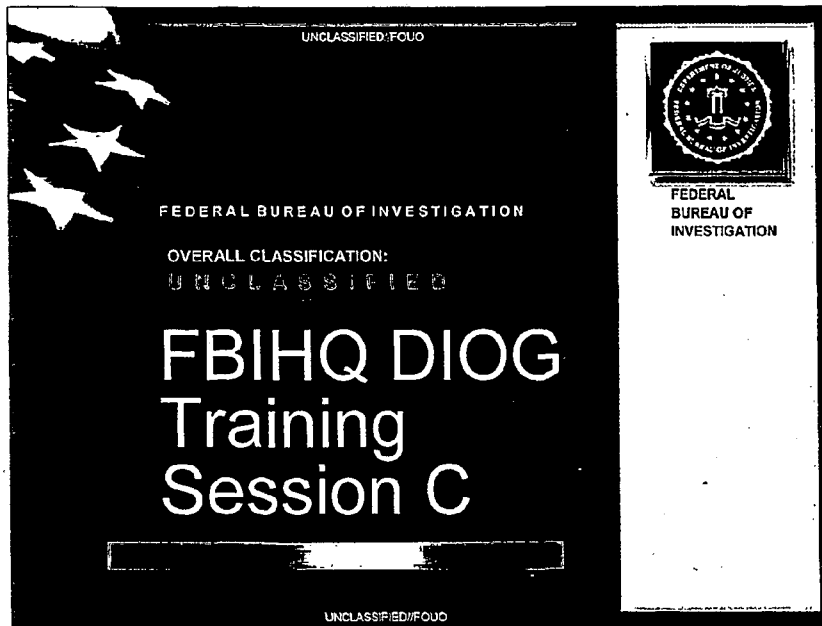






UNCLASSIFIED//FOUO

DIOG Section 5: Assessments

A new type of activity formed by combining:

- "Threat assessments" from the former AGG for FBI National Security Investigations and Foreign Intelligence Collection
- The "prompt and extremely limited checking of initial leads" allowed under the former AGG on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations

Assessment activities:

- Must always be based on an authorized purpose
- Require specific work flows for management and documentation (FD-71, Assessment Files,)

b7E

UNCLASSIFIED//FOUO

2



UNCLASSIFIED//FCUO

DIOG Section 5: Assessments

Before initiating or approving an assessment, an FBI employee or approving official must determine whether:

- An authorized purpose and objective exists to conduct the assessment
- The assessment is based on factors other than the exercise of First Amendment activities or the race, ethnicity, national origin or religion of the subject
- The assessment is an appropriate use of personnel and financial resources

UNCLASSIFIED//FOUO

3



UNCLASSIFIED//FOUO

DIOG Section 5: Assessments

FIRST AMENDMENT RIGHTS:

Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An assessment may not be initiated based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an assessment would be appropriate

UNCLASSIFIED//FOUO

4



UNCLASSIFIED//FOUO

DIOG Section 5: Type 1 and 2 Assessments

Investigative Methods in Type 1 and 2 Assessments require higher supervisory approval:

- Physical surveillance
- Certain interviews
- Tasking CHSs

UNCLASSIFIED//FOUO

5



UNCLASSIFIED//FOUO

DIOG Section 5: Type 1 and 2 Assessments

Investigation	Purpose	Duction	Documentation	Approval	Judication/Review	SM	Responsible Entity
Type 1	Activities constituting violations of federal criminal law or threats to the national security	As log as necessary to achieve purpose and objectives/Not in Int	SI, SI, or GARDEN	Any employee can Initiate; SS And IA Approval	Every 30 days	CDC or SAC approval	Investigative Squad
Type 2	The involvement of individuals, groups, or organizations (such as victims of labor)						

b7E

UNCLASSIFIED//FOUO

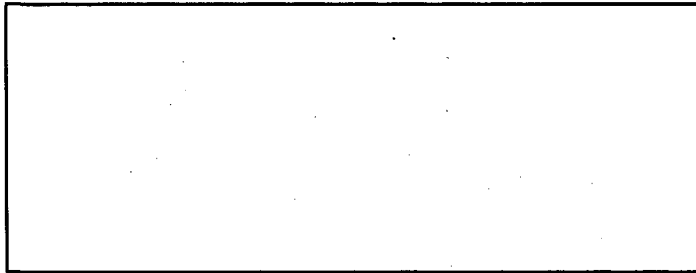
As of May 19, 2009

6



UNCLASSIFIED//FOUO

DIOG Section 5: Type 1 and 2 Assessment Example



b7E

- What would you do with this information?

UNCLASSIFIED//FOUO

7

Teaching Point: Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An assessment may not be initiated based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an assessment would be appropriate. DIOG 5.3

Assessments may not be initiated based solely on the exercise of 1st Amendment rights. People have the fundamental right to actively recruit others to join their cause as long as it's lawful activity. No investigative activity, including preliminary investigations, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject. DIOG 5.1

If this information is entered into Guardian, is there anything else that could be done with it before closing it? If appropriate and there is a purpose for doing so, e.g., the employee wants to know more about the son who sent the email, an FBI employee could conduct internal (FBI) or other U.S. Government database checks to which they have access without opening an assessment.

Does it matter how old the son is? Yes, this can be considered as a factor in the evaluation of the facts. Can they the mother be re-contacted for additional information without opening an assessment? Yes, clarifying interviews that stay within the confines the original complaint may be conducted without opening an assessment.

b7E

DIOG 5.1 An FBI employee can search historical information already contained within: (i) FBI data systems; (ii) United States Intelligence Community (USIC) systems to which an FBI employee has access (e.g., [redacted]); (iii) any other United States Government database to which an FBI employee has access; and (iv) the FBI employee can also conduct open-source internet searches without initiating an assessment (open-source internet searches do not include any paid-for-service databases such as Lexis-Nexis and ChoicePoint). This allows the FBI employee to possibly resolve a matter without the need to conduct new investigative activity or open an assessment. However, the use of paid-for-service databases cannot be accessed before initiating an assessment or a predicated investigation.

