreign, or international) that is charged with the responsibility of investigating, prosecuting, and/or enforcing such law, regulation, rule, order, or contract. Information identifying an USPER may also be disclosed to a legitimate agency of a foreign government, if the FBI determines that the information is: (1) relevant to that agency's responsibilities, (2) dissemination serves the best interests of the U.S. government, and (3) the purpose in making the disclosure is compatible with the purpose for which the information was collected.

(U//FOUO) The Privacy Act further requires that whenever information regarding "individuals" is disseminated outside the agency, "reasonable" care must be taken to ensure that the information is timely, complete, relevant, and accurate. It is the nature of intelligence, particularly the raw, unevaluated information contained in an IIR, that there is a trade-off between prompt dissemination and the desire to check the facts as carefully as possible. Making this trade-off requires the exercise of good judgment, taking into account all of the relevant circumstances.

(U//FOUO) It is also important to note that there are criminal penalties for agency employees who willfully disclose protected information when they know that the disclosure would otherwise be prohibited. Consequently, careful consideration should be paid to those IIRs that name USPERs, to ensure the identification meets the requirements described above.

(U//FOUO) For additional information, see [redacted] b7E

4.3.5.2. (U//FOUO) Approval for Identifying an USPER

(U//FOUO) The decision to identify an USPER within the releasable portion of an IIR is approved under the auspices of the originating field office's Special Agent in Charge (SAC).

(U//FOUO) [redacted] b7E

(U/FOUO) In summary, when determining whether to name an USPER in an IIR, reports officers should consider the following questions and take the following steps:

[redacted] b7E

(U//FOUO) For more information, see [redacted]

4.3.6. (U) Dissemination of Threat Information in an IIR

(U//FOUO) [redacted] b7E

4.3.6.1. (U) Does the Information Constitute a Threat?

(U) According to Part II.C.1 of the 02/11/2005 DOJ memorandum entitled *Field Guidance Concerning the Prosecution of Terrorism Hoaxes*, a "threat" is generally defined as a communicated intent (whether verbal, physical, or written) to inflict harm or loss on another or on another's property. Within this section of the memo, threat is defined as:

> (U) A threat is a statement expressing an intention to inflict bodily harm to someone of such a nature as could reasonably induce fear as distinguished from idle, careless talk, exaggeration, or something said in a joking manner . . . a serious expression of intent to inflict injury and not merely a vehement or emotional expression of political opinion, hyperbole, or arguments against government officials. Among other things, [one] should consider whether on their face and in the circumstances in which they were made defendant's statements were so unequivocal, unconditional, and specific as to convey to the recipient a gravity of purpose and apparent prospect of execution.

4.3.6.2. (U) Is the Information Detailed and Reliable Enough To Be Useful?

(U//FOUO) Once the information or intelligence has been deemed a threat, it must be determined whether disseminating the information makes sense.

[redacted] b7E

b7E

b7E

(U//FOUO)

b7E

b7E

(U//FOUO)

b7E

4.3.7. (U) Special Considerations for Criminal IIRs

(U//FOUO)

b7E

(U//FOUO)

b7E

4.3.8. (U) Special Considerations for Domestic Terrorism IIRs

(U//FOUO)

b7E

(U//FOUO)

(U//FOUO)

4.3.9.

b7E

(U//FOUO)

b7E

(U//FOUO) Crossover does exist between the programs. For example,

b7E

(U) Internet reporting can frequently blur the lines between open source and clandestine collection because of the disparate types of information available. These issues are addressed in detail in the following section.

4.3.10. (U) Dissemination of Open Source Information in an IIR

(U) It is not the purpose of an IIR to provide raw data obtained from open sources to the USIC and/or the U.S. law enforcement community. IIRs provide recipients with raw intelligence they would otherwise not have access to, because it has been obtained from FBI sources and/or assessments and predicated investigations. As such, the FBI does not routinely disseminate IIRs that report information that is wholly available in open sources. The FBI does, however, add publicly available information to IIRs (particularly using an FBI comment) when doing so provides context to the reporting. The DIOG defines "publicly available" information as information that:

- Has been published or broadcast for public consumption;
- Is available on request to the public;
- Is accessible online or otherwise to the public;
- Is available to the public by subscription or purchase;
- Could lawfully be seen or heard by any casual observer;
- Is made available at a meeting open to the public;
- Is obtained by visiting any place or attending any event that is open to the public; or

- Could be seen or heard by any casual observer, not involving unconsented intrusion into private places.

(U) As a general rule, if the information could be obtained through an internet search engine, it should not be reported in an IIR. The following points provide general guidance on common open source reporting scenarios.

4.3.10.1. (U) Some reporting is publicly available, some is not

(U//FOUO) If some of the reporting is publicly available, but some is not, the IIR author should determine whether the nonpublic information is important, i.e., whether it is considered intelligence on its own or enhances the open source reporting in a meaningful way.

b7E

4.3.10.2. (U) Information was posted online, but is no longer available

(U//FOUO)

b7E

(U//FOUO) Some websites archive information for limited or unknown periods of time. Since the information is not available after the limited time period, the information is reportable, provided it also meets (see Section 4.3.10.6.).

4.3.10.2.1. (U) Virtual Worlds

(U//FOUO) Authorized investigations may uncover the simulation of real-world interaction and private messaging capabilities featured in virtual world (i.e., online gaming) communities, such as These interactions should be treated as if the occurred in communities in the physical world.

b7E

4.3.10.3. (U) Information is currently publicly available, but the FO initially received it from an FBI source

(U) If the information is currently publicly available, but the FO initially received the information from an FBI source, it is possible open source reporting is corroborating source reporting, but it is also possible the source provided the information to the FBI by searching the Internet. Regardless of where the information originated, it is not reportable in an IIR, if it is currently publicly available.

4.3.10.4. (U)

b7E

4.3.10.5. (U)

4.3.10.6. (U) Information available online, but registration and/or a password is required

b7E

(S) [redacted] b1 b7E

4.3.10.7. (U) Threat or other information of interest is publicly available, but it is written in a foreign language

(U//FOUO) If a threat or other information of interest is publicly available, but it is written in a foreign language, such information is not reportable in an IIR. [redacted] b7E

4.3.11. (U) Dissemination of Grand Jury Information in an IIR

(U//FOUO) Disclosure of federal grand jury material is restricted under *Federal Rules of Criminal Procedure, Rule 6(e)* and implementing guidelines promulgated by the DOJ. Coordination with an attorney for the government is required to determine whether information is considered grand jury material, and if so, whether disclosure is permissible. More information about grand jury material may be found in the [redacted] b7E

4.3.11.1. (U) Disclosure without Restrictions

(U//FOUO) If the attorney for the government has authorized disclosure without further restrictions, it must be clearly annotated in the administrative note/tickler section of the IIR that grand jury material was utilized in the IIR, and that such use requires notification to the court that empanelled the grand jury, prior to any further dissemination. Approval of the attorney for the government for the disclosure of grand jury material must also be documented in the administrative note/tickler section of the IIR.

4.3.11.2. (U) Disclosure with Restrictions

(U//FOUO) If the attorney for the government has authorized disclosure with further restrictions, the *Grand Jury Guidelines* authorize the attorney for the government to impose additional restrictions on the use or disclosure of grand jury information, as is deemed necessary. Any such restrictions must be communicated by the attorney in writing, and any such written documentation should be retained in the case file.

(U//FOUO) IIRs containing grand jury material, that the authorizing attorney for the government has imposed use or disclosure restrictions upon, must provide an alert to IIR recipients of these restrictions in the body of the IIR. Legal review of an IIR with grand jury material includes verifying that these use or disclosure restrictions are clearly articulated in the body of the IIR.

4.3.11.3. (U) [redacted]

[redacted] b7E

[redacted]

4.3.11.4. (U) Information is Determined Not to Be 6(e) Material

[redacted] b7E

4.3.12. (U) Dissemination of Information Derived from Proffer Agreements

(U) Reporting derived from proffer agreements may be reportable in an IIR, as it is not publicly available. [redacted] The IIR should include the following context statement: b7E

[redacted]

4.4. (U) FBI Intelligence Dissemination Procedures

(U) Since IIR consumers use FBI intelligence in different ways, the FBI must tailor the dissemination of reports so each customer receives a product that meets its specific needs. It is also important to remain mindful of legal and operational concerns that arise when disseminating certain information to certain entities.

(U//FOUO) For example, EO 12333 (Section 2.3) prohibits the FBI from sharing USPER information with the USIC, when the information is purely domestic in nature. An exception to this legal limitation to sharing information may be found in Section 2.3(d), which explains that the FBI is authorized to disseminate information concerning USPERs when that information is "...needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations." For additional information regarding USPERs, including who/what is considered an USPER, refer to Section 4.6.2. of this PG.

(U//FOUO) The FBI routinely disseminates national security intelligence to the USIC. However, the FBI is authorized to disseminate information collected as part of a national security investigation to federal authorities outside the USIC as well, provided the information relates to a

crime or other violation of law or regulation which falls within the recipient's investigative jurisdiction, or the information otherwise relates to the recipient's authorized responsibilities.

4.4.1. (U) Dissemination to State, Local, and Tribal Law Enforcement Entities

(U//FOUO) Based on DIOG, Section 14.3, the FBI is authorized to disseminate information and intelligence produced through activities authorized under the AGG-Dom [redacted]

[redacted] DIOG, Section 12.4, also permits sharing of this unclassified information with other federal, state, local, and tribal law enforcement agencies through other, more direct means, to be documented in a [redacted] b7E

(U//FOUO) The FBI is also authorized to disseminate information obtained during the course of a national security investigation to state and local law enforcement officials by IIR when:

- The information relates to a crime or other violation of law or regulation which falls within the recipient's jurisdiction, and the dissemination is consistent with national security; or
- The dissemination is for the purpose of preventing or responding to a threat to national security, or to public safety, including a threat to the life, health, or safety of any individual or community.

4.4.2. (U) Dissemination of Teletype Memoranda

(U) The FBI uses teletype memoranda (TM) to share purely operational information with other United States Government (USG) agencies, or in conjunction with an IIR to share sensitive identifier information [redacted] b7E

[redacted] Identifier information may be added into an IIR, if approved by the FBIHQ operational divisions and the DI. If necessary, the PLA list may be limited (a limited dissemination IIR) in order to protect this sensitive information.

(U) Though TMs may be used to share operational information, the responsibility for sharing this information lies with FBIHQ operational divisions, not the intelligence components of the DI or FIGs.

(U//FOUO) [redacted] b7E

(U) TMs may also be used to respond to requests for information (RFI). TMs typically carry a "lead purposes only" caveat to ensure that readers know the information is intelligence, and should not be considered as evidence for the purpose of legal proceedings.

(U) TMs are not the appropriate mechanism for providing intelligence that meets the threshold for dissemination in an IIR to a limited number of recipients. In instances where limited

recipients are preferable due to the sensitive nature of the information, a limited dissemination IIR is more appropriate.

(U) Limited distribution IIRs may not be used in place of TMs, and vice versa. A limited distribution IIR is held to the same dissemination thresholds as a standard dissemination IIR, and therefore cannot contain only operational or identifier information, as a TM can. Nor can limited distribution IIRs be released "in conjunction" with standard dissemination IIRs, where the limited dissemination report repeats the standard report's intelligence with additional identifier information. Agencies that receive both a limited distribution IIR and [redacted] standard distribution IIR based on the same source information may believe they have reporting from two separate sources. b7E

4.4.3. (U) Dissemination of Tearlines

(U//FOUO) [redacted] b7E

This allows wider dissemination of the substantive intelligence information to authorized customers. Sanitized intelligence pertaining especially (but not exclusively) to the following topics should be considered for dissemination via tearline:

- Imminent threats to state, tribal, or local personnel or jurisdictions;
- Potential targets of terrorism within foreign, state, tribal, or local jurisdictions;
- Activities, financing, and capabilities of terrorist or criminal organizations; and
- Collaboration among terrorist or criminal organizations.

