



**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.

UNCLASSIFIED



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.”

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,



(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:

Page One

The State of the NSB

On This Date

This Month's
Hot Topic: New
Law Codifies FBI
Information Sharing
Initiatives

NSB News

Resources

NSB Q&A

NSB Memo
Survey

Archives

Contact Us

b2
b7E

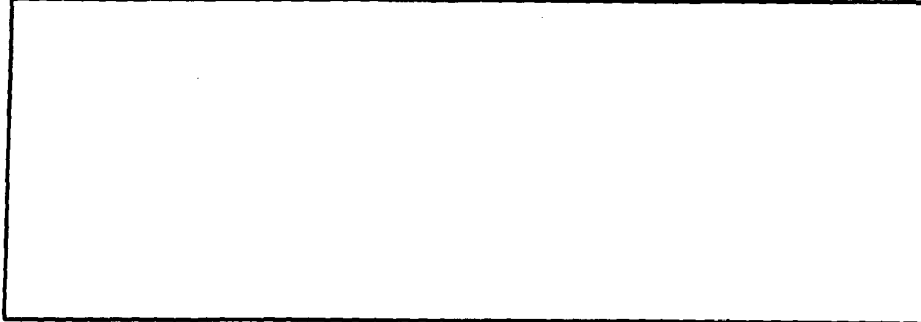
Top of Page ▲

Next Page ►

UNCLASSIFIED



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.



(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:

Page One

The State of the
NSB

On This Date

This Month's
Hot Topic: New
Law Codifies FBI
Information Sharing
Initiatives

NSB News

Resources

NSB Q&A

NSB Memo
Survey

Archives

Contact Us

b2
b7E

Top of Page ▲

Aug 2008

~~SECRET~~//NOFORN



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,



(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:

Page One

The State of the NSB

On This Date

This Month's
Hot Topic: New
Law Codifies FBI
Information Sharing
Initiatives

NSB News

Resources

NSB Q&A

NSB Memo
Survey

Archives

Contact Us

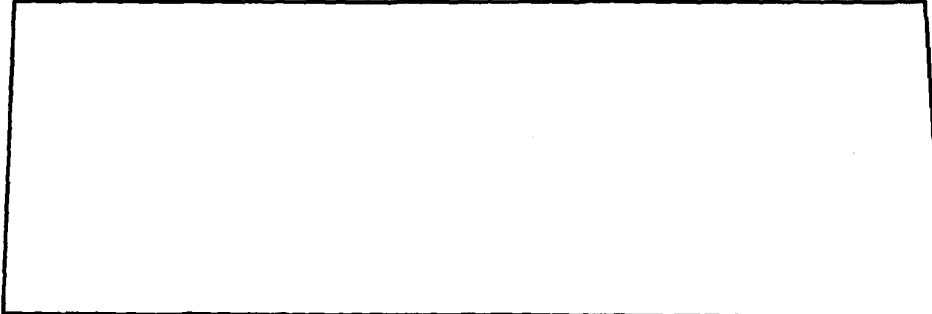
b2
b7E

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.

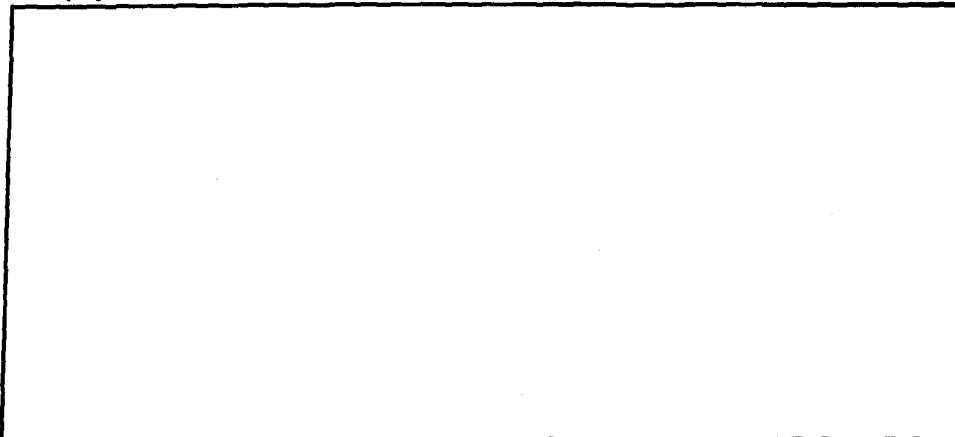


(U) It's important to distinguish between mapping of a specific demographic within a community, and mapping the population in general. To understand your domain, you can map an entire set of demographics across all lines to better understand your constituency. We want field offices to know what's in 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