If these systems and the open Internet are checked and no additional information is developed, the Guardian entry should not be assigned by the SSA (which would make this matter an Assessment). The Guardian entry, along with the negative database and/or internet checks should be placed in an unassigned/deleted category.

7

UNCLASSIFIED//FOUO



DIOG Section 5: Type 1 and 2 Assessment Example

- What can the agent do with this information?

UNCLASSIFIED//FOUO 8

b7E

Teaching Point: Type 1 Assessments are initiated when we are seeking information proactively or in response to other information constituting federal criminal activity or threats to the national security. In order to initiate a Type 1 Assessment you must have an authorized purpose and a clearly stated investigative objective; it must be based on factors other than 1st Amendment activities, race, ethnicity, national origin or religion; and the assessment must be an appropriate use of personnel and financial resources. Type 1 and 2 Assessments do not require prior SSA approval to initiate.

DIOG 5.1 Although "no particular factual predication" is required, the basis of an assessment cannot be arbitrary or groundless speculation nor can an assessment be based solely on the exercise of First Amendment protected activities.

b7E



UNCLASSIFIED//FOUO

DIOG Section 5: Type 1 and 2 Assessment Example

- What action will you take?

b7E

UNCLASSIFIED//FOUO

9

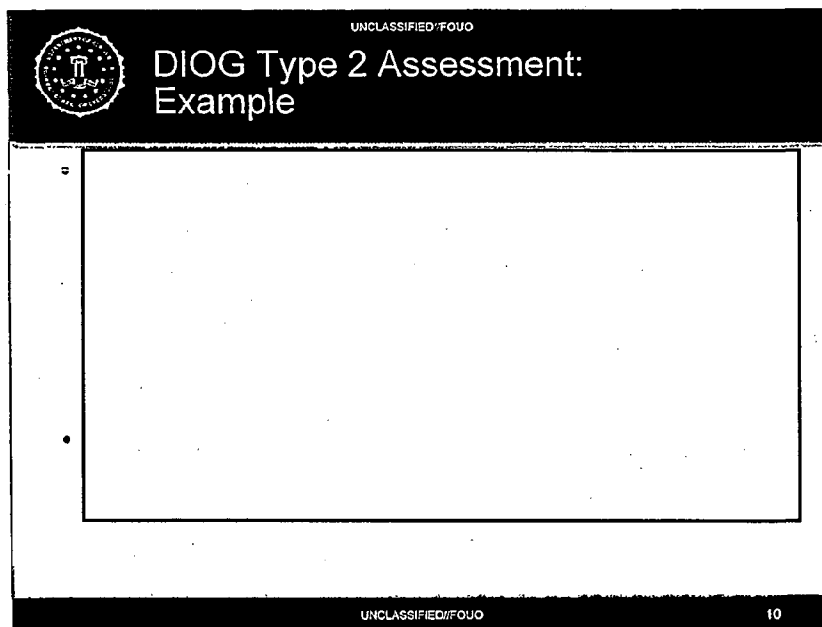
Teaching Point: Type 2 Assessments are opened when we are seeking information proactively or in response to other information relating to the role of individuals, groups, or organizations in criminal activities or threats to the national security. In order to initiate a Type 2 Assessment you must have an authorized purpose and a clearly stated investigative objective; it must be based on factors other than First Amendment Activities, race, ethnicity, national origin or religion; the assessment is an appropriate use of personnel and financial resources. Type 1 and 2 Assessments do not require prior SSA approval to initiate.

b7E

DIOG 5.6 A 1, 2

Based on the reliability of the source, you may consider opening a PI.

9



b7E

Teaching Points: You do not have to start with the initiation of an Assessment. The facts can warrant the opening of a predicated investigation, (either Preliminary or Full Investigation). Additionally, The facts of each case dictate the type of investigation you initiate as well as the methods of investigation. Is T&T an appropriate method under these circumstances? The least intrusive means standard is required by the AGG-DOM and **DIOG 4.4.A**, it requires that the "least intrusive" means or method be considered and, if operationally sound and effective, used to obtain intelligence or evidence in lieu of a more intrusive method. In this case, a more intrusive method may be needed based on the seriousness of the criminal activity and the potential harm to the victim. In this example, the intrusiveness question does not really come into play if the parents consented to the pen register.

An emergency pen register must be approved by DOJ.

DIOG 11.11.4 B.3 If approval has not been obtained within 48 hours the installation of the pen register/trap and trace must be terminated.

In this particular investigation, there were indicators that that teacher and student left the state, which invokes the federal nexus.



