U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

October 20, 2011

MS. JENNIFER LYNCH
ELECTRONIC FRONTIER FOUNDATION
454 SHOTWELL STREET
SAN FRANCISCO, CA 94110

Subject: FBI'S USE OF GEOSPATIAL TOOLS
(2009-PRESENT)

FOIPA No. 1166879- 000

Dear Ms. Lynch:

The enclosed 35 pages of documents, which are responsive to items 2, 3, and 5 of your request letter dated May 17, 2011, were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

Section 552		Section 552a
□(b)(1)	□(b)(7)(A)	□(d)(5)
☒(b)(2)	□(b)(7)(B)	□(j)(2)
□(b)(3)_____	☒(b)(7)(C)	□(k)(1)
_____	□(b)(7)(D)	□(k)(2)
_____	☒(b)(7)(E)	□(k)(3)
_____	□(b)(7)(F)	□(k)(4)
□(b)(4)	□(b)(8)	□(k)(5)
□(b)(5)	□(b)(9)	□(k)(6)
☒(b)(6)		□(k)(7)

☒ You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy, U.S. Department of Justice,1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Number assigned to your request so that it may be easily identified.

☒ See additional information which follows.

Sincerely yours,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Items 6 and 7 in your request letter are exempt from release pursuant to FOIA exemption (b)(5) [5 U.S.C. § 522 (b)(5)]. We continue to search the Central Records System for documents responsive to items 1 and 4.

Enclosure(s)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

~~Directorate of Intelligence~~
Geospatial Intelligence Unit (GIU)

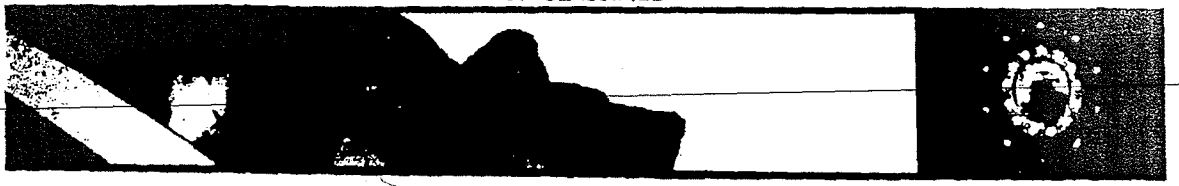
Reference Sheet for the Domestic Investigations and Operations Guide (DIOG)

This document provides a listing of particular references to Geospatial Intelligence (GEOINT) and related matters in the DIOG.[1] It is **not** a replacement for reading all relevant portions of the DIOG, nor is it legal advice. Any reader is strongly encouraged to review and comply with the DIOG in its entirety.[2] All legal questions regarding the content of the DIOG should be referred to the FBI Office of General Counsel (OGC) or Chief Division Counsel (CDC).

Subject	Reference
1. Mapping ethnic/racial demographics	4.3 C. 2. b.
2. FBI employee may produce GEOINT	5.1
3. [redacted]	5.2 A.
4. [redacted]	5.6 A. 4.
5. [redacted]	11.10.3 B. 6.
6. [redacted]	11.10.3 B. 6. d.
7. Systematically assessing particular geographic areas or sectors	15.2 B. 1.
8. Analysis and Planning not Requiring the Initiation of an AGG-DOM Part II Assessment	15.2 C.
9. Domain Management by Field Offices	15.7 A. 1.
10. Written Intelligence Products	15.7 B.
11. United States Person (USPER) Information	15.7 B.
12. FBI authorized to operate Intelligence Systems	15.7 C.
13. Definition of Geospatial Intelligence (GEOINT)	15.7 D.
14. GEOINT Acronym	Appendix F-3

b2
b7E

[1] Link to the DIOG Table of Contents (TOC). This link will take you to the DIOG Table of Contents on the FBI Corporate Policy Office Policy & Guidance Web.
[2] The FBI has a long-established commitment to Privacy and Civil Liberties. The DIOG Section 4. Privacy and Civil Liberties, and Least Intrusive Methods must be followed.