In This Issue:

Page One

The State of the NSB

On This Date

This Month's Hot Topic: New Law Codifies FBI Information Sharing Initiatives

NSB News

Resources

NSB Q&A

NSB Memo Survey

Archives

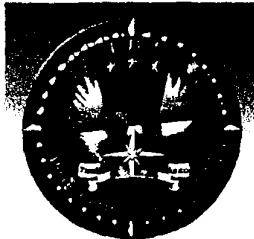
Contact Us

b2
b7E

Outside the Scope of Request

Top of Page ▲

Next Page ►



DIRECTORATE OF INTELLIGENCE



Geospatial Intelligence Unit

What We Do



Geospatial Intelligence Unit (GIU) Directorate of Intelligence



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



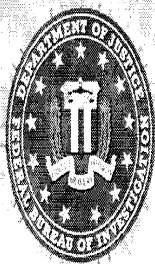
- Primary center of GEOINT analysis and product creation
- Leverage internal and external data sets to continuously create GEOINT products based on FBI priorities. Threats, vulnerabilities and gaps will be analyzed visually.
- Close work and support to Executive Production
- Develop relevant tradecraft, 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

CLASSIFICATION

FOI See

Map Title
Map Sub-Title
Legend

Text Box

Geospatial Intelligence Unit

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. 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. 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 administrative demographics	4.2 C. 2.1
2. FBI employees 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 of sectors	15.2 B. 1.
8. Analysis and Planning not Requiring the Inclusion of an AIGS/COMINT 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 Acronyms	Appendix F-3

¹ Link to 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 reflects Privacy and Civil Liberties, and Law Enforcement Methods, as well as the following:

b2
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 presentation to follow

b6
b7c

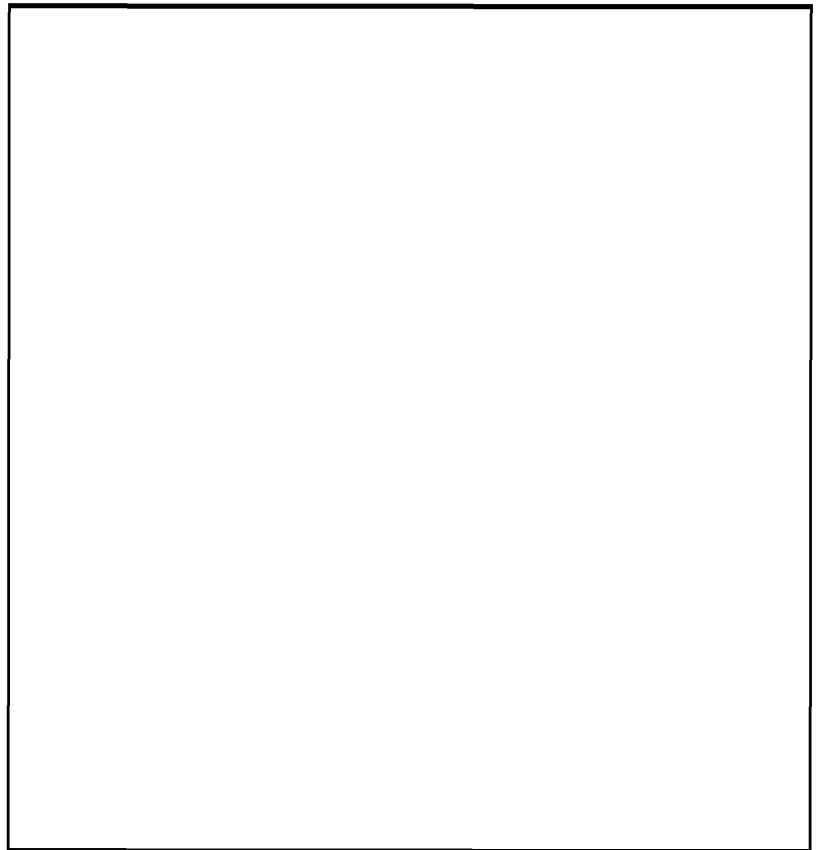


iDX3

(formerly iDomain)