UNCLASSIFIED//FOUO

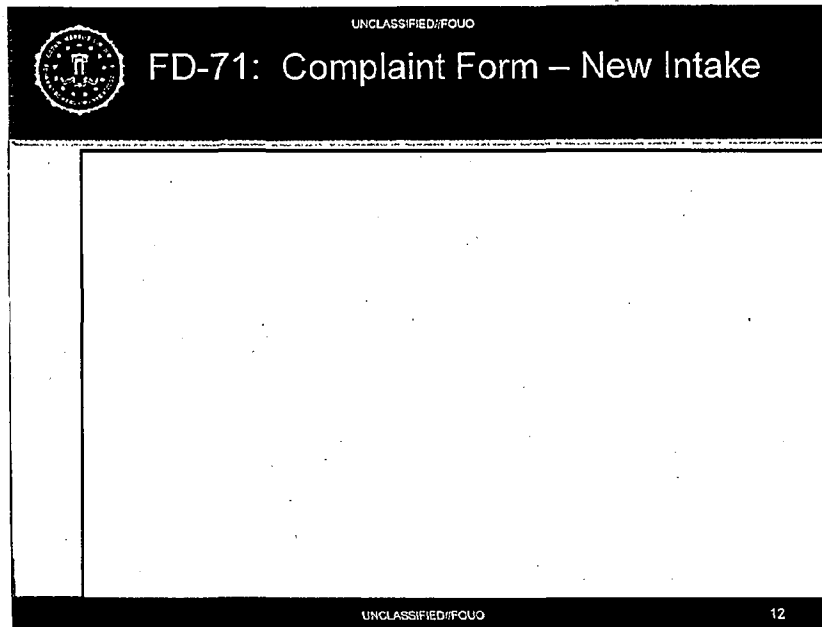
FD-71: Complaint Form – Updates

- Current version of the form: FD-71 v1.4: dated 3/10/2009
- V1.4 has major changes to:
 - SIM process
 - Supervisor decisions
 - Information dissemination
- Changes or new features are highlighted in this presentation with orange text boxes

UNCLASSIFIED//FOUO

11

Teaching Point: The FD-71 must be used for initiating all Type 1 & 2 assessments involving criminal or counterintelligence matters. National security related threats (CT, WMD, DT, Cyber) use Guardian to document the threat information.



UNCLASSIFIED//FOUO

FD-71: Complaint Form – New Intake

UNCLASSIFIED//FOUO 12

b7E

Teaching Point: The link to the FD-71 is located on the DIOG web page. This page also contains a user guide with step-by-step instructions on how to use the FD-71 and an FAQ section.

The FD-71 is an InfoPath form created in SharePoint. The data fields used in the FD-71 are searchable in the FD-71 SharePoint database.

UNCLASSIFIED//FOUO

 FD-71: Complaint Form – Intake

13

b7E

Teaching Point: This is the look and feel of the InfoPath forms. These type of forms and the work flow will be integrated into Sentinel in the future.



UNCLASSIFIED FOUO

FD-71: Complaint Form – Intake

--	--

b7E

14



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Intake

[Redacted Content]

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Intake

[Redacted content]

UNCLASSIFIED//FOUO

16

b7E





UNCLASSIFIED//FOUO

FD-71: Complaint Form – Intake

[Redacted content]

b7E...

UNCLASSIFIED//FOUO

 FD-71: Complaint Form - 

--	--	--

UNCLASSIFIED//FOUO 19

b7E

UNCLASSIFIED//FOUO

 FD-71: Complaint Form — 

UNCLASSIFIED//FOUO 20

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Intake

[Redacted Content]

UNCLASSIFIED//FOUO

b7E



UNCLASSIFIED FOUO

FD-71: Complaint Form – Intake

[Redacted Content]

b7E

UNCLASSIFIED//FOUO

 FD-71: Complaint Form – Intake

UNCLASSIFIED//FOUO 23

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Review

--

UNCLASSIFIED//FOUO

24

b7E



b7E

UNCLASSIFIED//FOUO

25



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Decision

--	--

27

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Decision

--	--

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Decision

--	--

b7E

29



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Intake

[Redacted Content]

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Decision

--

UNCLASSIFIED//FOUO

31

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Decision

[Redacted content]

32

b7E



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Decision

--	--	--

b7E

33



UNCLASSIFIED//FOUO

FD-71: Complaint Form – Supervisor Decision

--

UNCLASSIFIED//FOUO

34

b7E



UNCLASSIFIED//FOUO

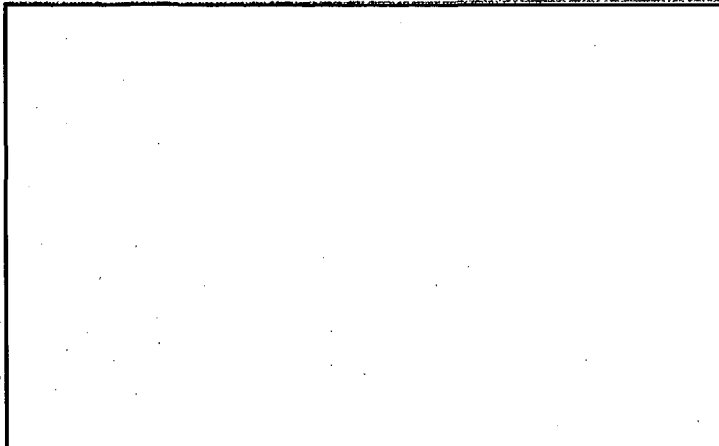
FD-71: Complaint Form – Indexing

[Redacted Content]

b7E

UNCLASSIFIED//FOUO

35



UNCLASSIFIED//FOUO

36

b7E



UNCLASSIFIED//FOUO

AGG DOM and Guardian

Guardian has been modified to coordinate with the 12/1/08 implementation of the new Attorney General Guidelines for Domestic FBI Operations (AGG-Dom)

There have been four changes in Guardian:



b7E

Guardian incidents once assigned with an authorized purpose and objective are considered



UNCLASSIFIED//FOUO

37

Teaching Point: [Redacted] It should be stressed once a Guardian incident is assigned an authorized purpose and objective, it is considered a [Redacted] Matters not assigned are not considered Assessments.

b7E

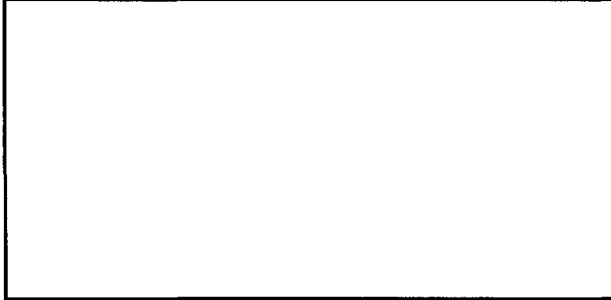


UNCLASSIFIED//FOUO

Guardian Policy

Information NOT permitted in Guardian:

-
-
-
-
-
-



b7E

UNCLASSIFIED//FOUO

38

Teaching Point: This is a reinforcement of existing Guardian policy



b7E

UNCLASSIFIED//FOUO

 Guardian:
Supervisor Oversight

 GUARDIAN TRAINING

Mail
Guardian Help D

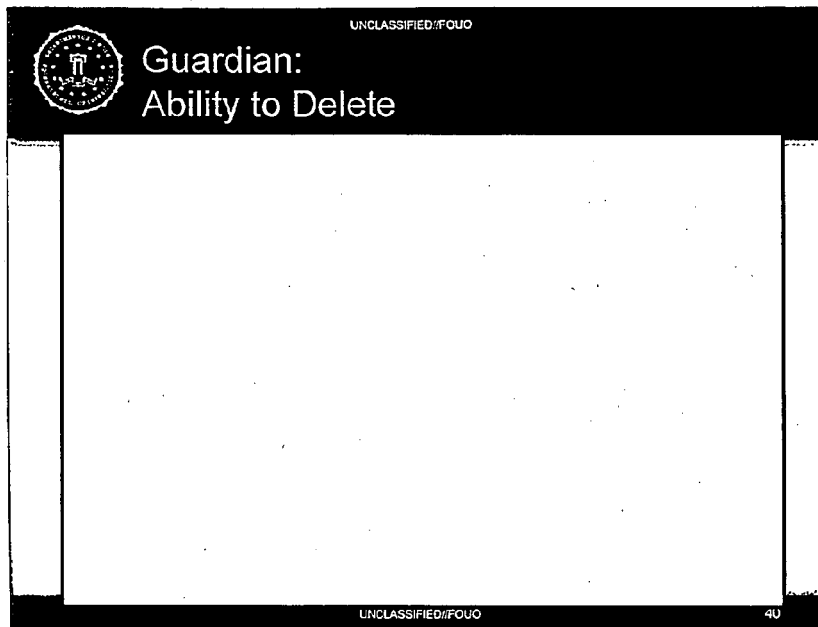
Logout Home My Account Help

UNCLASSIFIED//FOUO 39

b7E

Teaching Point

b7E



b7E

Teaching Point

Guardian Help Line

b7E



UNCLASSIFIED//FOUO

Guardian: Sensitive Investigative Matters

- Investigations and Assessments are deemed "Sensitive Investigative Matters (SIMs)" when they involve activities of:
 - A domestic public official (involving corruption or national security threat)
 - A political candidate (involving corruption or national security threat)
 - A religious or political organization, or individual prominent in such
 - News media
 - Matters having an academic nexus
 - Any other matter which should be brought to the attention of FBIHQ or DOJ, in the judgment of authorizing official
- SIMs Require Chief Division Counsel (CDC) review, SAC approval and notice to appropriate HQ Section/Unit

UNCLASSIFIED//FOUO

41

Teaching Point: Regarding the first change in Guardian, here is a reminder of what constitutes a Sensitive Investigative Matter.



b7E

Teaching Point:

It is planned that "SAC approval" will be added to this language.

b7E



UNCLASSIFIED//FOUO

Guardian: Incident Notes

[Redacted content]

UNCLASSIFIED//FOUO

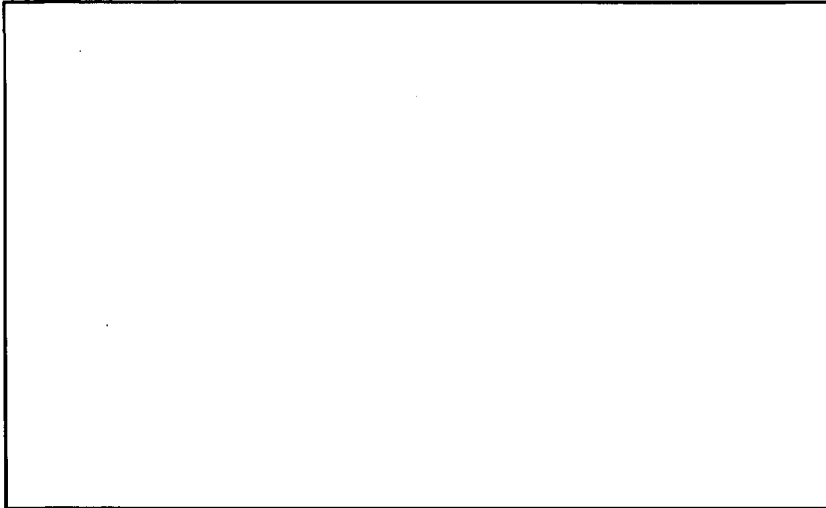
43

b7E

Teaching Point

[Redacted content]

b7E



UNCLASSIFIED//FOUO

44

b7E

Teaching Point

[Redacted]

[Redacted] These are the only investigative methods approved for use during an Assessment.



