~~(S)~~ HR 7-1/E.O. 12333 ISSUES: COLLECTION, RETENTION, DISSEMINATION OF US PERSON INFORMATION
Trainer's Training Template

(U//~~AIUO~~) PREFACE: You've just heard some of the background of E.O. 12333 and how it came to be promulgated. In looking at the issues around collecting and handling US person information, keep in mind that the rules flowing from the E.O. are extensions of the basic principle of protecting the constitutional rights of those people who are supposed to be protected by the constitution. Where the Agency is collecting against non-US persons outside the US, the Constitution doesn't protect these people and neither do the EO and our regulations: accordingly, there are fewer limitations on what kind of collection the Agency can do in those situations. Where our activities will or may affect people who are protected by the Constitution (as a practical matter, anyone inside the US and USPs anywhere), there are more restrictions. In addition, the more intrusive the collection, the more strict are the limitations on what the Agency can do and the higher level the approval necessary to do it.

~~(S)~~ APPLICABLE AUTHORITIES: Like all government activities, intelligence collection must be affirmatively authorized by law and must not fall within any legal proscriptions. The limitations on collection within the United States or against United States persons are grounded in the Fourth Amendment to the Constitution as well as broader American notions of privacy and of the propriety of CIA's intelligence activities. The first clause of the Fourth Amendment provides:

> *The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated . . .*

Implementing and expanding upon Fourth Amendment principles are Executive Order 12333 and its implementing procedures set out in HR 7-1, and its Annexes and Appendices. Annexes A and B are the so-called "Attorney-General-approved procedures" for CIA activities outside and inside the United States, respectively. The sections of HR 7-1 dealing specifically with collecting and handling US Person information are 7-1a(4) (b)-(c) and Annex A, for collection outside the US, and HR 7-1a (5)(b)-(d) Annex B, for collection inside the US.

B. ~~(AIUO)~~ Basic Principles for US Person Information

The fundamental questions for targeting for collection are "who?" and "where?": That is, who is the target, and is the collection occuring inside or outside the United States? The restrictions of US law and regulation generally apply to collection against US Persons anywhere and against any collection in the U.S. (Down the road when you're looking at how CIA must handle the intelligence we collect you'll also need to look at

"*whom* did we end up collecting information *about*?" no matter whom we were "collecting against".)

There are 3 basic rules that apply to all collection:

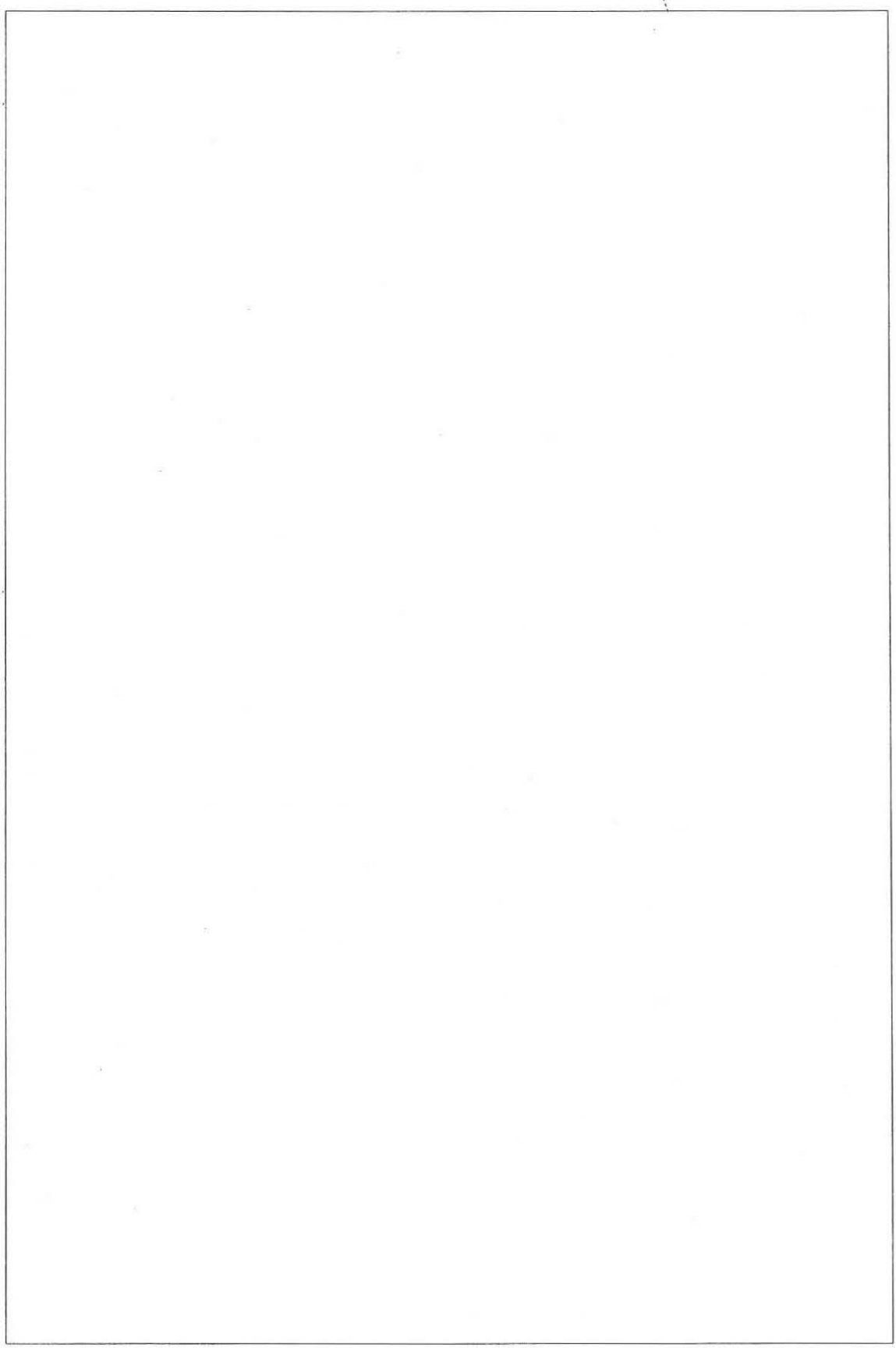
1. The CIA may only collect *foreign* intelligence. This includes information about counterintelligence, counterproliferation, foreign aspects of drug trafficking, international terrorists. Home-grown terrorists and local insurgents or drug lords who don't have international ties are not our bailiwick. So when the federal building in Oklahoma City blew up, the Agency explored whether international terrorists might have been at work. As it emerged that this was the work of an American, it became the FBI's job to identify and collect evidence against the bomber. If there had been some evidence that Timothy McVeigh had ties to al-Qa'ida, the Agency might have had a continuing role in that investigation.
The domestic activities of US persons are outside CIA's mandate and authority.
Note that Section 3 of the National Security Act defines "foreign intelligence" and "counterintelligence". [If not previously, identified: this is in of the HPSCI compilation of Intelligence Laws etc., aka the "blue book", which is now brown (p. 5).] There can be considerable overlap in the technical definitions of FI and CI, but as a practical matter it is most helpful to think of CIA's intelligence charter as needing to be foreign-focused. (Remember that, under the Law Enforcement proviso, the Agency "shall have no . . . internal security functions.")