(U//FOUO) [redacted] However, there are inherent (classified) sensitivities associated with the dissemination of foreign intelligence and counterintelligence to foreign governments. For more information regarding tearlines in general, please refer to the ODNI's tearline format specification implementation guide entitled [redacted] as well as the [redacted] b7E

4.4.3.1. (U) Designated Intelligence Disclosure Official Procedures

(U//FOUO) Only a designated intelligence disclosure official (DIDO) can approve the dissemination of classified FBI intelligence to a foreign government.

(U//FOUO) DIDO authority has been delegated to individuals, based on their position, who are trained and required to ensure that any dissemination to a foreign government is in accordance with relevant Presidential orders, DCIDs, DNIDs, and FBI policy [redacted] b7E

(S)

b1
b7E

4.4.4. (U) "No Double Standard" Policy

b7E

4.5. (U) IIRs and the Discovery Process

(U//FOUO) FBI IIRs are secondary documents. They derive all of their content from primary source documentation, such as the and are therefore not usually considered discoverable, if they contain only information also found in the source documentation. IIR authors should minimize the potential for discovery, by ensuring the replication of statements in the IIRs of potential defendants or witnesses from source documents are accurate, and summarized or paraphrased, rather than quoted verbatim.

b7E

(U//FOUO) In doing so, IIR authors must remain cognizant of the fact that potential problems can be inadvertently created if the paraphrasing creates inconsistencies between the IIR and the source documents. Fidelity to source documentation is paramount. In addition, IIR authors should be wary of including analytical judgments in FBI comments. Not only is an IIR not the vehicle for analysis, comments that tend to either inculpate (assign blame) or exculpate (exonerate) subjects, that later become defendants, may be discoverable.

(U) In addressing these matters, IIR authors should not compromise or modify the IIR criteria for timeliness, procedures, and/or content that serve the FBI's critical intelligence reporting mission out of fear of discovery in a subsequent criminal trial. For additional guidance regarding IIRs and the discovery process, please refer to the

b7E

4.6. (U) Writing an IIR: Tradecraft and Style

(U) When writing an IIR, the ultimate goal is to relay all relevant information as concisely as possible while using good grammar and adhering to formatting guidelines, to ensure the messaging system will transmit the data properly. The quality of IIRs submitted to a CRO or FBIHQ approver directly impacts whether they are disseminated in a timely manner. IIR quality also influences determinations of the authoring entity's intelligence performance in preparing IIRs. All IIRs should be formatted using the guidance set forth in this PG and in the [redacted] Failure to adhere to the guidance will result in delay or revision, and in some cases, non-dissemination of IIRs. IIRs should be carefully checked for spelling and grammar. Poorly phrased IIR text reaches thousands of individuals within the USG and reflects negatively on the FBI's reputation. b7E

[redacted] b7E

4.6.2. (U) [redacted]

[redacted] b7E

[3] (U) In applying the second bullet point, "if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining whether it is substantially composed of USPERs. If, however, the United States-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States shall be considered in determining whether it is

[redacted]

(U) Withholding the identity of an USPER in an IIR does not preclude the IIR author from including contextual information about the individual or organization in an FBI comment. For example, criminal history that is relevant to the information presented in the IIR may be included. Authors may also include an FBI comment to assist recipient agencies with analysis, even though the individual is not identified in the text of the IIR. For example [redacted] An agency may be able to use such information to articulate a need to know the identity of the USPER. However, too much information may permit the discovery of the USPER's identity. In such a case, the USPER identification procedures outlined in Section 4.3.5.2. of this PG must be followed, or some of the potentially identifying information should be omitted. b7E

(U//FOUO) Additional guidance regarding the identification of USPERs in IIRs is as follows:

- [redacted] b7E

[redacted]

substantially composed of Unites States persons. A classified directive provides further guidance concerning the determination of United States person status."

b7E

(U) For additional information regarding the standards and approval procedures for naming USPERs in IIRs, refer to Section 4.3.5. of this PG.

4.6.2.1. (U) U.S. Elected Officials

b7E

4.6.3. (U) Operational Information vs. Intelligence Information

usually contain both operational and intelligence information. While it is important to share intelligence with the FBI's partners, it is also necessary to avoid providing operational information that could unnecessarily jeopardize FBI sources, methods, or investigations. Therefore, it is necessary to distinguish between operational and intelligence information when drafting an IIR.

(U//FOUO) Operational information concerns the actual investigation or operation of sources and methods, and may include details that reveal how the FBI obtained information, how it may be able to obtain information, or explain how it plans to obtain information. General examples of operational information include how and when a source was contacted by a case/handling SA, methods and circumstances surrounding a source's meeting with an SA, the source's access to the information (how, when, where it was collected), information regarding relationships with the sourc

b7E

(U//FOUO) Examples of purely operational information that should not be in an IIR include the following:

(U//FOUO) Intelligence information is significant information extracted from data collected in response to consumer requirements and from which conclusions can be drawn to make better-informed decisions and advance operations. It is distinguished from operational information, since it does not include the particulars of *how* information was collected, such as source details or meeting circumstances.

b7E

(U//FOUO) Some identifier information can be both operational information and intelligence information, depending on the circumstances. This type of information should be considered for dissemination in IIRs if it would add intelligence value. If it is too sensitive, it may also be

disseminated using a limited distribution IIR or a TM accompanying a regular distribution IIR. However, identifier information that is purely operational in nature should not, as a general rule, be shared using either an IIR or a TM. Refer to Section 4.4.2. of this PG for additional information regarding the use of TMs.

4.6.4. (U) Partial Names

(U) When a partial name is provided, IIR authors have several options. For example, b7E

(U)

(U//FOUO) When provided with a partial name, IIR authors should research the name in relevant databases to determine possible identities for the individual, thereby increasing the actionable and analytic value of the raw intelligence. Using the example above, b7E

b7E

b7E

4.6.5. (U) Prohibited Characters

(U) Although some formatting requirements seem counterintuitive, adhering to them helps ensure the successful electronic transmission of IIRs [redacted] IIR authors must adhere to the basic rules when drafting IIRs, which are detailed below. b7E

[redacted] b7E

[redacted] b7E

4.6.6. (U) Source Document

(U) All IIRs must accurately reflect the information contained in the primary source document. As a quality assurance measure, [redacted] b7E

(U//FOUO) For the purposes of IIR production, a primary source document is defined as the original document in which the information officially entered the FBI. Examples include [redacted] police reports, [redacted] An electronic communication (EC) is only acceptable if it is the first written record of the information, as is often the case in counterintelligence investigations. However, ECs that reiterate, analyze, or otherwise expound upon [redacted] and other primary source documents, are not considered primary source documents. b7E

(U//FOUO) [redacted] b7E

4.6.7. (U) Style

(U) IIRs must conform to unique and rigid stylistic elements, in order to both maintain a strict professional writing standard and transmit accurately through FBI and USIC messaging systems. These elements are as follows:

- [redacted] in accordance with [redacted] b7E

[redacted] b7E

b7E

(U) IIRs authors should defer to the [redacted] for style issues that are not addressed in this PG.

b7E

4.6.8. (U) Surnames

[redacted]

b7E

b7E

[redacted]

(U) If a name appears only in a tearline and therefore is not indexed, insert an indexing comment (see Section 4.7.16.1.1.1. for further information).

4.6.9. (U) Tense.

([redacted] This is because the information IIRs present is only current as of the day the source acquired the information (i.e., the IIR's timeliness). By the time the information is disseminated in an IIR, the situation may have changed [redacted]

b7E

[redacted]

(U) For example, [redacted]

[redacted]

b7E

4.6.10. (U) Voice

b7E

(U [redacted] Active voice means that a sentence is structured in the following basic format: subject – verb – object. Passive voice, which is to be avoided, is formed as object – verb – subject. Passive voice may be identified by the fact that it is always

b7E

used to identify the source, when combined with the source byline and/or source context statement.

(U//FOUO)

b7E

4.6.11.1. (U) Single Source vs. Singular Source

b7E

(U//FOUO)

b7E

(U)

4.7. (U) Writing an IIR: How to Complete Each Component

(U) Each IIR consists of multiple sections, some of which are automatically completed by FIDS, and some of which require input from IIR authors.

4.7.1. (U) Distribution List

(U) An IIR's distribution list, also known as the PLA list, determines which agencies and agency

- b7E

b7E

(U//FOUO) The DI maintains standardized PLA lists for each of the FBI's investigative programs in FIDS, where they may be located for reference. The DI maintains standard PLA lists for counterintelligence, criminal, cyber, domestic terrorism (DT), foreign intelligence, international terrorism, and WMD reporting. However, IIR approvers should carefully consider each IIR's recipient list and determine whether additional recipients are warranted. For example,

(U//FOUO) Conversely, IIRs that identify USPERs by name must ensure the PLA has been tailored to those non-USIC agencies, sub-agencies or entities that have as one of their authorized functions the subject matter of the IIR. In these cases, PLAs may be removed from the standard lists, in order to conform to this requirement.

b7E

4.7.2.3. (U) Routine

[redacted]

4.7.3. (U) Classification

(U) [redacted]

[redacted] b7E

(U//FOUO) [redacted]

[redacted]

(U//FOUO) [redacted]

[redacted]

4.7.3.1. (U) Classification Markings

(U) [redacted]

4.7.3.1.1. (U) Confidential (C)

(U) [redacted]

[redacted]

4.7.3.1.2. (U) Secret (S)

(U)

4.7.3.2. (U) Classification Disputes

(U//FOUO)

(U//FOUO)

b7E

(U//FOUO)

(U//FOUO)

(U//FOUO)

b7E

4.7.3.3. (U) Declassification Markings

(U//FOUO) Classified IIRs are ordinarily assigned a declassification date 25 years after the day the IIR is released. Automatic declassification (denoted as "25 years" in FIDS) is appropriate for all IIRs b7E

(U//FOUO)

(U//FOUO b7E

(CAPCO) declared the declassification value within the banner line (overall classification) obsolete, meaning that the Manual Review (MR) control, formerly used in conjunction with also became obsolete. Banner line/overall classifications appear in three places within an IIR: (1) immediately following the first BT (begin transmission), (2) immediately preceding the FBI banner, and (3) immediately following the DISSEM prosign.

(U) The following are incorrect and correct examples of proper banner classifications for an IIR: b7E

4.7.3.4. (U) Dissemination Controls

(U) FBI-produced information (which is distinct from information produced by another agency and incorporated into an FBI IIR) can only carry the following handling caveats:

(U) For unclassified information:

(U) For classified information:

b7E

4.7.3.4.1. (U) For Official Use Only (FOUO)

(U//FOUO)

b7E

4.7.3.4.2. (U) Law Enforcement Sensitive (LES)

(U)

4.7.3.4.3. (U) Originator Controlled (ORCON)

(U//FOUO)

(U//FOUO

(U//FOUO) In addition, the ORCON control marking may not be used when access to the intelligence would reasonably be protected by its classification markings (e.g., CONFIDENTIAL or SECRET). For additional ORCON guidance, please refer to the [redacted] b7E
[redacted] mentioned above.