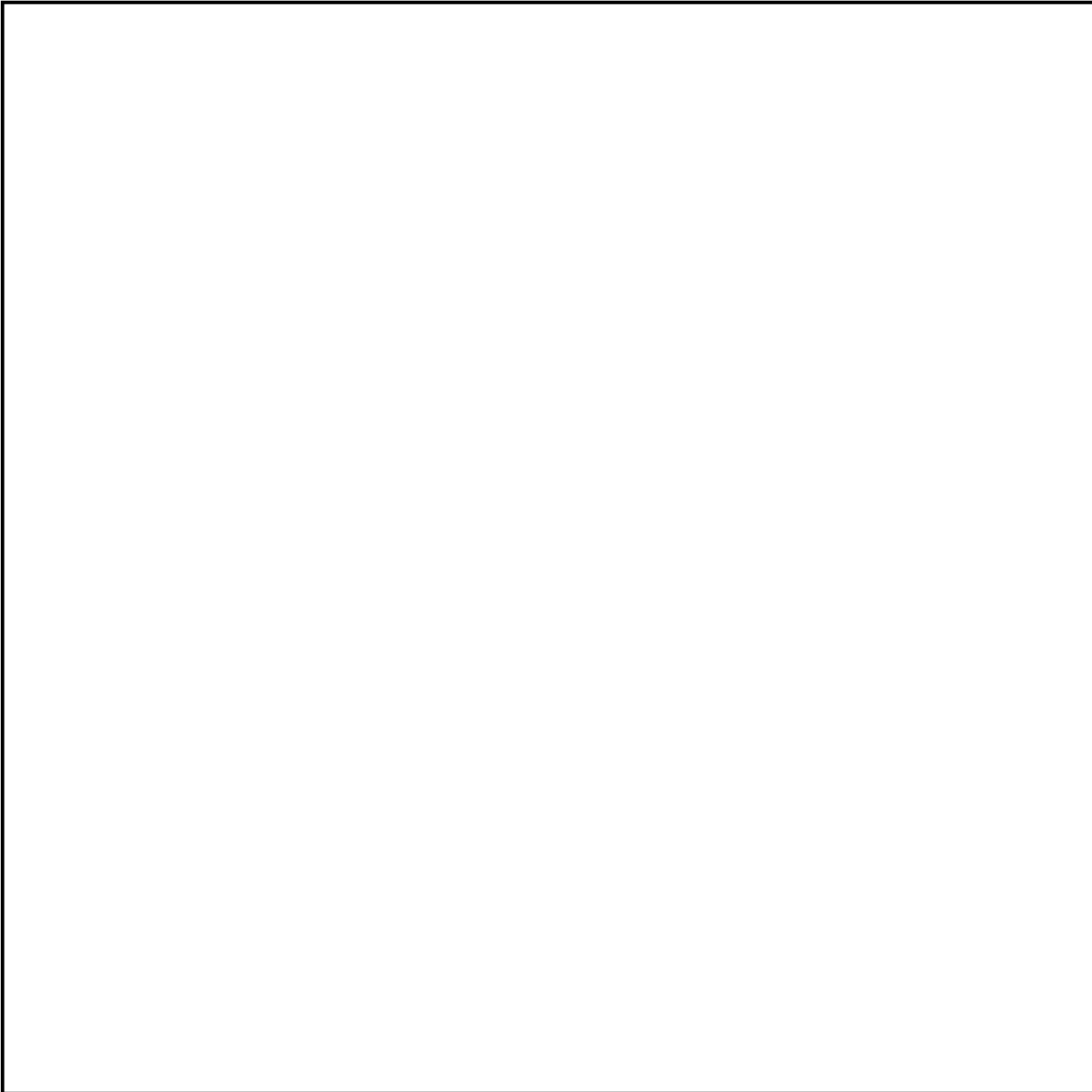
- Enterprise wide technology application
 - FBI web-based mapping application
 - Modeled after NGA's Palantira X3
 - Manage, Manipulate, Query and display geospatial data
- Multiple Data Sources
- Robust Requirements Process
- Analytical Tools
 - Routes, Drive Time, etc.
 - Buffers
- Data Sharing
- Imagery!