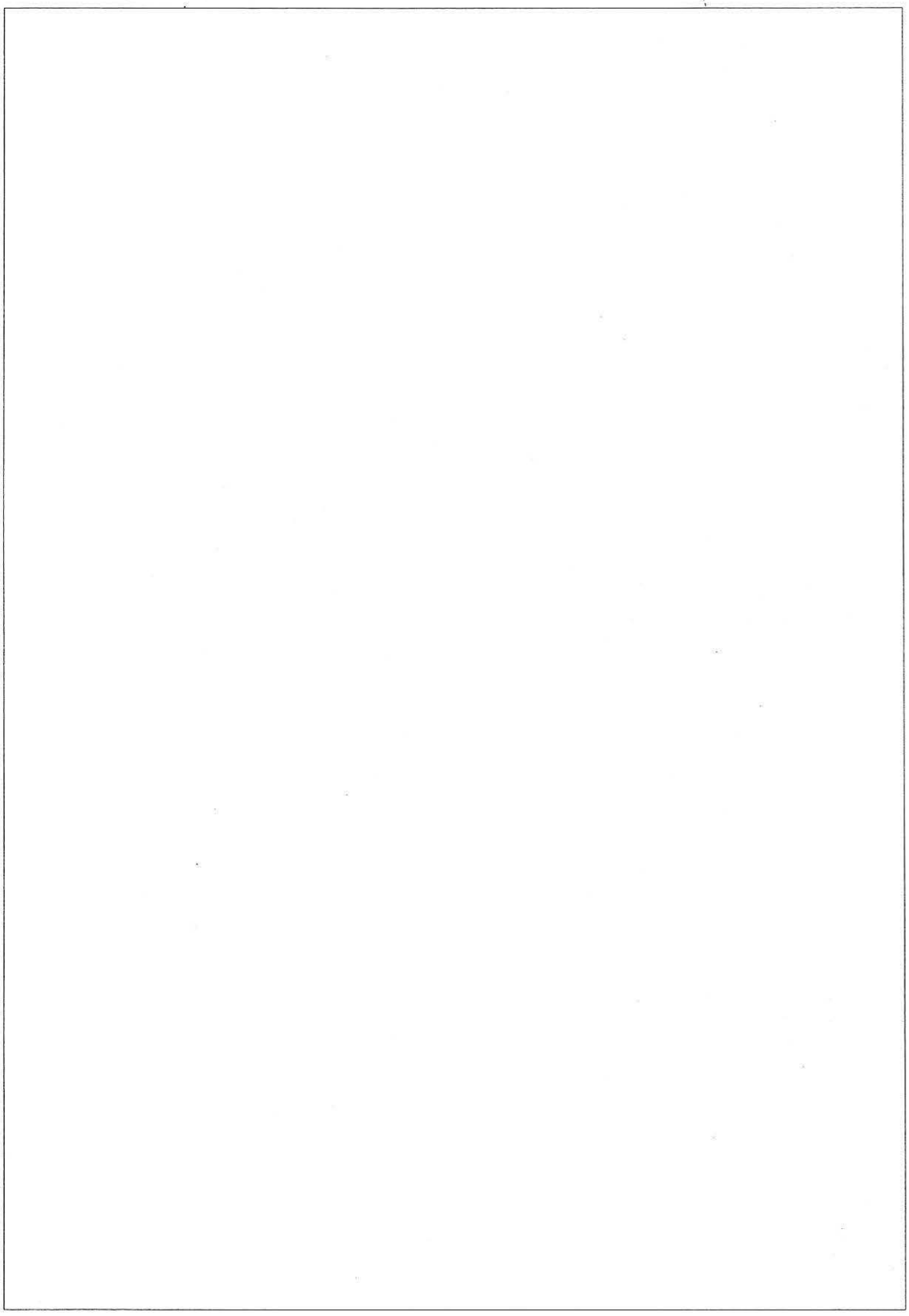
2. Another general principle is that the Agency must use least intrusive means available to obtain the intelligence we need. No matter who or where the target, it's sound policy not to shoot a fly with an elephant gun -- or not to plant a bug on a target's briefcase to find out where he lives, to get his address, if we can look it up in the phone book. When the CIA is dealing with people who have rights under the US Constitution, we have a legal duty, as well, not to intrude upon their privacy more than is necessary. This duty is imposed by § 2.4 of E.O. 12333 [p. 1079 of brown book]. (b)(1) (b)(3) NatSecAct