4.7.3.4.4. (U) Not Releasable to Foreign Nationals (NOFORN)

[redacted] b7E

4.7.3.4.5. (U) Releasable to (REL TO)

[redacted] b7E

b7E

4.7.3.4.6. (U) Foreign Intelligence Surveillance Act (FISA) - Derived

[redacted]

b7E

4.7.4. (U) Pass Line

b7E

b7E

[5] (U//FOUO) As of this PG's publication date, there were no Legats that required a pass line. Information regarding pass lines is being provided in this PG in the event a new LEGAT office is opened that does not immediately have teletype capability.

4.7.5. (U) Serial Number

b7E

4.7.6. (U) Country Line

(U) The country line designates the country(ies) to which the substance of the IIR refers, not necessarily the originating country or every country mentioned. The country appearing first should be most relevant, followed by any other countries in descending order of relevance/importance to the report. The United States *does not* need to be mentioned in every report's country line, nor does it need to be mentioned first in country lines that do feature it. For the purposes of the country line, the same rule applies to the United States as to any other nation.

(U) Each listing must include the full country name, followed by the authorized two-letter code (digraph) in parentheses. See Appendix A for a list of country codes. An example of a country line field is:

COUNTRY: (U) CYPRUS (CY); UNITED STATES (US); SYRIA (SY).

4.7.7. (U) IPSP Field

(U//FOUO) The Intelligence Priority for Strategic Planning (IPSP) field lists all relevant intelligence functional codes (IFC). The USIC Automated Data Handling System uses these codes to route IIRs to appropriate USIC and federal law enforcement customers.

(U) An IFC should be listed for each collection requirement addressed in the IIR. The most important/applicable IFC should always be listed first, followed by additional applicable IFCs in descending order of importance. An example of an IPSP field is:

IPSP: (U) IFC2210; IFC2211.

4.7.8. (U) Subject Line

(U) The subject (SUBJ) line is a brief summary of the IIR. Subject lines should be detailed, yet succinct, and should accurately reflect the contents of the entire IIR. The subject line should

b7E

enable consumers to quickly determine whether the IIR is relevant to their respective area of interest. For example:

b7E

b7E

(U) Using words such as "possible," "potential," and "alleged" is permissible in the subject line if the source used those exact words or similar words. It is also permissible to use such language if the FBI comments or the source context statement indicates doubt concerning whether the reported activity is likely to occur (e.g., doubts are expressed about the accuracy of the information and/or credibility of the source in the IIR), because although the text of the IIR reflects what the source reported, the subject reflects the content of the entire IIR.

b7E

(U) The following additional guidance also applies to the composition of subject lines:

- The subject should be written as a noun phrase that completes the following sentence: "This report is about the....";
- The subject line should not contain a verb; i.e., it should not be a complete sentence;

  Example 1

  Example 2

- Sensational language should not be used. IIR subject lines should not read like newspaper headlines;
- The subject information must not exceed four lines;
- The classification appears after the subject;
- A period should not be placed at the end of the subject line;
- Although a single subject is preferred, split subjects are permissible. Split subjects use the following format, but must still fall within the four-line limit:

b7E

b7E

[redacted]

- Subject lines should not be duplicated. If the report is an update, the new subject line should say "UPDATE TO" plus the subject of the original report (see Section 4.8.3.).

4.7.9. (U) Warning Statement

(U) FIDS generates a standard warning for each IIR that includes the overall classification and handling caveats. For example:

[redacted]

b7E

(U//FOUO[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[7] A more detailed classified caveat may be included in classified documents.

ATTORNEY GENERAL. CONSULT WITH OGC NSLB AT FBIHQ PRIOR TO ANY FOREIGN DISSEMINATION.

(U//FOUO) Also refer to the foreign dissemination section in the [redacted] if disseminating to a foreign government. There are additional considerations that apply when disseminating [redacted]

(U//FOUO) [redacted]

b7E

4.7.10. (U) DOI

(U//FOUO) The DOI is in YYYYMMDD (year [Y], month [M], and day [D]) format. It is the date of occurrence of the information contained in the IIR. If there is no action *per se*, it is the date on which the source last had access to the information reported. When more than one DOI is applicable for an IIR, the most recent date of information is referenced in the DOI field.

(U//FOUO) The DOI is never later than the acquisition date (ACQ) since the ACQ reflects the date the FBI received the information.

(U//FOUO) If the month or day is not available or is unknown, enter "00." For example [redacted] If a generalized date is used in the DOI entry, provide the actual date and explain the reason for the ambiguity in the administrative note/tickler of the IIR—specifically, in the fourth

b7E

[redacted] An example of a [redacted] follows:

[redacted] b7E

(S) [redacted] b1 b7E

(U//FOUO) There are no limits on the number of requirements that may be cited in an IIR, however, cite only those requirements sets that the IIR directly addresses. FBI national collection requirements, NHCDs, and intelligence requirements issued by OGAs may also be cited, if appropriate or applicable.

(U//FOUO) Requirements sets should be listed from most specific to most general (that is, ad hoc sets first, followed by standing sets, followed by NHCDs), and within this ranking, they should be further grouped by degree of relevance, with the most relevant sets listed first, as listed

(S) [redacted]

- (U) FBI National Standing and Ad-Hoc Collection Requirements Sets: FBI requirements sets should be cited down to the most specific level possible, also known as the "essential element(s) of information," [redacted] The overall set serial should not be cited alone. The following two examples below represent a correct and incorrect requirements set citation: b7E

(S) [redacted]

- (U) Requirements Sets Issued by Other Agencies: IIR drafters should follow any instructions for citation listed in the agency's requirements set, if known. If no instructions are included, only the serial number of the set should be cited.
- (U) Local and State Requirements: IIRs are intelligence products issued centrally by the FBI, not by individual field offices. As such, local and state requirements are not suitable collection requirements for IIRs, and should not be cited in them.

4.7.12. (U) Source Byline

(U//FOUO) The source byline provides generalized, non-specific information about an IIR source's reliability and access. The "source" of an IIR is defined as the individual (e.g., HUMINT) or technical system [redacted] that brought the information to the attention of the FBI. For example [redacted] b7E

[redacted] b7E

(U) A source's access statement is determined by the access the source has to the information reported in *the particular IIR*. Access statements are defined as follows:

[redacted]

b7E

(U) A sample source byline is as follows:

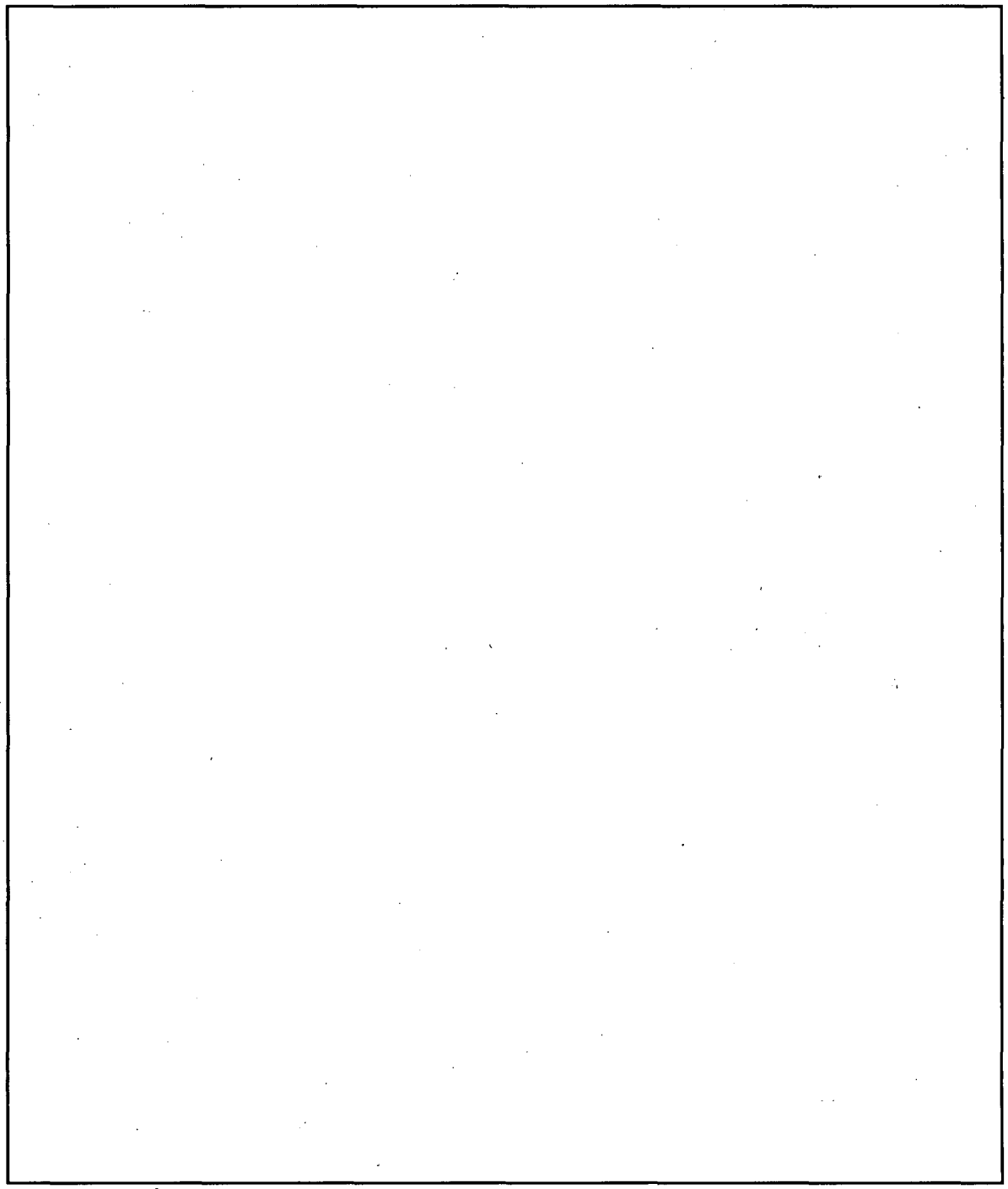
b7E

(U) If a report contains information from more than one source, the format is as follows:

b7E

b7E

b7E



b7E

b7E

4.7.12.1.15. (U) A Bank Secrecy Act (BSA)

(U) BSA, as administered by the Financial Crimes Enforcement Network (FinCEN)

b7E

SOURCE: (U) A BANK SECRECY ACT

[redacted] b7E

[redacted] b7E

[redacted] b7E

(U) Paragraphs must be grouped by source. For example, [redacted]

4.7.13. (U) Context Statement

(U//FOUO) A context statement is an optional field that describes, in greater detail than the source byline, the circumstances under which the source acquired the intelligence contained in the report. While the nature of the source's access is addressed in the general source description, the context statement provides an expanded but succinct statement describing how the source obtained the information. To the extent possible, it should also address the source's reporting history or other pertinent information regarding source credibility in a discrete statement. For example, [redacted]

(U//FOUO) [redacted] b7E

(U//FOUO) Context statements must be coordinated with the appropriate case/handling agent.

(U) In some instances, the source byline can stand alone and no context statement is needed. In these instances, the IIR author will make no entry in the source context statement field, and the completed IIR in FIDS will not reflect the context statement field. For an IIR that contains a tearline, the tearline context statement field requires an entry of the word "NONE," if no context statement will be used.