UNCLASSIFIED//FOUO

Guardian: FGJ Subpoenas

The results from a FGJS can be placed in a note in Guardian, as long as the information is not attributed to the Grand Jury

Usage:

Add a note to the incident and choose the method "FGJS for...subscriber information" to document that a subpoena is being sought

Example note:

b7E

UNCLASSIFIED//FOUO

45

Teaching Point: As a special note regarding the Investigative Methods change, a narrow category of Federal Grand Jury Subpoenas are now approved for use during an Assessment. 

b7E



UNCLASSIFIED//FOUO

Guardian: FGJ Subpoenas

When the results come back, add a new note to the incident and choose the method "Administrative note for informational purposes" and simply state the results. Do not refer to the FGJS

Example note:

b7E

UNCLASSIFIED//FOUO

46

Teaching Point: As a special note regarding the Investigative Methods change, a narrow category of Federal Grand Jury Subpoenas are now approved for use during an Assessment.

b7E

UNCLASSIFIED//FOUO



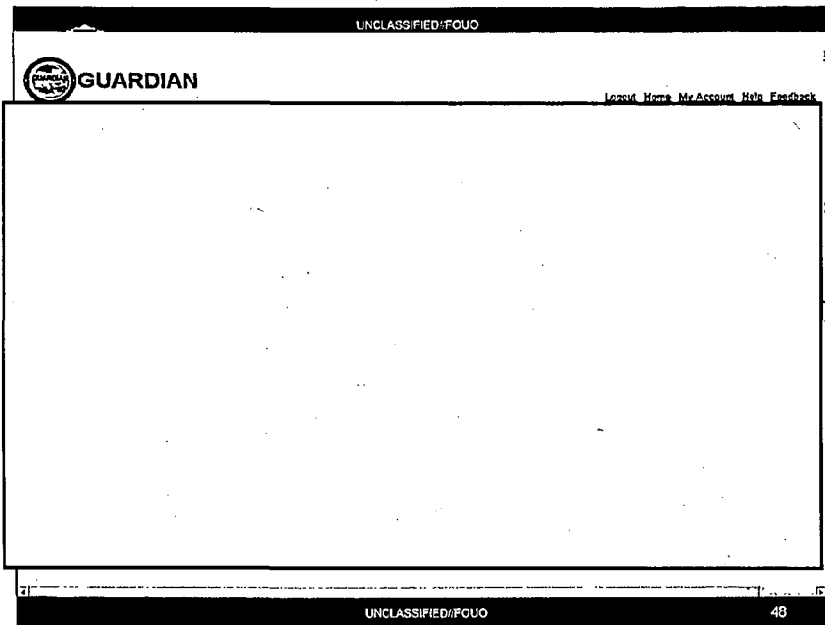
Guardian:
Disposition of Incidents

UNCLASSIFIED//FOUO 47

b7E

Teaching Point: The last two changes in Guardian

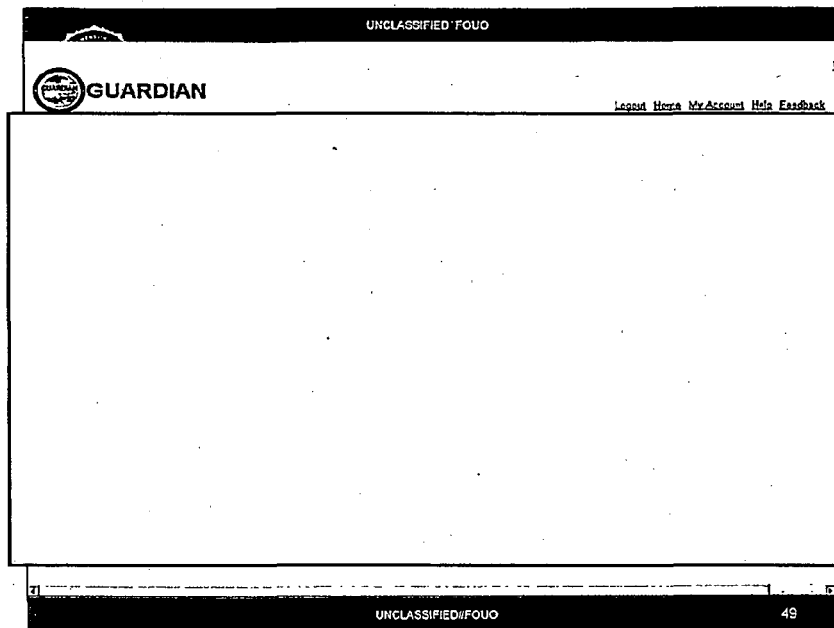
b7E



b7E

Teaching Point

b7E



b7E

Teaching Point

The user must choose the subtitle to which the FD-71(a) will upload corresponding to which group is involved in the incident. If no group was identified

b7E



UNCLASSIFIED//FOUO

Type 3 Assessments

Investigation	Purpose	Duration	Documentation	Approval	Justification Review	SIM	Responsible Entity
Type 3	For all Type 3 assessments, the purpose is to determine if the entity is in compliance with the requirements of the law.	For all Type 3 assessments, the duration is 12 months.		For all Type 3 assessments, the approval is required.	For all Type 3 assessments, the justification review is required.	For all Type 3 assessments, the SIM is required.	For all Type 3 assessments, the responsible entity is the Department of Justice.

UNCLASSIFIED//FOUO

As of May 19, 2009

50

b7E

DIOG: Section 5.2 – 5.6



UNCLASSIFIED//FOUO

Type 3 Assessment: Authorized Purpose & Objective

The authorized purpose of a Type 3 assessment is to obtain information on an identified potential threat or vulnerability in your domain.

The objective is to seek answers relating to the potential threat and vulnerability [REDACTED]

[REDACTED]

b7E

UNCLASSIFIED//FOUO

51

Teaching Point: [REDACTED]

[REDACTED]

b7E



UNCLASSIFIED//FOUO

Type 3 Assessment: Key Points

- Opened based upon a potential identified threat or vulnerability
- One assessment file per threat or vulnerability identified
- Must initiate a separate assessment if active collection falls out of the purview of an open assessment or predicated case
- Incidental collection does not require opening a Type 3 assessment, but can be reported out of the case it was collected in

UNCLASSIFIED//FOUO

52

b7E

Teaching Point: Type 3 assessments require supervisory approval and an EC for opening Type 3 assessments

and Field

Office substantive operational squads or FBIHQ units can initiate Type 3 assessments.