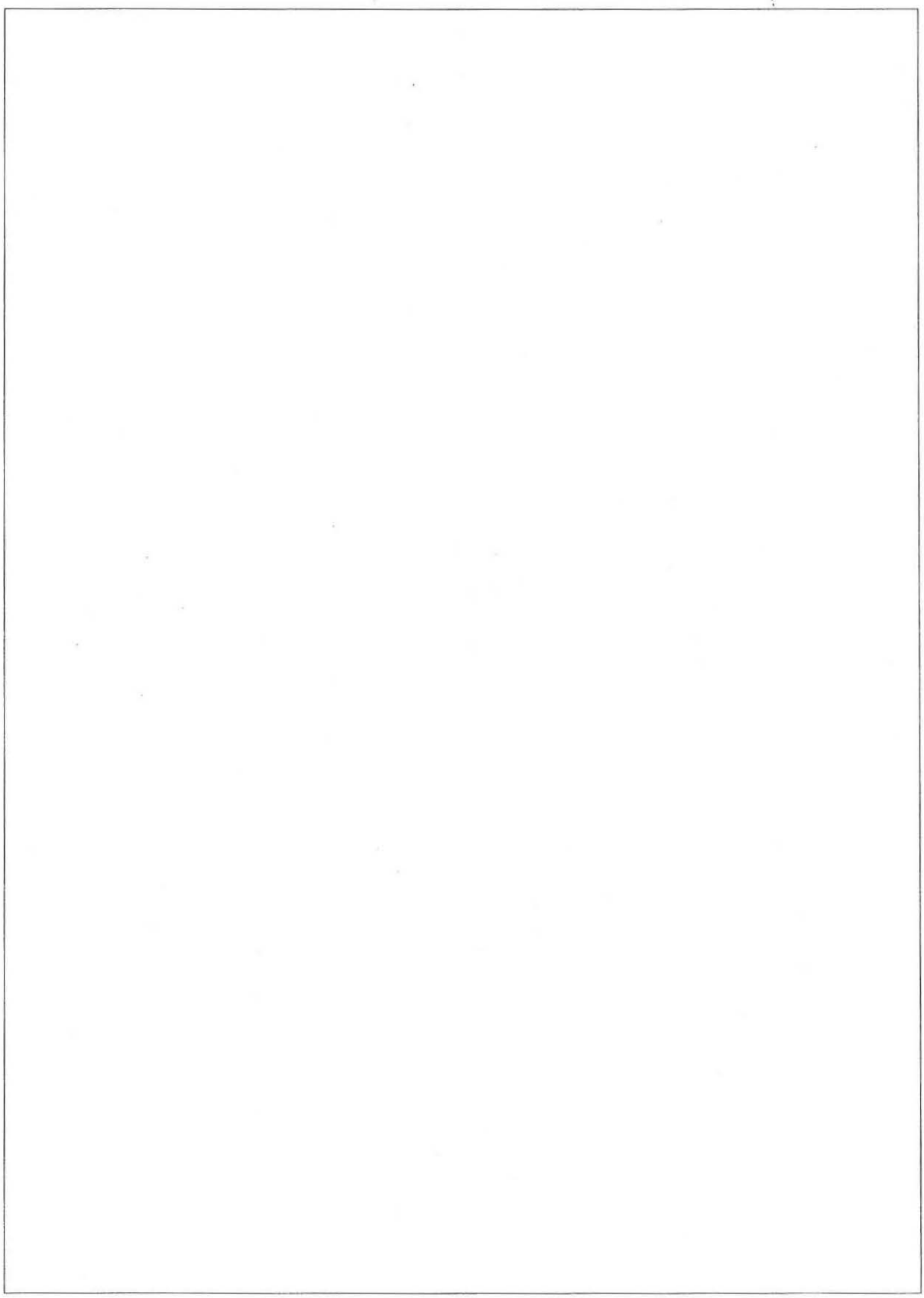
3. Collectors may not ask somebody else [redacted] to collect what they cannot. If it's against the rules for CIA to get it, we can't ask or hint for someone else to. (No telling liaison, "gee, we'd really like to get that information, and if you all gave it to us, we could use it, but our regulations say we can't tap his phone . . .[wink, wink, nudge, nudge].") Section 2.12 of the Executive Order sets out this rule against indirect participation.

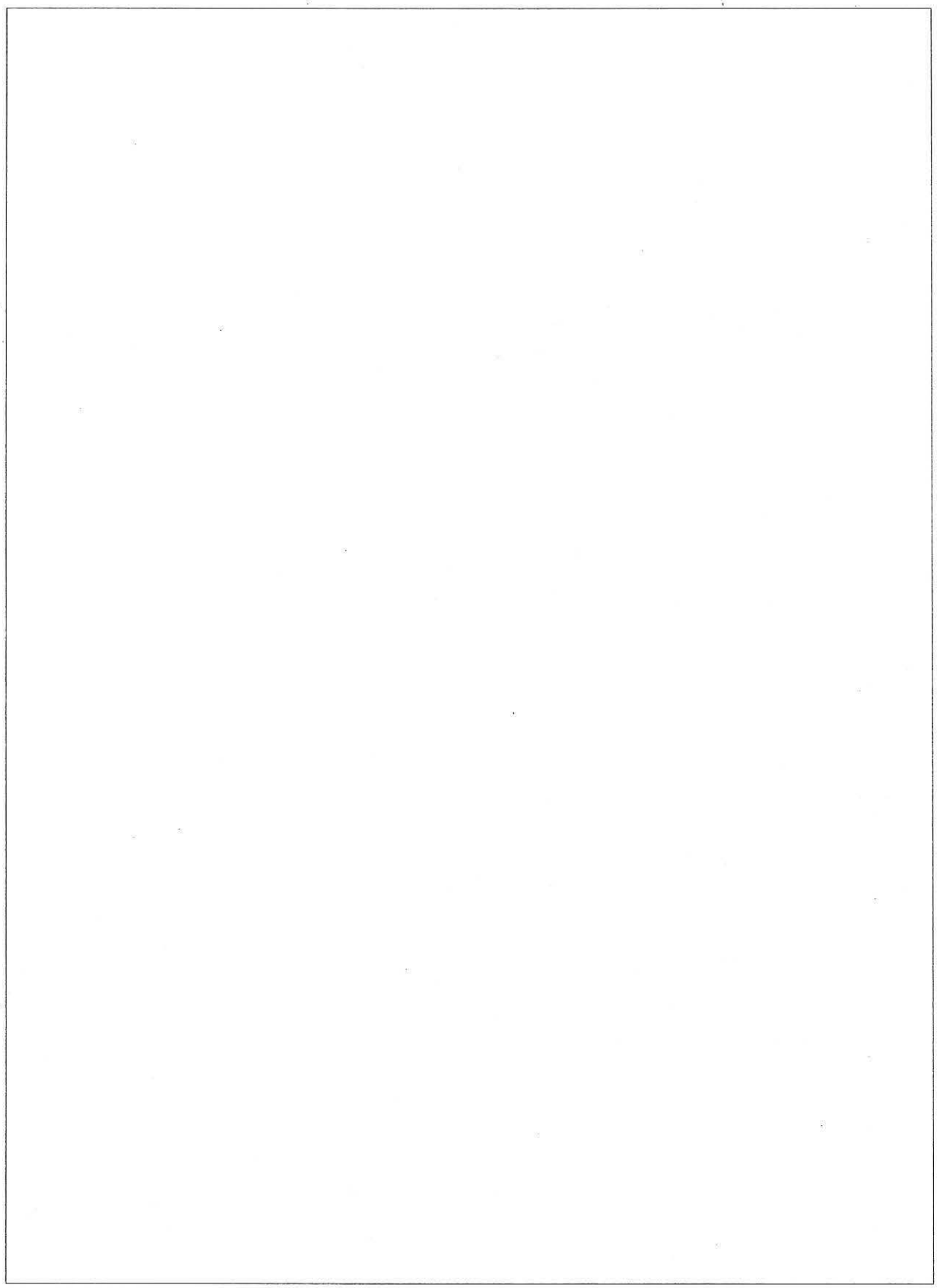
With respect to what CIA does with the information after it is collected: The general rule is, if it was properly collected, we may generally keep it, but ... information identifying US Persons must be excised as much as feasible without making the information useless. I'll address the basic principles of minimization after we talk about collecting the information in the first place.