The State of the NSB

(U) The State of the NSB

EAD-NSB Arthur M. Cummings II

(U) In early August, I had the opportunity to meet with employees from the Baltimore, Norfolk, Richmond, and Washington field offices who were at Headquarters for the second major phase of Strategic Execution Team training. Among the things I told these analysts and agents – who were the first to go through the initial SET rollout back in April – is how pleased I am about the pace at which the intelligence operations of the Bureau are changing in response to SET guidelines and recommendations.

(U) As we continue to build capacity and roll out SET, it is incumbent on us to ensure we have policies in place to guide these enhanced capabilities. Now that we are almost a third of the way through rolling out the new intelligence operations structure and functions to the field offices, I want to address some questions that have arisen about domain management activities within field offices, particularly domain mapping.

(U) The basic concept of domain management is simple: We need to develop a comprehensive understanding of the threats and vulnerabilities in each territory, so we can effectively deploy resources to support strategies that counter those threats. While we are still fine-tuning the policy that governs appropriate intelligence collection and domain mapping, field offices are collecting intelligence to understand their domain and address emerging threats.

"... you need to draw on intelligence requirements to articulate what the threat is before you start mapping it."

(U) In doing so, the most important thing to keep in mind is collection must always start with a threat. The new Attorney General Guidelines that are expected to be signed next month give us the authority collect intelligence outside of predicated cases. But in undertaking this collection, we must have an indication of a threat.

(U) Put another way, you need to draw on intelligence requirements to articulate what the threat is before you start mapping it.

(U) I envision appropriate collection and mapping in five steps: intelligence, analysis, analytic judgments, requirements, and operations. New intelligence comes in that indicates there is a threat. That intelligence is analyzed, and judgments are made about the threat to U.S. national security. Then we distill the intelligence down to collection requirements and start collecting.

(U) As a hypothetical example,

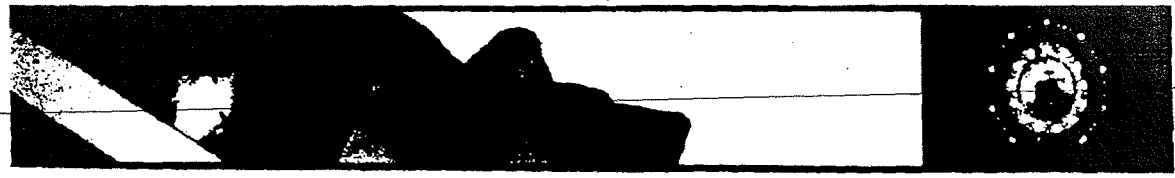
b2
b7E

(U)

What's the first step? We take the initial intelligence, and analyze it. Then we start making some judgments about it. Is it credible? Is there a threat to our national security?

In This Issue:

Top of Page ▲
Next Page ▶



What is the nature and scope of the threat? What is the extent of the presence in the United States? We'll distill those judgments into collection requirements, and send those out to the field to begin collecting and mapping.

[redacted]

(U) It's important to distinguish between mapping of a specific demographic within a community, and mapping the population in general. To understand your domain, you can map an entire set of demographics across all lines to better understand your constituency. We want field offices to know what's in their territory. But if you want to map just a specific category in the city's population, you need to do it because intelligence indicates the threat can be found from within a defined demographic. Once again, the key is in the ability to articulate the intelligence and analytic judgments that meet a reasonableness standard for non-predicated collection.

(U) We simply cannot afford to be seen as biased or arbitrary in our collection. Never forget that it is our responsibility to uphold and protect the civil rights of the American people. Carrying out our mission in large part depends on our ability to maintain the trust the American people have placed in us. If we always start with a threat, and match it with appropriate collection requirements, we can confidently do our job of protecting the American people and their liberties.

In This Issue:

b2
b7E

Aug 2008

The State of the NSB

(U) The State of the NSB

EAD-NSB Arthur M. Cummings II

(U) In early August, I had the opportunity to meet with employees from the Baltimore, Norfolk, Richmond, and Washington field offices who were at Headquarters for the second major phase of Strategic Execution Team training. Among the things I told these analysts and agents – who were the first to go through the initial SET rollout back in April – is how pleased I am about the pace at which the intelligence operations of the Bureau are changing in response to SET guidelines and recommendations.