UNCLASSIFIED//FOUO

Type 4 Assessments

Initiation	Purpose	Duration	Documentation	Approval	Justification Review	SIM	Responsibility
Type 4	Obtaining intelligence for intelligence analysis and planning	As long as necessary to achieve purpose objective to be met		SSA or SIA Approval	Every 90 days if probationary employee; every 60 days	ODD review approval	

b7E

UNCLASSIFIED//FOUO

As of May 19, 2009

53

Teaching Point: Type 4 Assessments are

b7E

Type 4 assessments require prior SSA or SIA approval and the authorized purpose and objectives documented in the opening EC.



UNCLASSIFIED//FOUO

Type 4 Assessment: Key Points

- The authorized purpose of a Type 4 assessment is to obtain information to inform or facilitate intelligence analysis and planning.



b7E

UNCLASSIFIED//FOUO

54

Teaching Point:



b7E



UNCLASSIFIED//FOUO

Type 4 Assessment: Key Points

- One file per assessment
- Must have authorized purpose and objective
- SSA/SIA approval needed to initiate
- CDC review/SAC approval for Sensitive Investigative Matters
- Subjected to 90 day file review

b7E

UNCLASSIFIED//FOUO

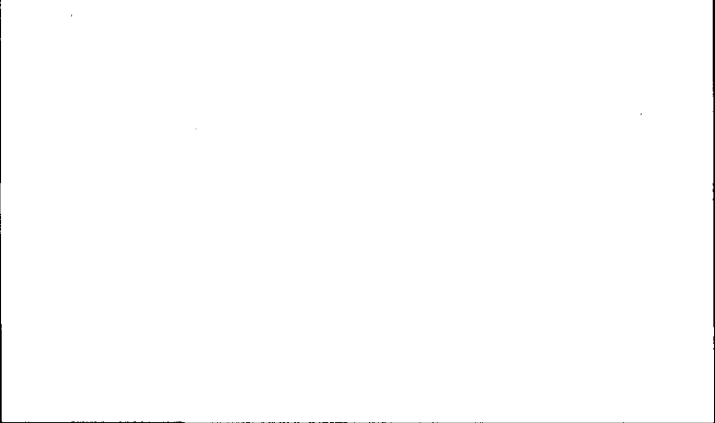
55

Teaching Point: All investigative methods authorized during assessments are permitted in Type 4 assessments.

UNCLASSIFIED//FOUO



Type 4 Assessment: Scenario



UNCLASSIFIED//FOUO 56

b7E

Teaching Point:

b7E



UNCLASSIFIED//FOUO

Type 5 Assessments

Investigator	Purpose	Division	Document No.	Approved	Justification Review	SI	Responsible
Type 5	Identify, assess, update criminal history cover capabilities GIS	CISMand AGG-GIS		CHSRand AGG-GIS	CHSRand	Not addressed in DOG, RCoInvestigative Follow GH Manual	Squad

b7E

UNCLASSIFIED//FOUO

As of May 19, 2009

57



UNCLASSIFIED//FOUO

Type 5 Assessments: Key Points

- **Two Distinct Activities**
 - Seeking information on a potential [redacted]
 - [redacted]
- **Limited techniques**
 - Th [redacted] - created for three purposes
 - Allow for an IA to do a [redacted]
 - [redacted]
 - Interim ACS solution until CHSPM is updated and approved (Difference between CHS and Type 5)
 - HUMINT Squad broad based recruitment

b7E

UNCLASSIFIED//FOUO

58

Teaching Points: On 12/3/08, "interim" policy was issued to establish the following are the only investigative methods that may currently be used in conducting Type 5 Assessments. However, the DI is working on comprehensive policy regarding the use of Type 5 Assessments in the CHS program.

1. Obtain publicly available information
2. Access/examine FBI & other DOJ records and obtain information from any FBI or DOJ personnel
3. Access and examine records maintained by and request information from other federal, state, local, tribal or foreign government entities or agencies
4. Use online services and resources (whether non-profit or commercial)
5. Interview or request information from members of the public and private entities
6. Accept information voluntarily provided by government or private entities
7. Engage in observation or surveillance not requiring a court order

UNCLASSIFIED//FOUO



Type 5 Assessments: Key Points



UNCLASSIFIED//FOUO 59

b7E

Teaching Points: On 12/3/08, "interim" policy was issued to establish the following are the only investigative methods that may currently be used in conducting Type 5 Assessments. However, the DI is working on comprehensive policy regarding the use of Type 5 Assessments in the CHS program.

1. Obtain publicly available information
2. Access/examine FBI & other DOJ records and obtain information from any FBI or DOJ personnel
3. Access and examine records maintained by and request information from other federal, state, local, tribal or foreign government entities or agencies
4. Use online services and resources (whether non-profit or commercial)
5. Interview or request information from members of the public and private entities
6. Accept information voluntarily provided by government or private entities
7. Engage in observation or surveillance not requiring a court order



UNCLASSIFIED//FOUO

DIOG Section 9: Foreign Intelligence

Investigation	Prediction	Origin	Documentation	Approval	Justification/Review	SIM	Responsibility
PFI 611	Investigate/obtain foreign intelligence that is responsive to foreign intelligence requirements	Highly relevant to the request is not a unit	EC	For D/MS notice to D/MS within 30 day	Every 90 days/ probationary employment, every 50 day	CD, B/View AS Approval; Chief of Approval	

b7E

UNCLASSIFIED//FOUO

As of May 19, 2009

60



UNCLASSIFIED//FOUO

DIOG Section 9: Foreign Intelligence

- **Foreign Intelligence** is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists."
- A **Foreign Intelligence Requirement** is a collection requirement issued by USIC and accepted by the FBI DI. Foreign Intelligence Requirements from the USIC fall into two categories which are
 - **FBI Requirements** are those that address national security issues that are within the FBI's core national security mission
 - **Positive Foreign Intelligence Requirements** are those that address the military, economic and foreign relations concerns of foreign governments, which are within FBI's responsibility as part of the USIC but are not directly related to national security concerns