(U//FOUO) To the extent that protection of sources and methods allows, a succinct, *generalized* statement may be included regarding the source's access, relevant reporting record, possible motivation, and any additional information that would enable recipients to more fully assess the

credibility of the information. [redacted] b7E

[redacted] refer to Section 4.7.21.4.

4.7.13.1. (U) Sample Source Context Statements

(U//FOUO) The following represents a sampling of context statements for use. This list is not all-inclusive, and appropriate wording will vary based on the circumstances surrounding individual source acquisition:

[redacted] b7E

b7E

4.7.14. (U) Text

(U) The text portion of the IIR relays the information reported by the source and should be written in the "bottom line up front" or "inverted pyramid" style, which means the most important information should be relayed first. The text portion of the IIR is divided into two sections: the executive summary, and the body text. The first paragraph is always the executive summary, which cannot exceed five lines and subsequent paragraphs comprise the body text. Each paragraph is numbered.

4.7.14.1. (U) Executive Summary

(U) The executive summary stands alone, without reference to the remainder of the text, and must accurately summarize the content of the entire IIR. Since the executive summary provides a synopsis of the body text (which begins with the second paragraph), all of the information contained in the executive summary must be expressed somewhere in the remainder of the text.

(U) If the length of the IIR is fewer than the five lines allotted for the executive summary, then the executive summary serves as the entire text. The executive summary should not be repeated as the second paragraph. It should also not be repeated in any tearlines contained in the report.

(U) It is permissible to use words such as "possible," "potential," and "alleged" in the executive summary, if an FBI comment or the source context statement indicate the reported activity is unlikely to occur (e.g., the FBI expresses doubts about the accuracy of the information and/or credibility of the source in the IIR). The reason for this is that although the text of the IIR reflects only what the source reported, the executive summary provides a synopsis of the entire IIR. However, actual information from the comments section (or any in-text comments) may not be included in the executive summary.

4.7.14.1.1. (U) Sample Executive Summaries

(U) The following three examples represent poor, weak, and good examples of an executive summary:

b7E

4.7.14.2. (U) Body Text

(U) Any text paragraphs following the executive summary comprise the body text. The body text describes, in greater detail, the events or information recounted in the executive summary. The body text should be written in narrative format when possible, however, in some situations, lists may be more appropriate (e.g., the results of a search warrant that yielded a great deal of items with intelligence value). The body text should *always* be written in complete sentences, using professional-level grammar, syntax, and vocabulary. IIR authors should avoid both short, choppy sentences, as well as run-on sentences. The body text of an IIR is highly formatted, with strict rules concerning style and grammar, that may not always agree with other types of grammatical styles of English. The divergences of IIR text styling from other forms of professional writing are explained at length in Section 4.6.

(U) The body text of an IIR is written from the standpoint of the source reporting the information. As mentioned in Section 4.6.11. of this PG, the source should never be identified, either by name, symbol, or type, in the text of an IIR, nor should the source be mentioned in the third person (e.g., "Source said..."). The body text should be written as if the source were simply providing the intelligence directly to the community, with all references to the source omitted. Neither the source's opinions nor any other entity's opinions (including the FBI's) may be placed into the body text. Only information of a strictly factual nature may be presented in the body text. Any opinions or analytical context must be placed either in the Comments section or in an in-text comment.

(U) The body text should be written in the "bottom line up front" (BLUF), "bottom line on top" (BLOT), or "inverted pyramid" style, where the most important information is provided first, followed by information of lesser or secondary importance. In some situations, BLUF style may not be appropriate; for example, a series of events may occur in which chronology is important for comprehension. In these situations, reverse chronology (most recent information first) is

preferred to standard chronological order, if possible. Standard chronology may be appropriate for situations that involve the explanation of ordered systems, such as a cyber fraud scheme.

(U)

b7E

b7E

(U) As a general rule, IIR authors should employ more stringent source protection methodology in a tearline. Generic terms can be used instead of specific intelligence sources, if attribution is necessary

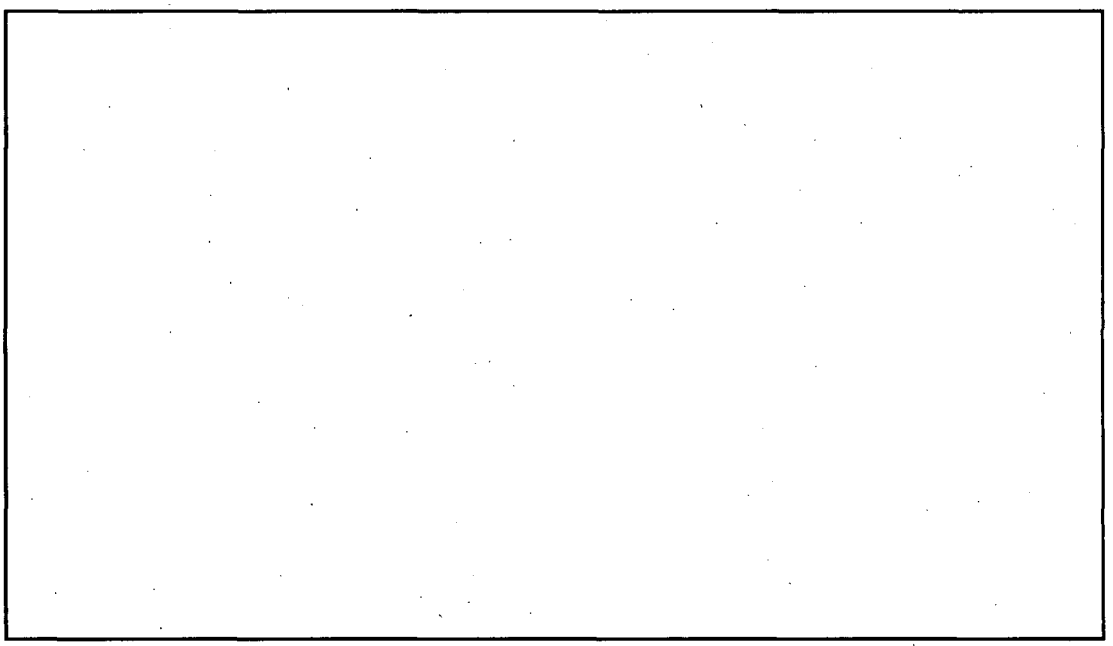
b7E

(U) There is no limit to the number of tearlines that may appear in the text portion of the IIR, however, to prevent confusion, it is recommended that releasable text be grouped together. The tearline portion carries lower classification/controls than does the original text. FIDS automatically provides instruction on how to disseminate the intelligence (in the warning statement) and, if the tearline contains FISA information, provides the tearline FISA warning statement.

4.7.15.1. (U) Sample Unclassified Tearline

(U) The following is a sample of an unclassified tearline:

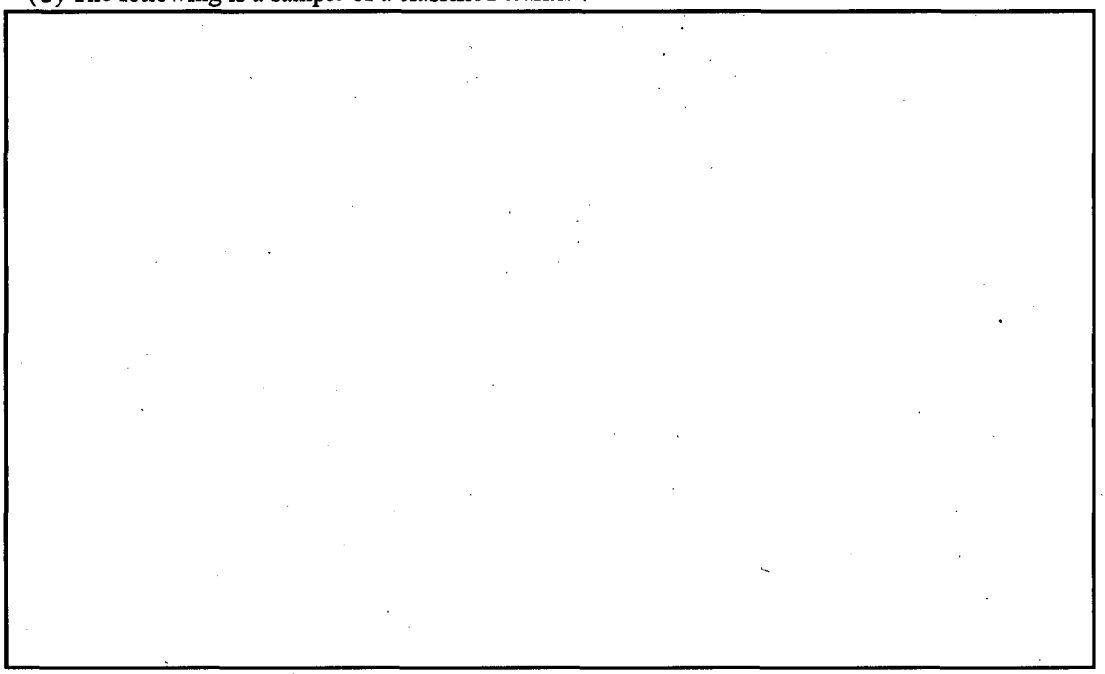
b7E

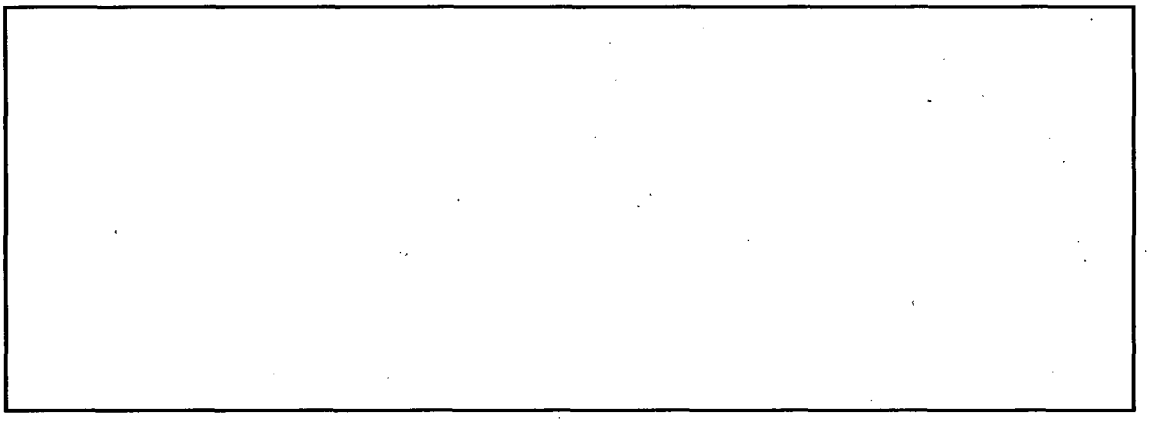


b7E

4.7.15.2. (U) Sample Classified Tearline

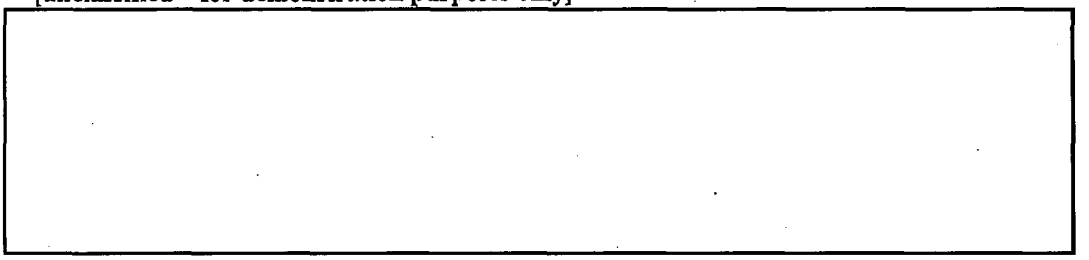
(U) The following is a sample of a classified tearline:





b7E

[unclassified – for demonstration purposes only]