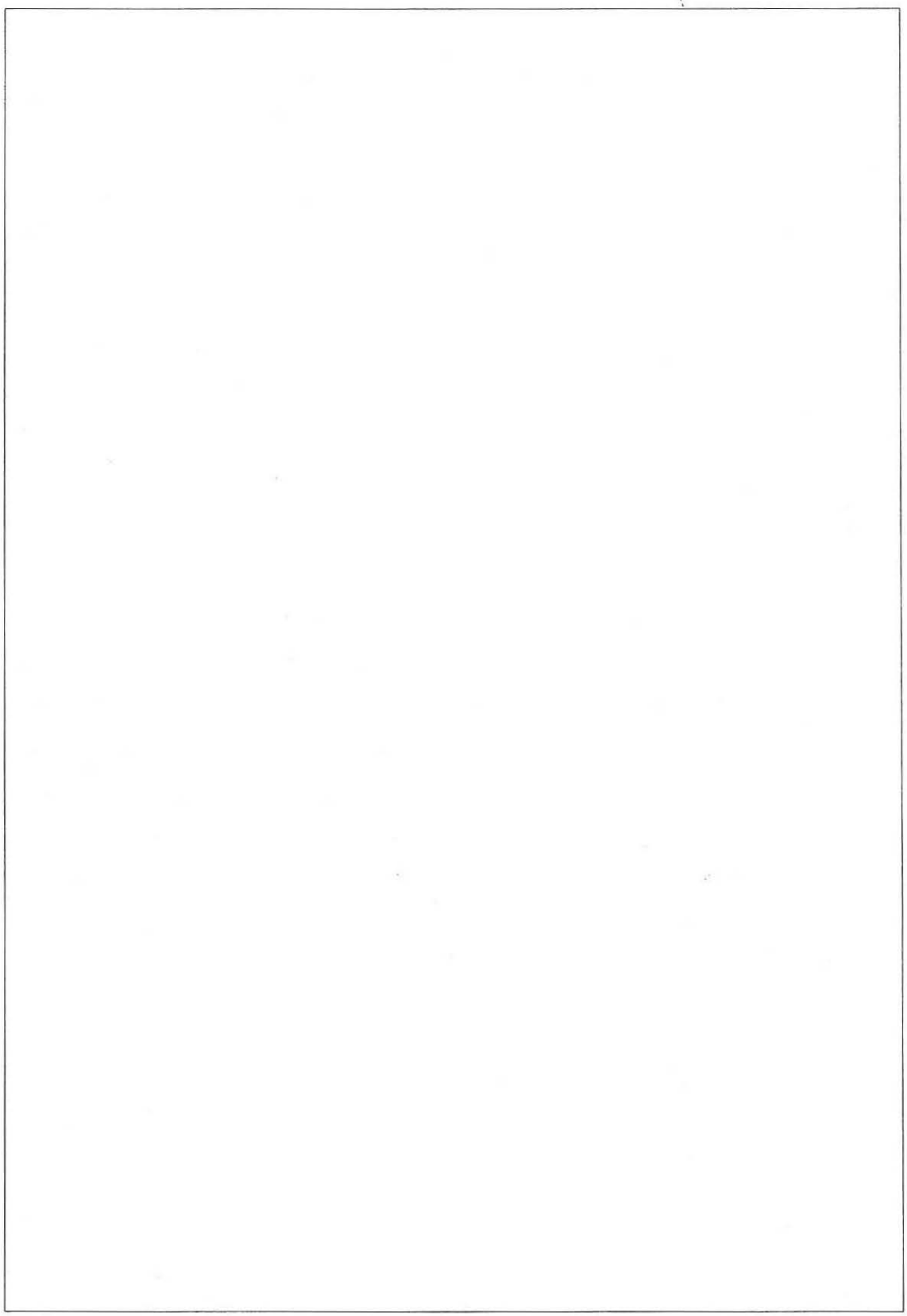
[redacted] (b)(1) (b)(3) NatSecAct

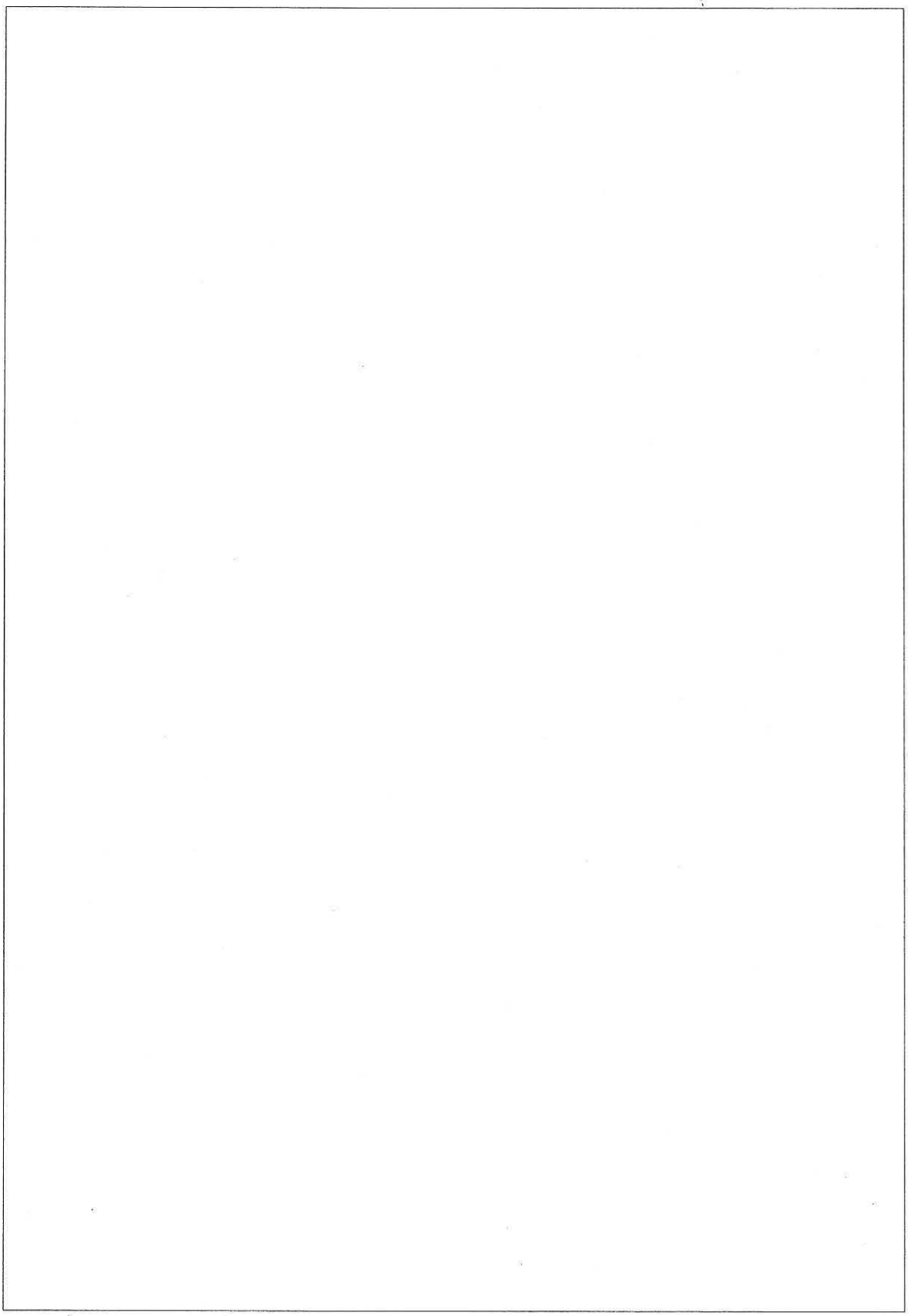


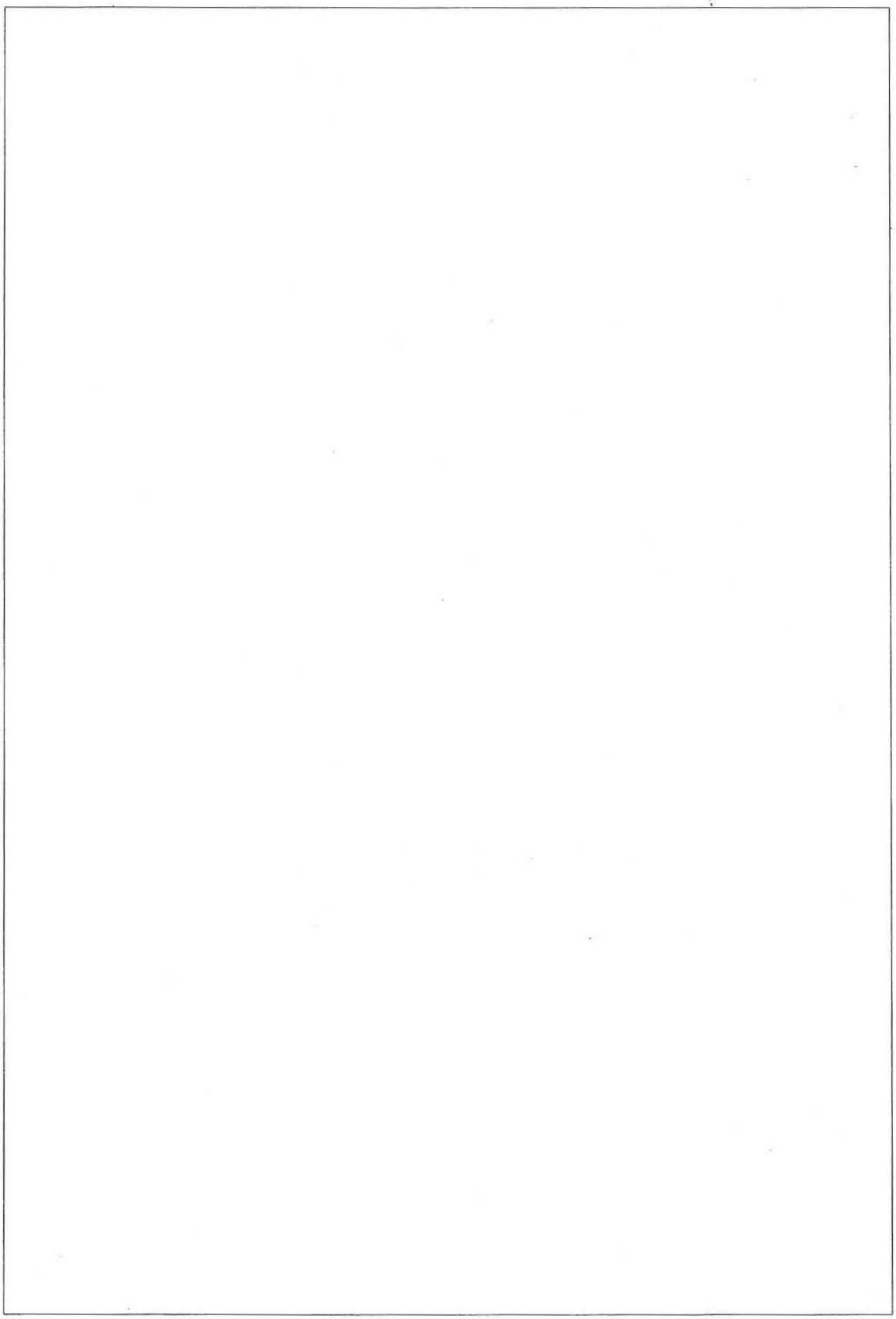












III. ***Rules for Retention and Dissemination of Information Concerning US Persons*** (AIUO) (*Annex A, § VI; Annex B, § VI; Appendix D to Annexes A and B.*)

A. (S) Overall general rules for retention and dissemination:

- Generally, if the Agency may collect it, it may keep it. But we may not disseminate identifying information about USPs outside the Agency unless the intelligence information is not meaningful without it.