(U) As we continue to build capacity and roll out SET, it is incumbent on us to ensure we have policies in place to guide these enhanced capabilities. Now that we are almost a third of the way through rolling out the new intelligence operations structure and functions to the field offices, I want to address some questions that have arisen about domain management activities within field offices, particularly domain mapping.

(U) The basic concept of domain management is simple: We need to develop a comprehensive understanding of the threats and vulnerabilities in each territory, so we can effectively deploy resources to support strategies that counter those threats. While we are still fine-tuning the policy that governs appropriate intelligence collection and domain mapping, field offices are collecting intelligence to understand their domain and address emerging threats.

"... you need to draw on intelligence requirements to articulate what the threat is before you start mapping it."

(U) In doing so, the most important thing to keep in mind is collection must always start with a threat. The new Attorney General Guidelines that are expected to be signed next month give us the authority collect intelligence outside of predicated cases. But in undertaking this collection, we must have an indication of a threat.

(U) Put another way, you need to draw on intelligence requirements to articulate what the threat is before you start mapping it.

(U) I envision appropriate collection and mapping in five steps: intelligence, analysis, analytic judgments, requirements, and operations. New intelligence comes in that indicates there is a threat. That intelligence is analyzed, and judgments are made about the threat to U.S. national security. Then we distill the intelligence down to collection requirements and start collecting.

(U) As a hypothetical example,

b2
b7E

(U)

What's the first step? We take the initial intelligence, and analyze it. Then we start making some judgments about it. Is it credible? Is there a threat to our national security?

In This Issue:

What is the nature and scope of the threat? What is the extent of the presence in the United States? We'll distill those judgments into collection requirements, and send those out to the field to begin collecting and mapping.

[redacted]

(U) It's important to distinguish between mapping of a specific demographic within a community, and mapping the population in general. To understand your domain, you can map an entire set of demographics across all lines to better understand your constituency. We want field offices to know what's in their territory. But if you want to map just a specific category in the city's population, you need to do it because intelligence indicates the threat can be found from within a defined demographic. Once again, the key is in the ability to articulate the intelligence and analytic judgments that meet a reasonableness standard for non-predicated collection.

(U) We simply cannot afford to be seen as biased or arbitrary in our collection. Never forget that it is our responsibility to uphold and protect the civil rights of the American people. Carrying out our mission in large part depends on our ability to maintain the trust the American people have placed in us. If we always start with a threat, and match it with appropriate collection requirements, we can confidently do our job of protecting the American people and their liberties.

This Month's Hot Topic

(U) Revised Executive Order 12333 Assigns IC Duties

[redacted]

In This Issue:

b2
b7E

Outside the Scope of Request

Top of Page ▲

Next Page ▶

DIRECTORATE OF INTELLIGENCE

Geospatial Intelligence Unit

What We Do

GIU Areas of Focus

- Executive Production
- GEOINT Analysis
- Standards, Policy & Administration
- Data Identification & Systems
- Training & Development
- Operational Support

Executive Production

FBIHQ Executive Management

- **Director's Office**
  - Director's Travel Book
  - Presidential Daily Brief
  - Director's Strategic Briefing
  - SAC Conference
  - AEAD Mullen Targeting Brief
- **Brief to Undersecretary of Defense for Intelligence (USDI)**
  - 07/29/2009
- **Briefings to AD's Favreau & Reinhold**
- **Investment Management Board (IMB)**

GEOINT Analysis

- Primary center of GEOINT analysis and product creation
- Leverage internal and external data sets to continuously create GEOINT products based on FBI priorities. Threats, vulnerabilities and gaps will be analyzed visually.
- Close work and support to Executive Production
- Develop relevant tradecraft, techniques, etc. for GEOINT in the FBI
- Identify geospatial relationships of significance
- Use GEOINT to better understand threats and vulnerabilities to inform investigations, analysis and resource allocations

GEOINT Analysis (cont.)

- Provide access to National Level Data sets for national threats and vulnerabilities
- Provide access to National Level Data sets for Strategic and Tactical Analysis
- Tactical Analysis for priority investigations
- GEOINT Analysis for FBIHQ Units
- Imagery….