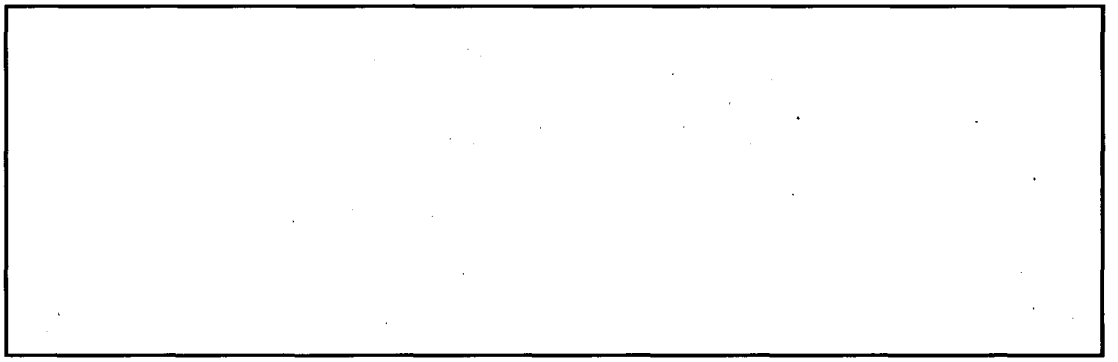


b7E

4.7.16. (U) Comments

(U) Comments add context to an IIR by providing background information, perspective, source opinions, or organizational opinions. They are also used to relay caveats and handling instructions for certain reports. Comments that are irrelevant to the report, source-revealing, or are not authoritative should be excluded from an IIR. Comments should never include source information that has not been previously reported. They should never offer critiques or a discussion of U.S. policy, or recommend changes in U.S. policy.

(U) Comments within the text of an IIR or in a tearline are always enclosed in parentheses, whether the comment is inserted into an existing paragraph or is a free-standing paragraph of its own.



b7E

(U) If the source of the IIR is a contact, a collaborative source, an established source, or a walk-in, call-in, or write-in, include a comment to advise recipients whether the source is available for re-contact. IIRs based on information derived from a technical source or the Bank Secrecy Act should always include a comment that the source is not available for re-contact.

(U) If the IIR responds to an evaluation, include a comment to cite the evaluation.

(U) If the IIR identifies individuals whose surnames were not enclosed in double parentheses due to the location in a tearline, include a comment for indexing purposes.

b7E

(U) When issuing an IIR recall (see Section 4.8.), insert the following comment after the executive summary:

(U) When issuing an IIR revision (see Section 4.8.), insert the following comment:

(U) For further information on recalls and revisions, please see Section 4.8.2. of this PG.

4.7.16.1.1.2. (U) Citation FBI Comments

(U) Citation comments add background to reporting, provide additional context, and can indicate a continued line of reporting. Citation comments may be written in standard or abbreviated format, depending on the usage. Ensure that any IIRs cited are germane to the current report.

(U//FOUO) Only documents disseminated to the USIC or law enforcement community may be cited, and not all such documents are appropriate for citation. For example, FBI operational cables, as well as, are intended only for a narrow audience, and may not be cited without permission from the originator. An ORCON document may only be cited if the PLA list on the new report is the same as the one found on the original document.

b7E

(U) Standard format citation comments should be used by default. Standard format citations should be placed either in the comments section, or at the conclusion of a tearline. Abbreviated format citations can be used in-text, or in a series of more than three citations in the comments section. Always repeat an in-text abbreviated citation in the standard format in the comments section.

(U) In a citation comment, you may wish to include an introductory sentence or two, before the actual citation itself. This will give readers a better idea of how relevant the cited reporting is to their needs. These sentences should briefly summarize the relevant reporting from the cited document.

(U) Standard Format: Standard format citation comments include the serial number, date/time group (DTG), subject line, and source byline of the report being cited. Three different examples follow. b7E

[redacted]

(U) Abbreviated Format: Abbreviated format citation comments include only the serial number and DTG of the report being cited a shown in the following two examples:

[redacted]

[redacted] b7E

b7E

(U) These comments, and any derivations thereof, are no longer used in IIRs.

b7E

4.7.16.2. (U) Order of Comments

(U) IIR authors should list comments in the comments section in order of importance. Comments that elaborate on information in the text should be listed first. Administrative comments (such as name indexing comments) should be last. There is no need to group comments together by type. For instance, if an FBI comment is necessary and a source comment elaborates on the FBI comment, the order of the comments could be (1) FBI comment, (2) source comment, and (3) FBI comment with administrative information.

4.7.16.3. (U) Placing Comments in the Text of the IIR

(U) Comments are generally placed in the comments section of the report because in-text comments interrupt the narrative flow of the source's reporting. However, there are instances when including them in the text is appropriate. Comments that elaborate on information provided in the text may be included directly after the sentence in the text, or at the end of the paragraph that contains the information to which the comment pertains. Comments should be as brief as possible, and set off by single parentheses (regardless of whether they are included within a paragraph or are their own paragraph). For example:

b7E

4.7.17. (U) INSTR

b7E.

4.7.18. (U) PREP

(U) This field notifies recipients who prepared the IIR for dissemination and provides a point of contact for questions. FIDS prints a standard contact paragraph here.

4.7.19. (U) ACQ

(U//FOUO) The date of acquisition (ACQ) is in YYYYMMDD format, and reflects the date the FBI received the intelligence from a human or technical source, or from investigative or collection activity. The ACQ is *not* the date of transcription, the date of translation, or the date a FIG or IIR drafter received the information. Since the ACQ reflects the date the information first entered the FBI, it is never earlier than the date of information (for more information on the DOI, refer to Section 4.7.10. of this PG).

(U) IIR authors must provide the exact date (by day, month, and year) that the FBI acquired the intelligence. For example, if a source reported intelligence to the FBI on 12/15/2007, the ACQ would be as follows:

b7E

4.7.20. (U) DISSEM

(U//FOUO) The dissemination field (DISSEM) identifies entities that were provided with a copy of the draft IIR prior to approval and dissemination. Since unapproved IIRs should not be distributed, the standard entry for this field is "NONE." For example:

DISSEM: (U) FIELD: NONE.

4.7.21. (U) Administrative Note/Tickler Count

(U//FOUO) The administrative note/tickler count (commonly referred to as the "admin tickler") provides additional information regarding the IIR to individuals within the FBI. Examples of information included in the admin tickler include: who approved the IIR, case number citations, and elaboration on the source using [redacted] The admin tickler is for internal use only. It is not disseminated to addressees on the IIR distribution list, and should never be provided to anyone via e-mail or hardcopy, unless the individual has a need to know the information *and* the individual could access the admin tickler in ACS.

b7E

(U//FOUO) The admin tickler should be portion marked as allowed by the FIDS program. The classification of the information in the admin tickler cannot exceed the overall classification of the IIR, as they are considered one document. The disseminated portion of the document cannot bear an overall classification higher than that of the information itself. For this reason as well, the tickler cannot contain information at a higher classification than that which appears in the disseminated portion.

(U) The admin tickler contains the following bolded warning statement:

ADMINISTRATIVE NOTE/TICKLER COUNT:

- **PLEASE REMOVE THE ADMINISTRATIVE (TICKLER) PAGE OF THIS COMMUNICATION WHEN SHARING THE CONTENTS OF THIS INTELLIGENCE INFORMATION REPORT WITH ANY NON-FBI EMPLOYEES, SINCE THE ADMINISTRATIVE (TICKLER) PAGE MAY CONTAIN SENSITIVE INFORMATION REGARDING INTELLIGENCE SOURCES AND METHODS, FBI INVESTIGATIVE ACTIVITY, AND/OR US PERSON INFORMATION.**

[redacted] b7E

4.7.21.1. (U) Case Number

(U) Enter the number of the case file that contains the source document. If the source document has not yet been uploaded when drafting an IIR [redacted] CHS files should not be included on this line, because in the interest of source protection, it is preferable to limit the number of documents that link an individual [redacted] with the individual's source file. b7E

4.7.21.2. (U) Field Office

(U) This field identifies the authoring FO, Legat, or FBIHQ entity, and is automatically populated by FIDS.

4.7.21.3. (U) Source

(U//FOUO) Enter [redacted] b7E

(U) For [redacted] specify th [redacted] For [redacted] specify the method used to collect the information [redacted] and include the source symbol. Identify foreign government agencies by name. b7E

4.7.21.4. (U [redacted]

[redacted] b7E

b7E

reporting by the source, and the results of any validation activities. If available, the source's pre- [redacted] may be entered here as well. Enter "N/A" when the source is an [redacted] or [redacted] For technical sources, simply provide the date that coverage was initiated. b7E

4.7.21.5. (U) Threat

(U) Does the IIR report a threat? Select "YES" or "NO." For information regarding what constitutes a threat, refer to section Section 4.3.6.1.

4.7.21.6. (U) Agent

[redacted] b7E

4.7.21.7. (U) Terrorist Groups

(U) List any terrorist groups that are mentioned in the IIR. Only those terrorist groups or terrorism support organizations approved by the Interagency Intelligence Committee on Terrorism (IICT) are permissible as entries.

4.7.21.8. (U) USPERS

[redacted] b7E

[redacted] b7E

[redacted] b7E

b7E

4.7.21.9. (U) Liaison

(U) List any entities that the authoring FO solicited (and received) supplementary information from and used to draft the IIR. Also include any entities the authoring FO worked with to address an issue presented in the report (e.g., verbally notifying relevant local, state, tribal, and federal agencies of an immediate threat to local infrastructure). If there are none, then the entry for this field is "NONE."

4.7.21.10. (U) Drafted By

(U) FIDS automatically populates this field with the name and phone number of the person who drafted the IIR.

4.7.21.11. (U) Received By

(U) FIDS automatically populates this section with the name and phone number of the CRO or FBIHQ approving official who reviewed the report.

4.8. (U) IIR Revisions, Recalls, and Updates

(U) In accordance with directives issued by the National Intelligence Analysis and Production Board, when an administrative, textual, or factual error is discovered in a published IIR, the IIR originator must issue either a "revision" or a "recall." A revision is a correction that results in the reissuance of the IIR with the same serial number. A recall uses the same serial number to announce cancellation of the IIR.

4.8.1. (U) Types of IIR Revisions and Recalls

(U) Recalls and revisions may be "administrative" or "substantive." Administrative indicates the change does not affect the substance of the IIR or its text. Substantive indicates the substance of the IIR has changed in a meaningful way.

4.8.1.1. (U) Administrative Revision

(U) An "administrative revision" notifies recipients that a modification has been made that does not affect the substance of the original product (e.g., misspellings, typographical errors, and additional recipients).

4.8.1.2. (U) Substantive Revision

(U) A "substantive revision" notifies recipients that a change has been made that affects the substance of the original product, but does not invalidate it (e.g., dropped words or sentences, or inaccurate paragraphs or comments).