b2
b7E



FIELD/HSIP



b2
b7E



Training & Development



- Training Accomplishments
 - As of 05/26/2010:
 - ☐ FBI Personnel trained for FBI Basic GEOINT
 - ☐ trained in FY 2010
 - ☐ external training opportunities in FY 2010
 - ☐ ESRI, Universities, etc.
 - ☐ NGA College
 - ☐ NGA Analyst Exchange

b2
b7E

- Daily Technical Support to the field and FBIHQ

b6
b7C

- GIA position

-
-

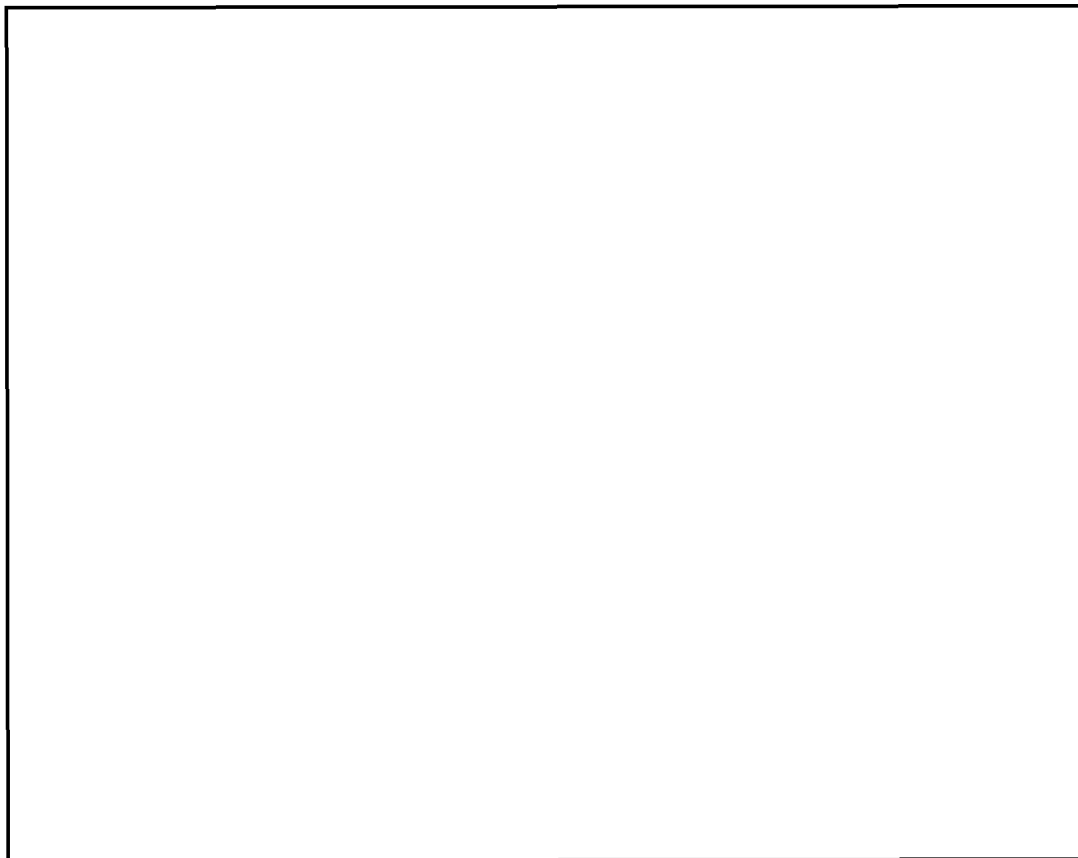
b2
b7E



Operational Support



-
-
-
-
-
-
-
-
-

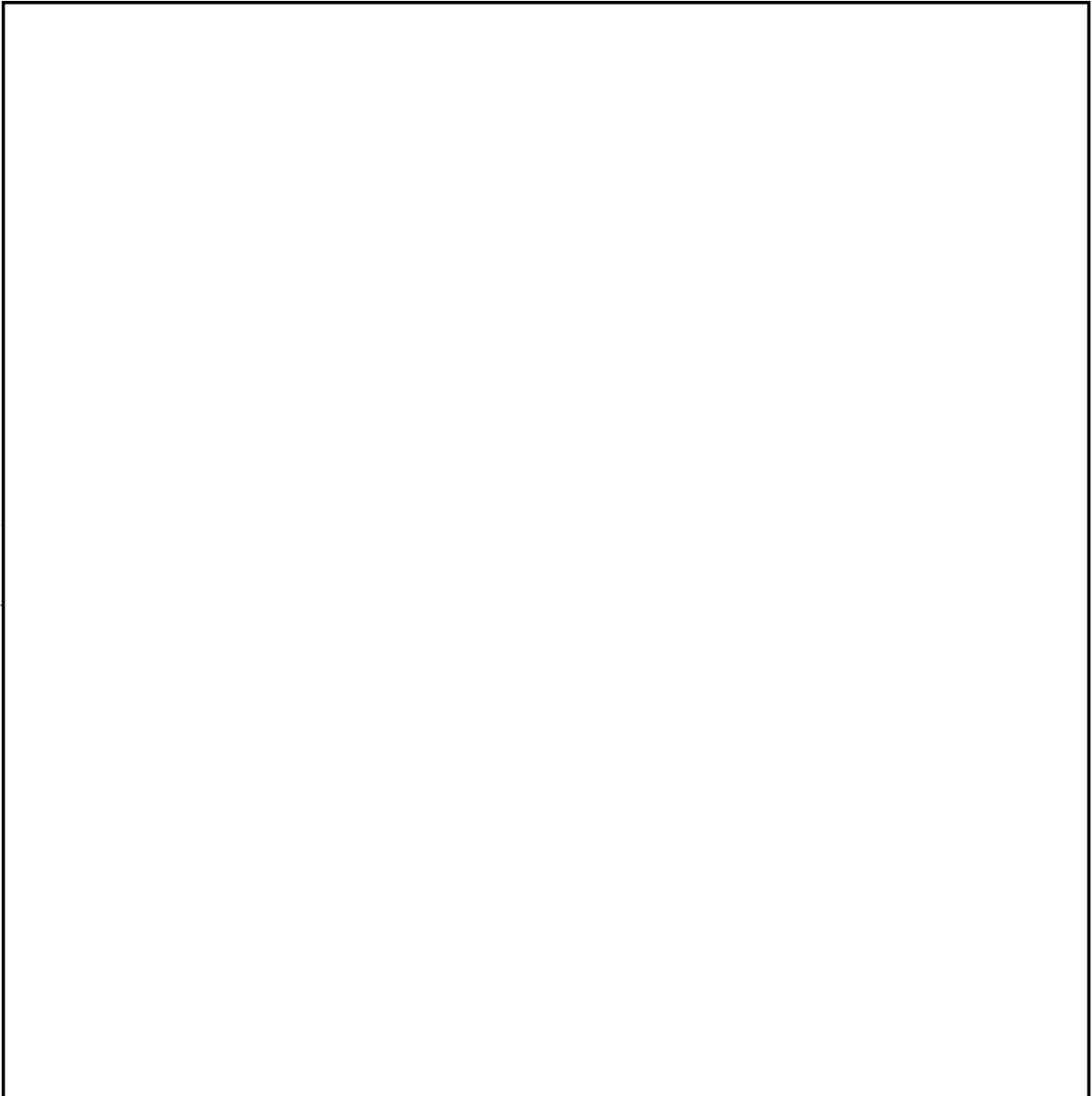


b2
b7E

- Guardian/eGuardian



NGA



b2
b6
b7C
b7E



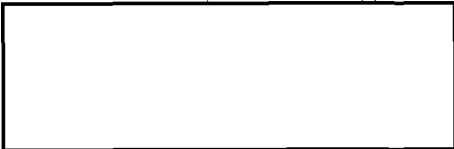
Questions?



GEOINT Techniques





b2
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 (THL, FISA, etc.)
 - Division/County/Address views