UNCLASSIFIED//FOUO

61



UNCLASSIFIED//FOUO

DIOG Section 9: Foreign Intelligence

- Requirements in the first category that are accepted by the DI as "FBI Requirements" will be worked within a properly authorized Type 3 Assessment or incidental to a predicated case worked by a substantive squad.
- Foreign Intelligence Requirements that fall into the second category will be worked exclusively under case

b7E

UNCLASSIFIED//FOUO

52



UNCLASSIFIED//FOUO

DIOG Section 9: Positive Foreign Intelligence

- Positive Foreign intelligence (PFI) collection in the FBI is a requirements-based activity
- Under the AGG-Dom, there are two categories of "authorized activity" under which PFI may be collected:
 - a (non-predicated) Assessment relating to "a matter of foreign intelligence interest" responsive to FI requirements
 - a Full Investigation predicated on an FI requirement
 - *Both must be requirements-based and approved by FBIHQ DI*
- In collecting FI, the FBI will generally be guided by nationally-determined intelligence requirements, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives issued under the authority of the Director of National Intelligence

UNCLASSIFIED//FOUO

63

Teaching Point: Further explain difference between foreign intelligence and positive foreign intelligence



UNCLASSIFIED//FOUO

PFI Full Investigations

- Used when a collection capability (source) is established or positively identified.
- PFI requirement must have been accepted by the FBI as the agency with "primary" collection responsibility.
- The authorized purpose must be documented in the opening EC (see [redacted])
- Must be approved in advance by DI, CMS, CPMU - Files opened by the Field Office.
- Sensitive PFI matters require field office CDC review, SAC approval & CMS Section Chief approval.
- [redacted]
- Approval EC from CPMU will contain explicit directions regarding the approved PFI investigation title, requirement, etc.
- No duration limit for PFI full investigations.

b7E

UNCLASSIFIED//FOUO

64



UNCLASSIFIED//FOUO

Privacy Act / USPER Considerations

- Avoid identifying individuals (USPERS) in PFI files unless ID is essential to satisfy the collection requirement.
- If you must ID U.S. persons (covered by the Privacy Act) limit any/all identifying info to basic identifiers.
- If you must ID U.S. persons (covered by the Privacy Act)
- Utilize or a Type 5 assessment to record information about prospective or potential sources, etc.

b7E

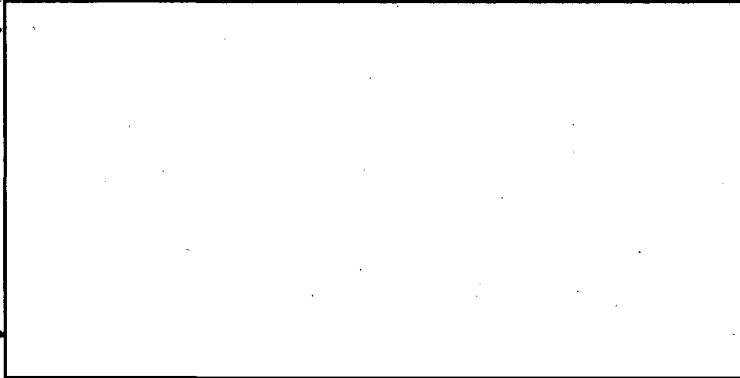
UNCLASSIFIED//FOUO

65



UNCLASSIFIED//FOUO

DIOG Section 9: Example

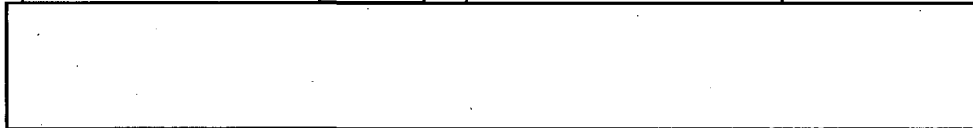


UNCLASSIFIED//FOUO

66

b7E

Teaching Point: A PFI Assessment or Full should **NOT** be opened. Although the questions are located in a [redacted] they do not fit the definition of a [redacted]



b7E

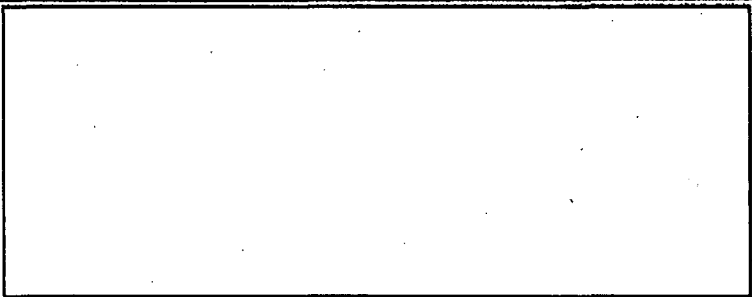
[redacted] under an Type 3 Assessment in
response to a National Requirement [redacted]

66

UNCLASSIFIED//FOUO



DIOG Section 9:
Example



UNCLASSIFIED//FOUO 67

b7E

Teaching Point: Preliminary investigations for the sole purpose of collecting positive foreign intelligence are **NOT** authorized. New York may open a full investigation.

New York may request to open either: a Type 6 Assessment, or a PFI full investigation. CPMU would approve a PFI full investigation based on NY's assertion that it has sources who are willing and able to report on the requirement.