4.8.1.3. (U) Administrative Recall

(U) An "administrative recall" notifies recipients that a product has been withdrawn because of technical, legal, policy, or operational issues (e.g., compromise of sources or methods, inappropriate identification of an USPER, otherwise revisable errors that occurred in the subject line or administrative note/tickler thereby necessitating a reissue, or improper classification).

4.8.1.4. (U) Substantive Recall

(U) A "substantive recall" notifies recipients that a product has been withdrawn because the content is inaccurate and/or misleading, or because the FBI has concerns about the accuracy of the source.

4.8.2. (U) Dissemination Guidelines for Revisions and Recalls

(U//FOUO) Revisions and recalls must be disseminated to each addressee who received the original IIR (i.e., the writer must ensure the new IIR includes all addressees listed in the original PLA). In each instance, use the same serial number as the original report and include a comment directing all recipients to destroy all copies (electronic as well as hard copies) of the original report. The original (incorrect) report should *not* be purged from ACS and FBI hard copy files. As a disseminated report, a file copy must be maintained.

(U) The subject line for IIR revisions and recalls is standardized. Simply precede the subject line in the original IIR with either administrative revision, substantive revision, administrative recall, or substantive recall, separated by a hyphen. For example, if the subject line of the original IIR were [redacted]' there would be four (and only four) possible choices for the new subject line:

[redacted] b7E

b7E

(U) The executive summary is also standardized. Include the original subject line, date/time group (DTG), classification of the original report, and a brief reason for the revision or recall. For example:

[redacted]

(U) When issuing a revision, repeat the original IIR, but correct the mistakes. Then add the following FBI comment:

> (U//FOUO) RECIPIENTS SHOULD DESTROY ALL ELECTRONIC AND HARD COPIES OF THE ORIGINAL REPORT. RECIPIENTS SHOULD ALSO ENSURE THAT ANY CITATION OF THIS INFORMATION IN FINISHED INTELLIGENCE PUBLICATIONS DRAWS ON THE CORRECTED VERSION OF THIS REPORT RATHER THAN THE EARLIER VERSION.

(U) When issuing a recall, do not repeat the text of the original IIR. Instead, add the following FBI comment:

> (U//FOUO) RECIPIENTS SHOULD DESTROY ALL ELECTRONIC AND HARD COPIES OF THE ORIGINAL REPORT.

4.8.2.1. (U) Recall/Reissue

(U) If a revisable error is found in either the subject line or in the administrative note/tickler, the entire IIR must be recalled and reissued with a new serial. [redacted] b7E
[redacted]t is impossible to modify a subject line or the administrative note/tickler. Therefore, issue an administrative recall of the original IIR, and reissue the original with corrections as a new serial number. Do not cite the original report or the administrative recall in the reissued report.

4.8.2.2. (U) Recalls and Revisions in Tearline Reports

(U//FOUO) In addition to the requirements listed above, an IIR that contains a tearline that must be revised or recalled, must also include a revision or recall tearline. The tearline subject line should follow the same format as the overall IIR subject line, and the first paragraph of the tearline should adhere to the structure of the executive summary for a revision or recall. Also include the appropriate comment for either a revision or recall. For example: b7E

[redacted]

4.8.3. (U) IIR Updates

(U) When information updating a previous IIR becomes available, an IIR update may be appropriate. IIR updates should only be done when information in an earlier IIR has developed further. The same source need not provide the new substantive information, but there should be a direct, evolutionary link from the original report to the update.

(U) IIR updates are assigned their own serial numbers in FIDS. In order to demonstrate that a report is an update, preface the previous report's subject line with the words "UPDATE TO." For a second update, use "SECOND UPDATE TO," and so forth. For example, a report whose original subject line was [redacted] would be rendered in an update as: [redacted] b7E

(U) Updated IIRs should, to the extent possible, not repeat information from the original IIR. Instead, they should contain an FBI citation comment referencing the original report, prefaced by the phrase "THIS IIR IS AN UPDATE TO AND SHOULD BE READ IN CONJUNCTION WITH [...]."

5. (U) Legal Review of IIRs

5.1. (U) Necessity of Legal Review

(U) Because IIRs may be distributed to a diverse audience involved in law enforcement or intelligence activities, the FBI must take care to ensure that information contained in an IIR is disseminated in accordance with constitutional, statutory, regulatory, and policy considerations. To ensure that the FBI is in compliance with these limitations, legal review and approval of an IIR may be required before it can be disseminated. This section of [redacted] will detail the circumstances in which legal concurrence is necessary to disseminate an IIR. For more in depth discussion, see the [redacted] b7E

5.2. (U) Legal Reviewers of IIRs

(U) Legal reviewers of IIRs in the field will generally be CDCs and, at FBIHQ, will be FBIHQ attorneys in OGC.

5.2.1. (U) Chief Division Counsels

(U//FOUO) When required, in accordance with the [redacted] CDCs are responsible for providing legal review and concurrence of IIRs originating within their field office. CDCs are responsible for having current knowledge of the laws and regulations that govern dissemination of FBI-gathered information and FBI policy developments regarding sensitive matters. CDCs will provide IIR authors and reviewers within their field office with training and guidance, when needed, on statutory and policy developments concerning matters covered by this PG and the [redacted]

5.2.2. (U) Office of the General Counsel

(U//FOUO) When required, in accordance with the [redacted] is responsible for providing legal review and concurrence of IIRs originating within FBIHQ or Legats. OGC is responsible for providing comprehensive information to IIR authors, IIR reviewers, and CDCs regarding the legal requirements and policies relevant to the dissemination of FBI-gathered information or FBI policy regarding sensitive matters. OGC is also responsible for having current knowledge of the laws and regulations that govern dissemination of FBI-gathered information and FBI policy developments regarding sensitive matters. OGC will provide IIR authors and reviewers with training and guidance, when needed, on statutory and policy developments concerning matters covered by this PG and the [redacted] b7E

5.3. (U) Circumstances Under Which Legal Review is Required

(U//FOUO) [redacted] requires that if an IIR contains information derived from one of the following sources, or involves an issue listed below, then legal review is required.

[redacted] b7E

b7E

For additional information, see OGC

b7E

6. (U) Recordkeeping Requirements and IIR Metrics

6.1. (U) Data Storage

(U) The FBI requires that disseminated IIRs be stored in ACS.

(U) Each IIR [redacted] is automatically uploaded by [redacted] to the following files:

[redacted]

b7E

(U) FIDS uploads [redacted] with their ticklers, as listed below:

[redacted]

(U) IIRs that contain classified [redacted] manually uploaded to:

[redacted]

(U//FOUO) For a complete list of subfiles, see the List of Country-Specific Suffixes (note: while the subfiles conform to the ISO 3166 standard trigraphic country codes found in Appendix A of this PG, not every trigraphic country code has an accompanying foreign disclosure subfile).

(U) In addition, a hard copy of each IIR, with a signed cover sheet, must be mailed to the [redacted] This hardcopy must include:

- A copy of the original approver's signature;
- The case IDs and serial numbers of all case files to which the IIR was uploaded; and
- A date/time group.

(U) Instructions for transferring hard copy files to the ARC can be found on the [redacted] [redacted]

b7E

6.2. (U) IIR Production Metrics

(U) A variety of IIR metrics are monitored by the DI. Certain monitored IIR metrics are reported within the [redacted] for use with [redacted] with FO SACs. Intelligence managers and supervisors should be familiar with the metrics detailed below, as IIR metrics are taking an increasingly central role in [redacted]

b7E

6.2.1. (U) IIR Velocity Rate

(U) The IIR velocity rate is the total time it takes to produce an IIR (including field collection, drafting the IIR in FIDS, and dissemination to the USIC and/or law enforcement community) and is a measurement of the FBI's performance in intelligence production. The velocity of IIRs

is measured from the point of intelligence collection (date of acquisition), to the time of dissemination (the date/time group assigned by FAMS), and is calculated on a monthly basis.

(U) Rigorous and efficient measures should be in place to move collection requirements-driven intelligence from the investigator through the FIGs, in the form of an IIR in an expeditious manner.

6.2.2. (U) Other IIR Metrics

(U) Due to the transition to direct dissemination from FBI field offices, new IIR metrics are under development in order to capture relevant performance data and will be included in future versions of this PG.

7. (U) Summary of Legal Authorities

(U) Numerous laws and regulations pertain to the dissemination of raw intelligence information by the FBI. IIR authors and reviewers should familiarize themselves with the following laws, regulations, and policy documents:

- (U) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001*
- (U) *Intelligence Reform and Terrorism Prevention Act* (IRTPA)
- (U) *Foreign Intelligence Surveillance Act of 1978*
- (U) *Omnibus Crime Control and Safe Streets Act of 1968 (Title III)*
- (U) *Privacy Act of 1974*
- (U) *Federal Wiretap Act*, 18 U.S.C. § 2510, et seq.
- (U) *Bank Secrecy Act*, 31 U.S.C. § 5318(g), et seq.

[redacted]

- *(U) The Attorney General's Guidelines for Domestic FBI Investigations*

[redacted]

- *(U) Domestic Investigations and Operations Guide (DIOG)*

b7E

[redacted]

8. (U) Addenda and Errata

(U) Below is a comprehensive list of all substantive revisions made since the release of the previous version of this PG. Minor language and stylistic changes are not included, nor are changes made to reflect the reorganization of the former Reports Section. Sections in bold type are new to this version; sections in italics are from the previous PG version and have been removed or combined with other sections.

Section	Revision
4.2	Included updated requirements information from the Collection Management Section
4.3.4	Revised "of interest" threshold to "meets a requirement" per DI front office
4.3.5	Added new procedures for approving USPER information in IIRs
4.3.7	Added more information concerning criminal IIRs
4.3.8	Added more comprehensive description of DT threshold
4.3.9	Replaced with section on Internet reporting
4.3.10	Includes revised definitions of open source information
4.3.10.1-4.3.10.7	Broke original *Section 4.3.9* into seven sub-sections and expanded on them
4.3.11	Clarified dissemination of criminal grand jury information
4.3.12	Added section on [redacted]
4.4.1-4.4.7	*Deleted PLA lists from PG*
4.4.2	Clarified rules for when to use teletype memoranda
(S) **4.4.3.2**	[redacted]
4.4.4	Recommended consideration of an Unclas tearline in No Double Standard situations
4.4.12	Moved to Section 5.2
4.4.13	Deleted; not pertinent to the PG
4.6.2	Various changes concerning naming conventions and labeling of USPERs; expansion of USPER definition based on DIOG
4.6.3	Clarified definition of operational information vs. identifier information and what products to use to disseminate both
4.6.4	Removed quotations from around the name in the example; addition of rules regarding partial names as USPERs, and regarding phonetic approximations of