GEOINT methodology

Define/visualize the Domain

Foundational datasets (boundaries, topography, demographics, etc.)

Describe/visualize threats and vulnerabilities within the Domain

Use available data to show specific activities, events, and areas of interest

Analyze/evaluate threats and vulnerabilities within the Domain

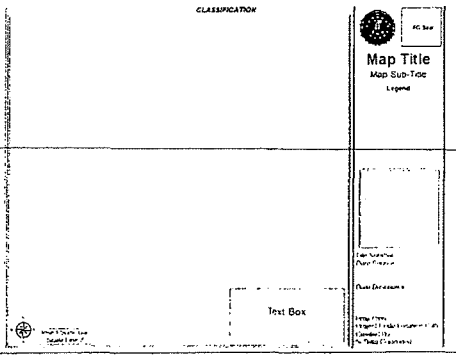
Regression Analysis, Data Modeling, Predictive Analysis

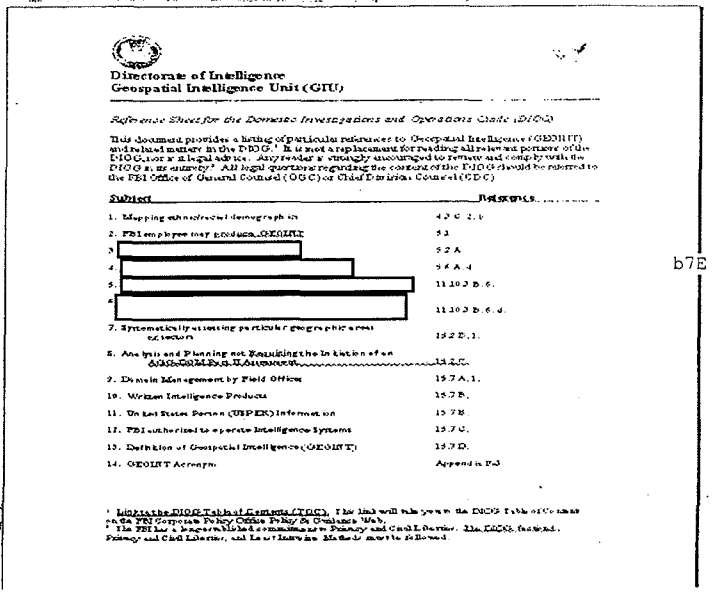
Develop analytical conclusions to support Domain Management

Threat Prioritization, Vulnerability Awareness, Resource Allocation

Standards, Policy & Administration

- Develop and implement standards within the FBI for GEOINT products
- Quality control on FBI GEOINT products.
- Legal and regulatory matters for GEOINT in the FBI
- Close coordination with the FBI Office of General Counsel (OGC)
- Develop and Implement Imagery Policy for the FBI





Directorate of Intelligence
Geospatial Intelligence Unit (GIU)

Reference Sheet for the Domestic Investigations and Operations Guide (DIOG)

This document provides a listing of particular references to Geospatial Intelligence (GEOINT) and related matters in the DIOG.[1] It is not a replacement for reading all relevant portions of the DIOG, nor is it legal advice. Any reader is strongly encouraged to review and comply with the DIOG in its entirety.[2] All legal questions regarding the content of the DIOG should be referred to the FBI Office of General Counsel (OGC) or Chief Division Counsel (CDC).

Subject	DIOG Section
1. Mapping ethnic/racial demographics	4.3.C.2.b
2. FBI employee may produce GEOINT	5.1
3. [redacted]	5.2.A
4. [redacted]	5.6.A.4
5. [redacted]	11.10.3.B.6.
6. [redacted]	11.10.3.B.6.d.
7. Systematically assisting particular geographic area or sector	15.2.E.1.
8. Analysis and Planning not Requiring the Initiation of an Assessment	15.3.C.
9. Domain Management by Field Office	15.7.A.1.
10. Written Intelligence Products	15.7.B.
11. United States Person (USPER) Information	15.7.B
12. FBI authorized to operate Intelligence Systems	15.7.C.
13. Definition of Geospatial Intelligence (GEOINT)	15.7.D.
14. GEOINT Acronym	Appendix A-3