Identity of a USP may be retained and disseminated along with the information about the USP if the information qualifies for retention under the AG procedures (usually, that means if the information is FI) and the identity is necessary (or it is reasonably believed to be necessary) to understand or assess the associated information. May retain and disseminate USP info to authorized recipients if it amounts to FI or CI or falls into another category in VI.A. of Annex A, [redacted]

(b)(1)
(b)(3) NatSecAct

The extent to which USP information can be kept around and/or disclosed depends in part on the purpose for which the intelligence is to be used. The USP-specific information in a body of data or an intelligence report might not be necessary for that purpose. And if it isn't, we don't disseminate it.

(b)(1)
(b)(3) NatSecAct

- Information collected may be retained for a reasonable period to determine whether it meets standards for retention.
- [redacted]
- The retention/dissemination rules are the same whether the information was acquired within or outside the U.S. (*see HR 7-1a(5)(b)).*

[redacted]

(b)(1)
(b)(3) NatSecAct

- Administrative justification: (1) needed for purposes of oversight, accountability or redress, (2) relevant to an administrative, civil, or criminal proceeding or investigation, (3) required by law to be retained, or (4) necessary to determine whether requirements of these procedures are satisfied.
- Secret meaning: the information is suspected or known to be enciphered or to contain a secret meaning.
- DJ-review catchall: retention is necessary to a lawful activity of the US and the General Counsel, in consultation with the Department of Justice, determines that such retention is lawful.
- Retention is necessary to determine whether the information falls within one of the foregoing categories. (This reason may justify retention for a reasonable period of time, not indefinitely.)

(b)(1)
(b)(3) NatSecAct

C. [redacted] Dissemination

Once it is determined the information may be retained, as above, it may be disseminated:

- Within the Agency on need-to-know basis (to employees, contractors, assets).
- To another IC agency to determine whether it may be retained under its rules. (Each Agency in the intelligence community has minimization rules; each Agency is responsible for following its own requirements and procedures.)
- To recipients listed in Annex A, VI.A.2. a-h. [redacted]

(b)(1)
(b)(3) NatSecAct

[redacted]

- The GC, in consultation with DoJ, may approve dissemination to other recipients if it is necessary to a lawful activity of the U.S.
- The identification of the US Person may be disseminated along with the information about him if the identity is necessary (or it is reasonably believed it may become necessary) to understand or assess the information.

D. [redacted] Retention or Dissemination

(b)(1)
(b)(3) NatSecAct

- Requirements are contained in Appendix D to Annexes A and B to HR 7-1.
- General rule: USP information derived from electronic surveillance may be retained and disseminated if the identity of the USP and all personally identifiable information are deleted. If identifying information is necessary to understand or assess the information (or it is reasonably believed that it may become necessary), it may be retained or disseminated if it meets any of 14 conditions listed in Appendix D1. The most common justification is that the information is FI or CI. Others include [redacted] information regarding criminal activity (b)(1) anything threatening the safety of a person or intelligence agency, and (b)(3) NatSecAct information needed to determine how it or related information must be handled.

- USP information that does not meet one or more of the criteria in Appendix D must be destroyed.
- [redacted]

(b)(3) CIAAct

E. (S) Additional Policy Cautions [redacted]

(b)(1)
(b)(3) NatSecAct

[redacted]

Additional requirements that apply to requests from any other Executive Brance officials to the Agency for US Person information include:

- Purpose and Authority for Request: If an Agency employee is unclear regarding the legitimacy or propriety of a request, the employee must inquire into the purpose of the request and the requester's authority to receive the information.
- Documentation: All requests from outside CIA for dissemination of US person information must be documented in Agency record systems.
- Sourcing: Responses to requests for US person information shall bear appropriate caveats as to the relative reliability and general sourcing of the data (*e.g., "unsubstantiated information derived from publicly available documentation"*).
- Unusual or Sensitive Requests: If a request appears to be unusual, particularly sensitive, for an inordinate purpose, or from an individual of questionable authorization, the request must be referred to a senior Agency manager for resolution (as set out in AN 7-1-39). [redacted]