b1
b7E

	names
4.6.5	Included alternatives to using special characters
4.6.6	Addresses use of e-mails as source documents
4.6.7	Retitled section; added clarification on use of numbers; added additional accepted acronyms; clarified use of time zones; included a section on the parenthetical comma in city/state combos; provided guidance on map coordinates
4.6.8	Excluded double parentheses from executive summary; noted countries where surname is not last name
4.6.9	Changed ACQ to timeliness, as last date information was known to be true
4.6.10	Added section on active/passive voice
4.7.1	Added embassies and Legat dissemination guidance to INFO section
4.7.3.2	Changed section title; simplification of dispute process and additional guidance
4.7.3.3	Brought declassification marking guidance into line with recent CAPCO revisions eliminating the banner line declassification value and manual review
4.7.3.4	Corrected title of section; added FISA control
4.7.3.4.2	Clarified the removal of LES from IIR usage
4.7.3.4.5	Prohibits use of REL TO in overall classifications
4.7.3.4.6	Added section on use [redacted] control
4.7.5	Added older CRCs for reference
4.7.8	Added information and examples on SUBJ
4.7.11	Clarified and expanded on how and when to cite which requirements
4.7.12	Defined "source"; stipulated usage of (U) portion marking on all source bylines; defined access statements and corroboration statements
4.7.12.1.1	Changed title
4.7.12.1.2	Added section on limited contact byline
4.7.12.1.3	Expanded on definition o[redacted]
4.7.12.1.7	Expanded on usage of "An FBI SA"
4.7.12.1.8	Expanded on usage of "An Employee of the FBI"
4.7.12.1.11	Added section on "Officer of Another USG Entity"
4.7.12.1.12	Included sensitive[redacted]n the sensitive category
4.7.12.2	*Previous 4.7.12.2 incorporated into section* 4.7.12.-Now concerns multiple sources
4.7.12.3	*Incorporated into section 4.7.12*

b7E

b7E

4.7.13	Included guidance to generalize context statements
4.7.13.1	Removed "source speculation" sample context statement
4.7.14.1	Prohibited use of comment information in executive summaries
4.7.14.2	Added a section on body text
4.7.15.2	Added a sample Classified tearline b7E
4.7.15.3	Added a section on PLA lists for [redacted]
4.7.16	Clarified that any in-text comments should be enclosed in parentheses
4.7.16.1.1.2	Added a full section on citation comment
4.7.16.1.1.3	Added a section on prohibited, defunct comments
4.7.21	Added all relevant entries for approval and coordination
4.7.21.3	Elaborated on when to name a source in the source field
4.7.12.4.3	Included subsources in timeliness
4.7.21.8	Specified that both named and unnamed USPERs must be included in USPERS field
4.7.21.12	Deleted; copy counts no longer in use
4.8.2	Prohibits the purging of revised or recalled reports from ACS; corrected DTG citation
4.8.2.1	Issued guidance for revising subject lines and administrative notes/ticklers
4.8.2.2	Issued guidance for revising reports with tearlines
4.8.3	Created a section on IIR updates
5	Created a section on legal review
6.1	Updated soft copy and hard copy storage requirements
6.2	Created section on IIR metrics, including definitions for velocity rate, throughput rate, and first-time throughput rate b7E
Appendix B	[redacted]
Appendix C	*removed*
Appendix F	*removed*
Appendix G	*removed*

(U) Appendix A: List of Digraph and Trigraph Codes

Entity	FIPS 10-4	ISO 3166
Afghanistan	AF	AFG
Albania	AL	ALB
Algeria	AG	DZA
American Samoa	AQ	ASM
Andorra	AN	AND
Angola	AO	AGO
Anguilla	AV	AIA
Antarctica	AY	ATA
Antigua and Barbuda	AC	ATG
Argentina	AR	ARG
Armenia	AM	ARM
Aruba	AA	ABW
Ashmore and Cartier Islands	AT	-
Australia	AS	AUS
Austria	AU	AUT
Azerbaijan	AJ	AZE
The Bahamas	BF	BHS
Bahrain	BA	BHR
Baker Island	FQ	-
Bangladesh	BG	BGD
Barbados	BB	BRB

Entity	FIPS 10-4	ISO 3166
Bassas da India	BS	-
Belarus	BO	BLR
Belgium	BE	BEL
Belize	BH	BLZ
Benin	BN	BEN
Bermuda	BD	BMU
Bhutan	BT	BTN
Bolivia	BL	BOL
Bosnia and Herzegovina	BK	BIH
Botswana	BC	BWA
Bouvet Island	BV	BVT
Brazil	BR	BRA
British Indian Ocean Territory	IO	IOT
British Virgin Islands	VI	VGB
Brunei	BX	BRN
Bulgaria	BU	BGR
Burkina Faso	UV	BFA
Burma	BM	MMR
Burundi	BY	BDI
Cambodia	CB	KHM
Cameroon	CM	CMR
Canada	CA	CAN
Cape Verde	CV	CPV

Entity	FIPS 10-4	ISO 3166
Cayman Islands	CJ	CYM
Central African Republic	CT	CAF
Chad	CD	TCD
Chile	CI	CHL
China	CH	CHN
Christmas Island	KT	CXR
Clipperton Island	IP	-
Cocos (Keeling) Islands	CK	CCK
Colombia	CO	COL
Comoros	CN	COM
Congo, Democratic Republic of the	CG	COD
Congo, Republic of the	CF	COG
Cook Islands	CW	COK
Coral Sea Islands	CR	-
Costa Rica	CS	CRI
Cote d'Ivoire	IV	CIV
Croatia	HR	HRV
Cuba	CU	CUB
Cyprus	CY	CYP
Czech Republic	EZ	CZE
Denmark	DA	DNK
Djibouti	DJ	DJI
Dominica	DO	DMA

Entity	FIPS 10-4	ISO 3166
Dominican Republic	DR	DOM
East Timor	TT	TLS
Ecuador	EC	ECU
Egypt	EG	EGY
El Salvador	ES	SLV
Equatorial Guinea	EK	GNQ
Eritrea	ER	ERI
Estonia	EN	EST
Ethiopia	ET	ETH
Europa Island	EU	-
Falkland Islands (Islas Malvinas)	FK	FLK
Faroe Islands	FO	FRO
Fiji	FJ	FJI
Finland	FI	FIN
France	FR	FRA
France, Metropolitan	-	FXX
French Guiana	FG	GUF
French Polynesia	FP	PYF
French Southern and Antarctic Lands	FS	ATF
Gabon	GB	GAB
The Gambia	GA	GMB
Gaza Strip	GZ	PSE
Georgia	GG	GEO

Entity	FIPS 10-4	ISO 3166
Germany	GM	DEU
Ghana	GH	GHA
Gibraltar	GI	GIB
Glorioso Islands	GO	-
Greece	GR	GRC
Greenland	GL	GRL
Grenada	GJ	GRD
Guadeloupe	GP	GLP
Guam	GQ	GUM
Guatemala	GT	GTM
Guernsey	GK	GGY
Guinea	GV	GIN
Guinea-Bissau	PU	GNB
Guyana	GY	GUY
Haiti	HA	HTI
Heard Island and McDonald Islands	HM	HMD
Holy See (Vatican City)	VT	VAT
Honduras	HO	HND
Hong Kong	HK	HKG
Howland Island	HQ	-
Hungary	HU	HUN
Iceland	IC	ISL
India	IN	IND

Entity	FIPS 10-4	ISO 3166
Indonesia	ID	IDN
Iran	IR	IRN
Iraq	IZ	IRQ
Ireland	EI	IRL
Isle of Man	IM	IMN
Israel	IS	ISR
Italy	IT	ITA
Jamaica	JM	JAM
Jan Mayen	JN	-
Japan	JA	JPN
Jarvis Island	DQ	-
Jersey	JE	JEY
Johnston Atoll	JQ	-
Jordan	JO	JOR
Juan de Nova Island	JU	-
Kazakhstan	KZ	KAZ
Kenya	KE	KEN
Kingman Reef	KQ	-
Kiribati	KR	KIR
Korea, North	KN	PRK
Korea, South	KS	KOR
Kuwait	KU	KWT
Kyrgyzstan	KG	KGZ

Entity	FIPS 10-4	ISO 3166
Laos	LA	LAO
Latvia	LG	LVA
Lebanon	LE	LBN
Lesotho	LT	LSO
Liberia	LI	LBR
Libya	LY	LBY
Liechtenstein	LS	LIE
Lithuania	LH	LTU
Luxembourg	LU	LUX
Macau	MC	MAC
Macedonia	MK	MKD
Madagascar	MA	MDG
Malawi	MI	MWI
Malaysia	MY	MYS
Maldives	MV	MDV
Mali	ML	MLI
Malta	MT	MLT
Marshall Islands	RM	MHL
Martinique	MB	MTQ
Mauritania	MR	MRT
Mauritius	MP	MUS
Mayotte	MF	MYT
Mexico	MX	MEX

Entity	FIPS 10-4	ISO 3166
Micronesia, Federated States of	FM	FSM
Midway Islands	MQ	-
Moldova	MD	MDA
Monaco	MN	MCO
Mongolia	MG	MNG
Montenegro	MJ	MNE
Montserrat	MH	MSR
Morocco	MO	MAR
Mozambique	MZ	MOZ
Myanmar	-	-
Namibia	WA	NAM
Nauru	NR	NRU
Navassa Island	BQ	-
Nepal	NP	NPL
Netherlands	NL	NLD
Netherlands Antilles	NT	ANT
New Caledonia	NC	NCL
New Zealand	NZ	NZL
Nicaragua	NU	NIC
Niger	NG	NER
Nigeria	NI	NGA
Niue	NE	NIU
Norfolk Island	NF	NFK

Entity	FIPS 10-4	ISO 3166
Northern Mariana Islands	CQ	MNP
Norway	NO	NOR
Oman	MU	OMN
Pakistan	PK	PAK
Palau	PS	PLW
Palmyra Atoll	LQ	-
Panama	PM	PAN
Papua New Guinea	PP	PNG
Paracel Islands	PF	-
Paraguay	PA	PRY
Peru	PE	PER
Philippines	RP	PHL
Pitcairn Islands	PC	PCN
Poland	PL	POL
Portugal	PO	PRT
Puerto Rico	RQ	PRI
Qatar	QA	QAT
Reunion	RE	REU
Romania	RO	ROU
Russia	RS	RUS
Rwanda	RW	RWA
Saint Helena	SH	SHN
Saint Kitts and Nevis	SC	KNA

Entity	FIPS 10-4	ISO 3166
Saint Lucia	ST	LCA
Saint Pierre and Miquelon	SB	SPM
Saint Vincent and the Grenadines	VC	VCT
Samoa	WS	WSM
San Marino	SM	SMR
Sao Tome and Principe	TP	STP
Saudi Arabia	SA	SAU
Senegal	SG	SEN
Serbia	RB	SRB
Seychelles	SE	SYC
Sierra Leone	SL	SLE
Singapore	SN	SGP
Slovakia	LO	SVK
Slovenia	SI	SVN
Solomon Islands	BP	SLB
Somalia	SO	SOM
South Africa	SF	ZAF
South Georgia and the Islands	SX	SGS
Spain	SP	ESP
Spratly Islands	PG	-
Sri Lanka	CE	LKA
Sudan	SU	SDN
Suriname	NS	SUR

Entity	FIPS 10-4	ISO 3166
Svalbard	SV	SJM
Swaziland	WZ	SWZ
Sweden	SW	SWE
Switzerland	SZ	CHE
Syria	SY	SYR
Taiwan	TW	TWN
Tajikistan	TI	TJK
Tanzania	TZ	TZA
Thailand	TH	THA
Togo	TO	TGO
Tokelau	TL	TKL
Tonga	TN	TON
Trinidad and Tobago	TD	TTO
Tromelin Island	TE	-
Tunisia	TS	TUN
Turkey	TU	TUR
Turkmenistan	TX	TKM
Turks and Caicos Islands	TK	TCA
Tuvalu	TV	TUV
Uganda	UG	UGA
Ukraine	UP	UKR
United Arab Emirates	AE	ARE
United Kingdom	UK	GBR

Entity	FIPS 10-4	ISO 3166
United States	US	USA
United States Minor Outlying Islands	-	UMI
Uruguay	UY	URY
Uzbekistan	UZ	UZB
Vanuatu	NH	VUT
Venezuela	VE	VEN
Vietnam	VM	VNM
Virgin Islands	VQ	VIR
Virgin Islands (UK)	-	-
Virgin Islands (US)	-	-
Wake Island	WQ	-
Wallis and Futuna	WF	WLF
West Bank	WE	PSE
Western Sahara	WI	ESH
World	-	-
Yemen	YM	YEM
Zaire	-	-
Zambia	ZA	ZMB
Zimbabwe	ZI	ZWE

(U) Appendix B: Definitions

(U) **Bot:** Short for "robot," it is a computer application that automatically performs a certain (generally nefarious) programmed task.