[1] See the DIOG Table of Contents (TOC). The link will take you to the DIOG Table of Contents on the FBI Corporate Policy Office Policy & Guidance Web.
[2] The FBI has a long-established commitment to Privacy and Civil Liberties. The DIOG, for example, Privacy and Civil Liberties, and Least Intrusive Methods must be followed.

b7E

Data Identification & Systems

- Expertise and zealous advocacy for the development of IT hardware and software solutions that match user requirements for GEOINT in the FBI

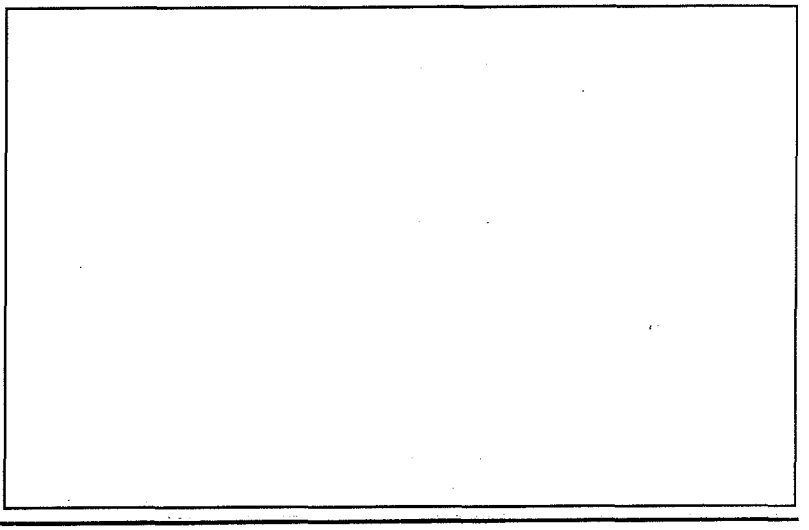
- SSA [redacted] presentation to follow

b6
b7C

iDX3

(formerly iDomain)

- Enterprise wide technology application
  - FBI web-based mapping application
  - Modeled after NGA's Palanterra X3
  - Manage, Manipulate, Query and display geospatial data
- Multiple Data Sources
- Robust Requirements Process
- Analytical Tools
  - Routes, Drive Time, etc.
  - Buffers
- Data Sharing
- Imagery!