UNCLASSIFIED//FOUO

Type 6 Assessments

Investigation	Purpose	Duration	Deauthorization	Approval	Justification/Review	SIM	Responsibility
Type 6 and FFI Assessments	Minimization of foreign intelligence information requirements	As long as necessary to achieve purpose and objective. Minimized		For SAs or SA and HQ/D approval	Every 90 days. If extraordinary, on days every 60 days	CCC Review 90 days	

b7E

UNCLASSIFIED//FOUO

As of May 19, 2009

68



UNCLASSIFIED//FOUO

Type 6 Assessments: Key Points

- Must be approved by DI/CPMU.
- PFI is FI that is not directly related to the FBI's core national security and law enforcement missions.
- If FI can fall under one of the substantive programs (IT DT CD CYB CID WMD) then it is not PFI.
- [REDACTED]
- One Type 6 assessment file per USIC Requirement
- Incidental collection does not require a Type 6 assessment opening and can be reported out of the case it was collected in
- [REDACTED]

b7E

UNCLASSIFIED//FOUO

69

Teaching Point: [REDACTED] files used for Type 6 assessments are country specific. Each assessment must have an authorized purpose documented in opening EC.

b7E

Collection priorities are primary—collecting incidental to the investigations/assessments will not be a priority.



UNCLASSIFIED//FOUO

Type 6 Assessments: Authorized Purpose and Objective

The authorized purpose of a Type 6 assessment is to obtain positive foreign intelligence that is responsive to a USIC foreign intelligence requirement that the FBI has been designated as a primary collector.

The objective is to seek answers relating to the USIC foreign intelligence requirement that the FBI has been designated as a primary collector. The objective should define the scope, time and manner to achieve the underlying purpose.

UNCLASSIFIED//FOUO

70

Teaching Point: Type 6 Assessments are used to determine whether the FBI has the ability to collect information on the approved Foreign Intelligence requirement. Once that capability has been established, a Full PFI may be approved.



UNCLASSIFIED//FOUO

DIOG Section 15: Intelligence Analysis and Planning

- **Overview:** Authority for planning and developing intelligence analysis to support the intelligence functions and missions of the FBI is incorporated in AGG-Dom, Part IV. This section elaborates upon the means by which the investigative assessments outlined in AGG-Dom, Part II are authorized for the FBI to undertake in executing its mission to discover and avert criminal threats and threats to US national security
- The term "assessment" as used within the DOJ to describe aspects of investigative activity should not be confused with the intelligence community use of the same word to describe intelligence analysis products such as an intelligence assessment

UNCLASSIFIED//FOUO

71



UNCLASSIFIED//FOUO

DIOG Section 15: Intelligence Analysis and Planning

- **Strategic Planning and Analysis:** The FBI is authorized to develop overviews and analysis of threats to and vulnerabilities of the United States and its interests in areas relative to the FBI's responsibilities. The FBI employs the following methodologies to identify, target and assess these threats:
 - Domain Management
 - Collection Management
 - Written Intelligence Products
 - Geospatial Intelligence (GEOINT)

UNCLASSIFIED//FOUO

72



UNCLASSIFIED//FOUO

DIOG Section 15: Intelligence Analysis and Planning

- **Domain Management (cont.):** Domain Management is undertaken at the Field Office and national levels. All National Domain Assessments must be coordinated in advance with the Directorate of Intelligence. All information collected for Domain Management must be documented in an
- **Collection Management:** A formal business process through which Intelligence Information Needs and Intelligence Gaps (e.g., unknowns) are expressed as Intelligence Collection Requirements (questions or statements requesting information), prioritized in a comprehensive, dynamic Intelligence Collection Plan.

b7E

UNCLASSIFIED//FOUO

73



UNCLASSIFIED//FOUO

DIOG Section 15: Intelligence Analysis and Planning

Written Intelligence Products: The FBI produces written intelligence products which represent the results of collection efforts in the field (raw intelligence) and analytic judgments made from the compilation and synthesis of relevant raw intelligence (finished intelligence).

US Person Information: Information regarding US persons is not to be included in intelligence products if the pertinent intelligence can be conveyed without including identifying information. An exception would be if the context for usage is publicly accessible information, i.e., the white powder anthrax letter addressed to Senator Tom Daschle in October 2001.

UNCLASSIFIED//FOUO

74



UNCLASSIFIED//FOUO

DIOG Section 15: Intelligence Analysis and Planning

[REDACTED]
[REDACTED] Such reporting information is typically captured in Intelligence Information Reports (IIRs), FD 302s and ECs.

b7E

[REDACTED]
the Intelligence Bulletin (IB), Intelligence Assessment (IA) and Special Event Threat Assessment (SETA). Domain Assessments and briefings can also represent finished intelligence products.

UNCLASSIFIED//FOUO

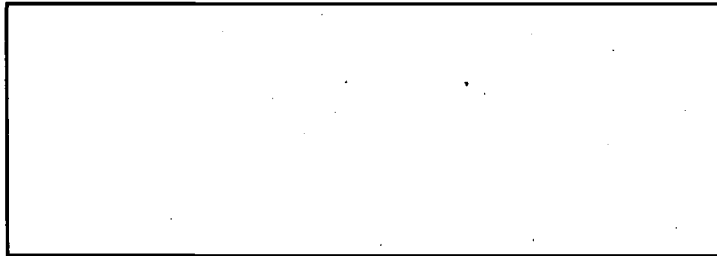
75



UNCLASSIFIED//FOUO

DIOG Section 15: Intelligence Analysis and Planning

Intelligence Systems: The FBI is authorized to operate intelligence, identification, tracking and information systems in support of authorized investigative activities or for such other additional purposes as may be legally authorized, such as intelligence tracking systems related to terrorists, gangs, or organized crime groups.



b7E

UNCLASSIFIED//FOUO

76



UNCLASSIFIED//FOUO

DIOG Section 15: Intelligence Analysis and Planning

Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically- referenced activities on the Earth. **Mapping** is an activity under GEOINT and may be used in assessments (Domain Management; Collection Management) and predicated investigations

UNCLASSIFIED//FOUO

77