(U) **Botnet:** Short for "robot network," it is a network of compromised computers remotely controlled by a hacker. A botnet is often referred to as a "zombie army."

(U) **Communications Intelligence (COMINT):** Technical and intelligence information derived from foreign communications by someone other than the intended recipients.

(U) **Date/Time Group (DTG):** In an FBI IIR, the DTG indicates the exact time an IIR was disseminated via SAMNET. DTGs are formatted as follows: P DDHHHHZ MON YY, where P = precedence, DD = day, HHHH = hour in Zulu time, MON = month, YY = calendar year, and Z = Zulu time. An FBI DTG of "R 261445Z NOV 07" indicates a routine IIR was disseminated via SAMNET on 11/26/2007 at 14:45 Zulu time.

Other agencies use a different DTG format, which IIR authors should be familiar with. This convention is as follows: P YYMMDDHHHHZ, where P = precedence, YY = calendar year, MM = month, DD = day, HHHH = hours, and Z = Zulu time. An example would be DTG P 0709171839Z, which is a priority report released on 7 September 2009, at 1839h, Zulu time. In the format employed by the FBI, this would become DTG P 171839Z SEP 07.

(U) **Declassification:** The determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation. When media is lowered to unclassified, it must be properly sanitized before it can be downgraded.

(U) **Denial of Service (DOS):** A type of cyber attack that floods a network with so many requests (or so much information) that regular service is slowed or interrupted.

(U) **Derivative Classification:** The incorporating, paraphrasing, restating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(U) **Distributed Denial of Service (DDOS):** A type of denial-of-service attack in which an attacker uses malicious code, installed on multiple computers, to attack a single target.

b7E

(U) **Domain Name System (DNS):** An Internet service that translates domain names into Internet Protocol (IP) addresses. For example, the domain name "cnn.com" translates to IP address 64.236.16.52. The "s" in "DNS" can also stand for "service" or "server."

(U) **Downgrading:** Changing a security classification from a higher to a lower level.

(U) **DRAIN:** An acronym which represents the threshold for an IIR. The information in an IIR must: be detailed, respect the rights of United States persons to participate in constitutionally-protected activities, be authoritative, be of interest, and be new.

(U) **Executive Order (EO):** A rule or order signed by the President.

(U) **File Transfer Protocol (FTP):** The name of an application, as well as the protocol used by the application, to move files from one machine to another.

(U) **Foreign National:** Any individual who is not a citizen of the United States by birth or through naturalization, including resident aliens, students, refugees, and émigrés. The term "foreign national" and "non-U.S. citizen" may be used interchangeably.

(U) **Hacker:** For purposes of intelligence collection and dissemination, a hacker is an individual who uses a computer for the purposes of exploitation (i.e., to take advantage of a vulnerability on a target computer).

(U) **Hacktivist:** An individual who uses hacker techniques in furtherance of the individual's cause [redacted] b7E

(U) **Hard Copy:** Any document that is initially published and distributed by the originating component in physical form.

(U) **Human Intelligence (HUMINT):** A category of intelligence derived from information collected and/or provided by human sources.

(U) **Hyper Text Transfer Protocol (HTTP):** The method used by the Internet to communicate with the World Wide Web. When a computer requests a specific Web page, HTTP is the way in which the Web page is sent to the computer.

[redacted] b7E

(U) **Internet Protocol (IP) Address:** A unique address for a computer or device on a network.

(U) **Keylogger:** Software or hardware that records the key depressions on a computer. Keyloggers (also known as "keystroke loggers") are often trojans designed to steal passwords.

(U) **Malware:** Short for "malicious software," malware is any software developed for the purpose of infiltrating (or doing harm to) another computer. Examples of malware include trojans, worms, viruses, and rootkits.

[redacted]

b7E

(U) **Media Access Control (MAC) Address:** A unique code assigned and burned into most network hardware. For example, the MAC address for a network adapter would resemble the following: 00-08-74-4C-7F-1D.

(U) **National Security Information (NSI):** Includes any information that has been determined, pursuant to EO 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is so designated. The levels Top Secret, Secret, and Confidential are used to designate such information.

(U) **National Security Threat List (NSTL):** A Federal Bureau of Investigation listing of strategic country and issue threats.

[redacted]

(U) **Original Classification:** An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(U) **Phishing:** A social engineering practice designed to acquire protected information, such as bank account numbers, passwords, credit card numbers, and social security numbers.

(U) **Plain-Language Address (PLA):** A phrase used to denote the abbreviated language coding of an activity short title used in message addressing.

[redacted]

b7E

(U) **Server:** A computer or device on a network that manages network resources. For example, a print server is a computer that manages one or more printers.

[redacted]

(U) **Sniffer:** A program that captures traffic from a computer network. Sniffers are often used to gather sensitive information such as user IDs and passwords as they are transmitted across a local area network.

(U) **SQL (Structured Query Language) Injection:** A vulnerability that exists in the database layer of an application that could grant an unauthorized user access to the

database. SQL is a computer language that data retrieval programs (such as Microsoft Access) use to store and retrieve information.

(U) Subsource: If the source of an IIR does not directly observe the activity the source is reporting on, but rather learns of it through an intermediary, the intermediary is known as a subsource.

(U) Trojan: A computer program that appears legitimate, but performs some illicit activity when run.

(U) Virus: A computer program that produces copies of itself and inserts them into other programs, usually performing a malicious action, such as deleting data.

(U) Voice-over Internet Protocol (VoIP): Allows a voice connection that is similar to a telephone connection, but uses Internet Protocol (IP) lines, rather than telephone lines.

(U) Worm: A computer program that replicates itself over a computer network and usually performs a malicious action.

(U) Zulu Time: Zulu time is the international atomic time scale that serves as the basis of timekeeping for most of the world. The hours, minutes, and seconds expressed by Zulu time represent the time of day at the Prime Meridian (0° longitude) located near Greenwich, England, as reckoned from midnight. Zulu time is calculated by the Bureau International des Poids et Measures (BIPM) in Sevres, France. The BIPM averages data collected from more than 200 atomic time and frequency standards located at about 50 laboratories worldwide. Zulu time is also referred to as "Coordinated Universal Time (UTC)."

(U) Appendix C: Acronyms

AB	Analysis Branch (DI)
ACDC	Assistant Chief Division Counsels
ACQ	Date of Acquisition
ACRO	Associate Chief Reports Officer
ACS	Automated Case System
AD	Assistant Director
ADIC	Assistant Director in Charge
AGG-Dom	The Attorney General Guidelines for Domestic FBI Operations
[redacted]	
ASAC	Assistant Special Agent in Charge
AUSA	Assistant US Attorney
BLUF	Bottom Line Up Front (writing style)
BOP	Bureau of Prisons
BSA	Bank Secrecy Act
CAPCO	Controlled Access Program Coordination Office
CD	Counterintelligence Division
CDC	Chief Division Counsel
CFR	Code of Federal Regulations
CHS	Confidential Human Source
CID	Criminal Investigative Division
CIR	Current Intelligence Report
CIS	Criminal Intelligence Section (DI)
CMIR	Report of International Transportation of Currency or Monetary Instruments
COMINT	Communications Intelligence
CRO	Chief Reports Officer
CSCC	Central Strategic Coordinating Component
CT	Counterterrorism
CTD	Counterterrorism Division

b7E

b7E

CyBIS	Cyber Intelligence Section (DI)
CyD	Cyber Division
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCMB	Domain and Collection Management Branch (DI)
DDR	Director's Daily Report
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIDO	Designated Intelligence Disclosure Official
DIOG	Domestic Investigations and Operations Guide
DNI	Director of National Intelligence
DNID	Director of National Intelligence Directive
DOI	Date of Information
DOJ	Department of Justice
DNI	Director of National Intelligence
DT	Domestic Terrorism
DTG	Date/Time Group
EAD	Executive Assistant Director
EC	Electronic Communication
ELSUR	Electronic Surveillance
EO	Executive Order

b7E

FI	Foreign Intelligence
FIDS	FBI IIR Dissemination System
FIG	Field Intelligence Group
FinCEN	Financial Crimes Enforcement Network
FISA	Foreign Intelligence Surveillance Act
FO	Field Office

FOUO	For Official Use Only
GPS	Global Positioning Satellite
HUMINT	Human Intelligence
IA	Intelligence Analyst
ICD	Intelligence Community Directive
IFC	Intelligence Functional Code
IFODDP	IIR Field Office Direct Dissemination Procedure
IIR	Intelligence Information Report
IMINT	Imagery Intelligence
IOB	Intelligence Oversight Board; Intelligence Operations Branch (DI)
IOD	International Operations Division
IP	Internet Protocol
IPSP	Intelligence Priority for Strategic Planning
IT	International Terrorism
KIO	Known Intelligence Officer
LA	Language Analyst
LEGAT	Legal Attache
LES	Law Enforcement Sensitive
LPR	Legal Permanent Resident
MASINT	Measurement and Signature Intelligence
MOU	Memorandum of Understanding
MR	Manual Review
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NGA	National Geospatial Intelligence Agency
NIPF	National Intelligence Priorities Framework
NHCD	National HUMINT Collection Directives
NOFORN	Not Releasable to Foreign Nationals
NSB	National Security Branch

NSISC	National Security Information Security Classification (Guide)
NSRRS	National Security Reports and Requirements Section (DI–Reports Section predecessor)
NSL	National Security Letter
OCA	Original Classification Authority
OCE	Online Covert Employee
ODNI	Office of the Director of National Intelligence
OGA	Other Government Agency
OGC	Office of the General Counsel
ORCON	Originator Controlled
OS	Operations Specialist (Intelligence Analyst)
OSC	Open Source Center
OSINT	Open Source Intelligence
PII	Personally Identifying Information
PLA	Plain Language Address
REL TO	Release To
RFI	Request for Information
RO	Reports Officer (Intelligence Analyst)
SA	Special Agent
SAC	Special Agent in Charge
SAR	Suspicious Activity Report
SAR-M	Suspicious Activity Report for Money Service Businesses
SBU	Sensitive But Unclassified
SC	Section Chief
SCI	Sensitive Compartmented Information
SIA	Supervisory Intelligence Analyst
SIGINT	Signals Intelligence
SIO	Suspected Intelligence Officer
SIOC	Strategic Information and Operations Center

b7E

T-III	Title III
TFO	Task Force Officer
TM	Teletype Memorandum
UC	Unit Chief
UCE	Undercover Employee
UCO	Undercover Operation
U//FOUO	Unclassified//For Official Use Only
USA	United States Attorney
USAO	United States Attorney's Office
USG	US Government
USIC	US Intelligence Community
USPER	United States Person, United States Persons, USPERs, USP, USPs, US Person, US Persons, U.S. Person, U.S. Persons
WMD	Weapons of Mass Destruction