b7E

HIFLD/HSIP

-
-
-

b7E

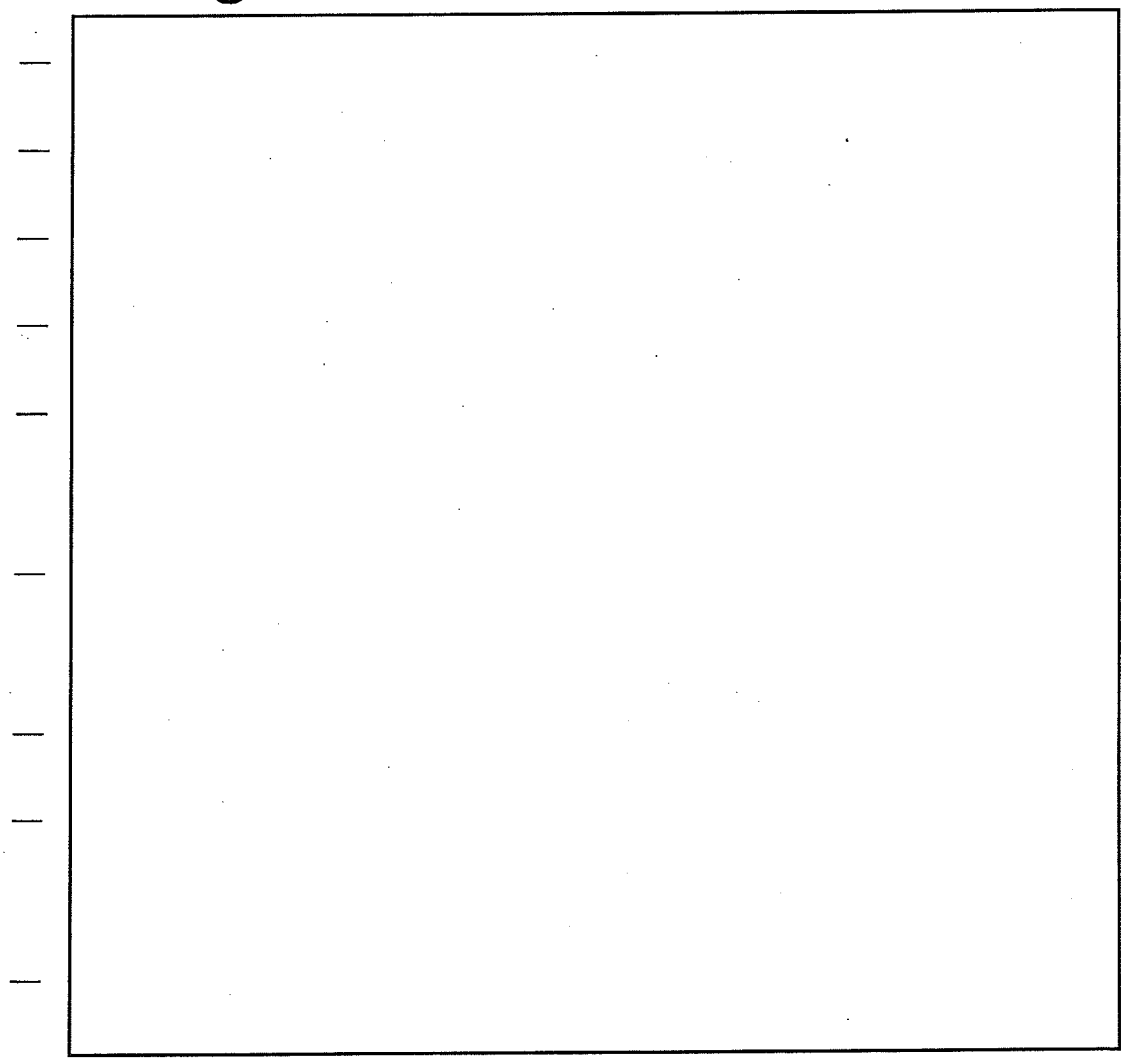
Training & Development

- Training Accomplishments
  - As of 05/26/2010:
    - [ ] FBI Personnel trained for FBI Basic GEOINT b7E
      - [ ] trained in FY 2010
    - [ ] external training opportunities in FY 2010
      - [ ] ESRI, Universities, etc.
      - [ ] NGA College
      - [ ] NGA Analyst Exchange
- Daily Technical Support to the field and FBIHQ

  [ ] b6 b7C
- GIA position
  - [ ] b7E
  - [ ]

Training & Development

- Training Planned for FY 2011



b7E

Operational Support

-
-
-
-
-
-
-
-
- Guardian/eGuardian

b7E

NGA

-
-
-
-
-

b6
b7C
b7E

Questions?

GEOINT Techniques

b7E

- National Strategic Maps
  - Risk Based Planning
  - PDB
- Network Analyst/Tracking Analyst
- Canvass
  - Narrow down interview area
  - Narrow down interview list
- Travel (CONUS & OCONUS)
  - Analyze travel patterns
  - Route Analysis
  - Determine destinations of interest
  - Population densities as a relevant factor
- Confidential Human Sources
  - Source coverage
  - Reporting areas
  - Gaps in reporting
  - Vetting/Validation
- Financial Transactions
- FBI Data
- Imagery
- Communications Analysis
- Cases
  - Historical v. Present
  - Sophisticated Techniques (TIII, FISA, etc.)
  - Division/County/Address views

Use of Race and Ethnic Identity in Assessments and Investigations

- The DIOG reiterates Department of Justice (DOJ) guidance which permits the consideration of ethnic and racial identity information based on specific reporting (i.e. eyewitness accounts).

- Consideration of race or ethnicity is permitted in investigative or collection scenarios, if relevant. Examples may include investigations of ethnic-based gangs or terrorist organizations known to be comprised of members of the same ethnic grouping.

Collecting and Analyzing Demographics

- The DIOG also reiterates DOJ guidance permitting the collection and analysis of demographics if the identification of concentrated ethnic communities will reasonably aid in the analysis of potential threats and vulnerabilities or assist domain awareness for the purpose of performing intelligence analysis.