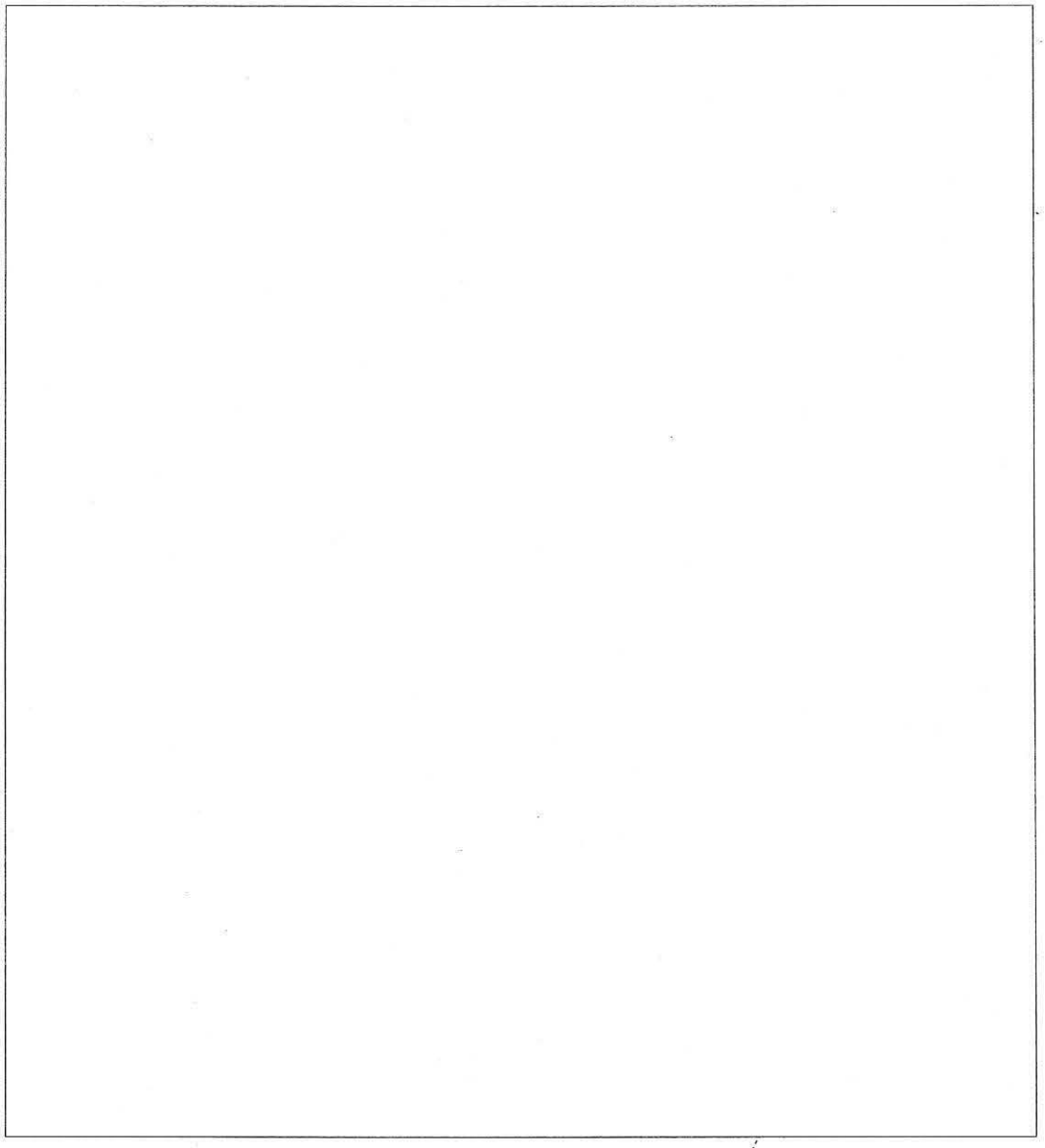
(b)(1)
(b)(3) NatSecAct

[redacted]

F. [redacted]

(b)(3) NatSecAct

- [redacted]



(b)(1)
(b)(3) NatSecAct

STUDENT OUTLINE FOR OGCU TRAINING MODULE INSERT:
EXPLORATION of USP COLLECTION/RETENTION/DISSEMINATION ISSUES

Collection, Retention and Dissemination of US Person Information

I. ***Overview: Primary Sources and Fundamental Collection/Retention Principles***

A. References/sources of rules: (b)(1) (b)(3) NatSecAct

Constitution of the United States, Fourth Amendment; Executive Order 12333; HR 7-1a(4)(b)-(c), (5)(b)-(d), Annex A, Annex B, Appendix D; AN 7-1-39;

[redacted]

B. Basic Principles for US Person Information

- Ask "who?" and "where?": the restrictions generally apply to collection against US Persons anywhere and against any collection in the U.S.
- Can only collect foreign intelligence (FI, CI, CP, foreign aspects of drug trafficking, international terrorists)
- Must use least intrusive means available.
- Can't ask another [redacted] to collect what you cannot.
- Once you have it, you may generally keep it, but ...
- Information identifying US Persons must be excised as much as feasible without making the information useless.

(b)(1) (b)(3) NatSecAct

The domestic activities of US persons are outside CIA's mandate and authority.

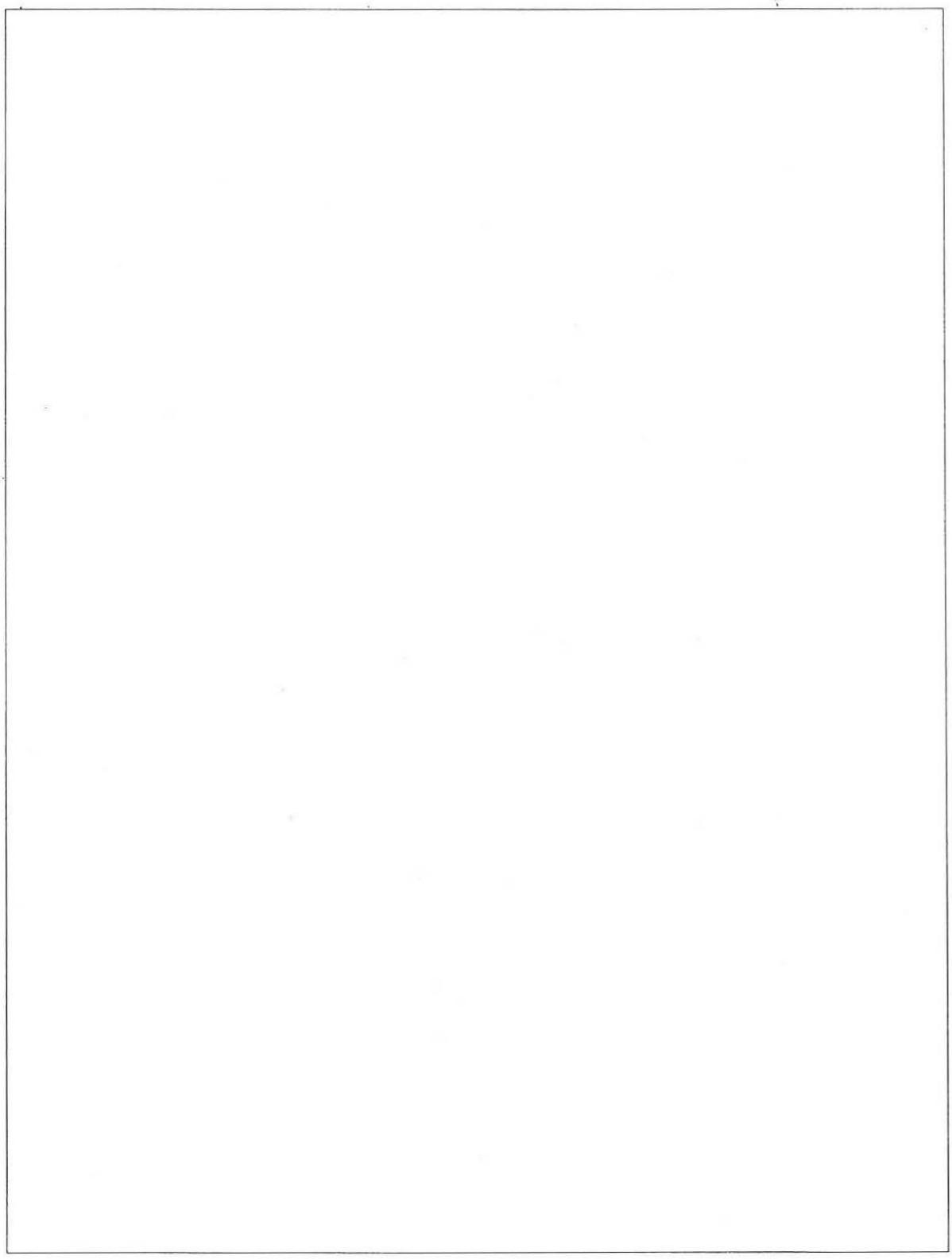
[redacted] (b)(1) (b)(3) NatSecAct

[redacted]

(b)(1) (b)(3) NatSecAct

OGCU 2003
9/24/03

COPY



OGCU 2003
9/24/03

COPY

D. Emergency Rules (*See Annex A, § IV.E; Annex B, § IV.E.*)

An "emergency" is when a person's life or physical safety is reasonably believed to be in imminent danger *or* if approval time would cause failure to obtain significant intelligence.