- In addition, the locations of ethnic-oriented businesses or other facilities may be collected if their locations will reasonably contribute to an awareness of threats and vulnerabilities and intelligence collection opportunities.

Collecting and Analyzing Demographics

- If the collection of ethnic/racial demographics is legally allowable in an investigation, it may also be "mapped" using sophisticated computer geo-mapping technology.
- These maps may be used for domain awareness of an area of responsibility, to track crime trends, or to identify specific communities or areas of interest to support specific assessments or investigations.
- Regardless of the purpose for its use, the relevance of the ethnic or racial information must be clearly demonstrated and documented.

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion of the subject or the exercise of First Amendment rights.
- Corollary to this AGG requirement is the Privacy Act, which states that each agency that maintains a system of records shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or **unless pertinent to and within the scope of an authorized law enforcement activity.** 5 U.S.C. 552a(e)(7).

DIOG Section 4 Scenario

- [redacted]
- What can you do with this information?
- [redacted]

b2
b7E

UNCLASSIFIED//FOUO

DIOG Section 4 Scenario

-
-

b2
b7E

UNCLASSIFIED//FOUO 45

UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

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 46

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS (cont.):

- No investigative activity, including assessments, 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.
- If an assessment or predicated investigation touches on or is partially motivated by First Amendment activities, race, ethnicity, national origin or religion, it is particularly important to identify and document the basis for the assessment with clarity

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

All activities must be consistent with the Attorney General's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (forbids the use of racial profiling and requires activities involving the investigation or prevention of threats to the national security to comply with the Constitution and laws of the United States)

The DIOG stresses several points in each section:

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion, or exercise of First Amendment rights
- The FBI must use the least intrusive method that is feasible under the circumstances
- In connection with Foreign Intelligence collection, agents must operate openly and consensually with U.S. Persons, to the extent practicable
- All investigative activities must have an "authorized purpose"

UNCLASSIFIED//FOUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to individuals:

1. Permits the consideration of ethnic and racial identity information based on specific reporting;
2. The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected when gathering information about or investigating the organization; or
3. Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person

UNCLASSIFIED//FOUO 49

UNCLASSIFIED//FOUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to a community:

1. Collecting and analyzing demographics – if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness
2. Geo-Mapping ethnic/racial demographics – if properly collected
3. General ethnic/racial behavior – cannot be collected, unless it bears a rational relationship to a valid investigative or analytical need
4. Specific and relevant ethnic behavior
5. Exploitive ethnic behavior – by criminal or terrorist groups

UNCLASSIFIED//FOUO 50

UNCLASSIFIED//FOUO

DIOG Section 4: Least Intrusive Investigative Method

The AGG-DOM and the DIOG require 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

UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

By emphasizing the use of less intrusive means, employees will be able to balance:

Our need for evidence/intelligence

vs.

Mitigating potential negative impact on the privacy and civil liberties of people/public

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)

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 [redacted] b2 b7E

- **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.

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.

DIOG Section 15: Intelligence Analysis and Planning

- **Raw Intelligence:** This represents information collected from sources which is generally considered to be unvetted or not confirmed by other reporting means. Such reporting information is typically captured in Intelligence Information Reports (IIRs), FD 302s and ECs.

- **Finished Intelligence:** Such reports represent judgments made by intelligence analysts in the field or at FBIHQ regarding the synthesis of multiple, relevant raw intelligence source reports which indicate probable intent or action by threat actors of either a criminal or national security nature. FBI finished intelligence products used are the Intelligence Bulletin (IB), Intelligence Assessment (IA) and Special Event Threat Assessment (SETA). Domain Assessments and briefings can also represent finished intelligence products.

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.

Information is shared both internally within the FBI and externally to LE or USIC partners as appropriate based on the classification and handling instructions established by the managers of the programs which have created these files or reports. Common information platforms used for sharing and receiving intelligence products are Law Enforcement Online (LEO), Intellink (both Secret and Top Secret for the USIC) and [redacted] for the counter-terrorism community.

b2
b7E

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