III. *Rules for Retention and Dissemination of Information Concerning US Persons*
(*Annex A, § VI; Annex B, § VI; Appendix D to Annexes A and B.*)

A. Overall general rules for retention and dissemination:

- Generally, if you may collect it, you may keep it.
- Information collected may be retained for a reasonable period to determine whether it meets standards for retention.
- Identity of a USP may be retained and disseminated along with the information about the USP if the information qualifies for retention under the AG procedures and the identity is necessary (or it is reasonably believed to be necessary) to understand or assess the associated information.

- [redacted]
- The retention/dissemination rules are the same whether the information was acquired within or outside the U.S. (*see HR 7-1a(5)(b)).*

May retain and disseminate USP info to authorized recipients if it amounts to FI or CI or falls into another category in VI.A. of Annex A, which distinguishes between information that is and is not derived from special collection techniques. (b)(1) (b)(3) NatSecAct

B. Information Not Derived from Special Collection: Retention

US Person information may be retained if one or more of these descriptors applies:

- Publicly available, consensual, or identifying information (i.e., basic collection) may be retained.
- Foreign intelligence or counterintelligence; concerns international narcotics activities; needed to protect safety of persons or organizations; needed to protect sources and methods ; concerning security (of personnel, facilities or things, communications); from overhead reconnaissance; concerning possible illegal activity; necessary for administrative purposes. (b)(1) (b)(3) NatSecAct
- Concerns potential sources or contacts [redacted]
- Retained in such a manner that it cannot be retrieved by reference to the person's name or other identifying data. (b)(1) (b)(3) NatSecAct
- Minimized: processed to delete identity of USP to greatest extent possible without losing meaning. [redacted]
- Administrative justification: (1) needed for purposes of oversight, accountability or redress, (2) relevant to an administrative, civil, or criminal proceeding or investigation, (3) required by law to be retained, or (4) necessary to determine whether requirements of these procedures are satisfied. (b)(1) (b)(3) NatSecAct
- [redacted]
- DJ-review catchall: retention is necessary to a lawful activity of the US and the General Counsel, in consultation with the Department of Justice, determines that such retention is lawful.
- Retention is necessary to determine whether the information falls within one of the foregoing categories. (This reason may justify retention for a reasonable period of time, not indefinitely.)

C. Information Not From Special Collection: Dissemination

Once it is determined the information may be retained, as above, it may be disseminated:

- Within Agency on need-to-know basis.
- To another IC agency to determine whether it may be retained under its rules.
- To recipients listed in Annex A, VI.A.2. a-h. Inside USG, dissemination is usually okay if reasonably necessary for government purpose; outside USG it is more restricted. The GC, in consultation with DoJ, may approve dissemination to other recipients if it is necessary to a lawful activity of the U.S.
- The identification of the US Person may be disseminated along with the information about him if the identity is necessary (or it is reasonably believed it may become necessary) to understand or assess the information.

D. Information Derived from Special Collection: Retention or Dissemination (b)(1) (b)(3) NatSecAct

- Requirements are contained in Appendix D to Annexes A and B.
- General rule: USP information derived from electronic surveillance may be retained and disseminated if the identity of the USP and all personally identifiable information are deleted. If identifying information is necessary to understand or assess the information (or it is reasonably believed that it may become necessary), it may be retained or disseminated if it meets any of 14 conditions listed in Appendix D1. The most common justification is that the information is FI or CI. Others include [redacted] information regarding criminal activity or anything threatening the safety of a person or intelligence agency, and information needed to determine how it or related information must be handled.
- USP information that does not meet the criteria above must be destroyed.

[redacted]

(b)(1)
(b)(3) NatSecAct

E. Additional Policy Cautions [redacted] (b)(3) CIAAct

[redacted] additional requirements were added as a matter of policy. These relate to ensuring that an official who requests information is in fact an authorized recipient (which might dictate an inquiry into the purpose for the request) and reducing the likelihood that dissemination of unreliable information might cause unnecessary harm to a US person. Additional requirements that apply to requests to the Agency for US Person information include:

- Purpose and Authority for Request: If an Agency employee is unclear regarding the legitimacy or propriety of a request, the employee must inquire into the purpose of the request and the requester's authority to receive the information.

(b)(1)
(b)(3) NatSecAct

- Documentation: All requests from outside CIA for dissemination of US person information must be documented in Agency record systems.
- Sourcing: Responses to requests for US person information shall bear appropriate caveats as to the relative reliability and general sourcing of the data (*e.g., "unsubstantiated information derived from publicly available documentation"*).
- Unusual or Sensitive Requests: If a request appears to be unusual, particularly sensitive, for an inordinate purpose, or from an individual of questionable authorization, the request must be referred to a senior Agency manager for resolution (as set out in AN 7-1-39).

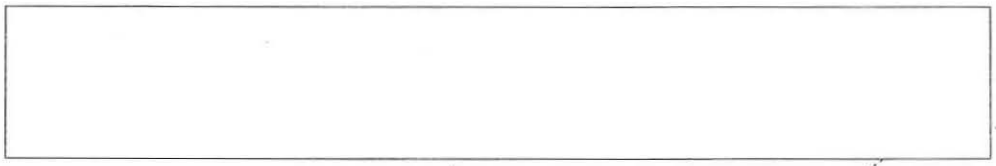
(b)(1)
(b)(3) NatSecAct

[redacted]

(b)(1)
(b)(3) NatSecAct

OGCU 2003
9/24/03

COPY



(b)(1)
(b)(3) NatSecAct

OGCU 2003
9/24/03

COPY