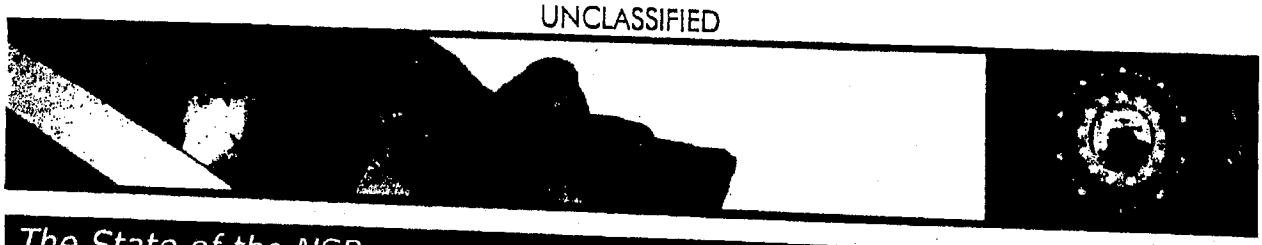


The State of the NSB

(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

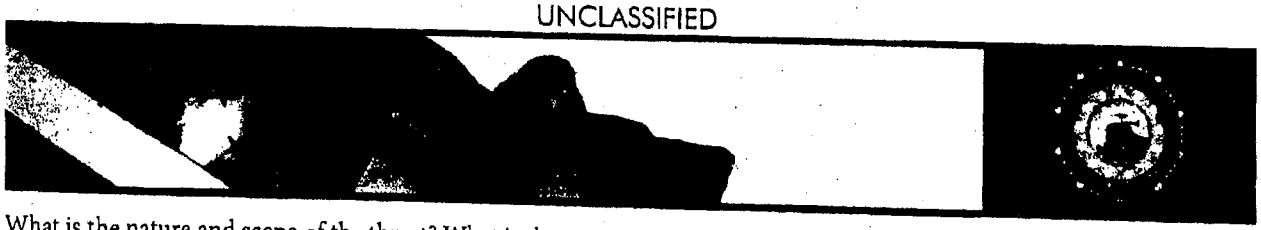
(U)

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:

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

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:

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

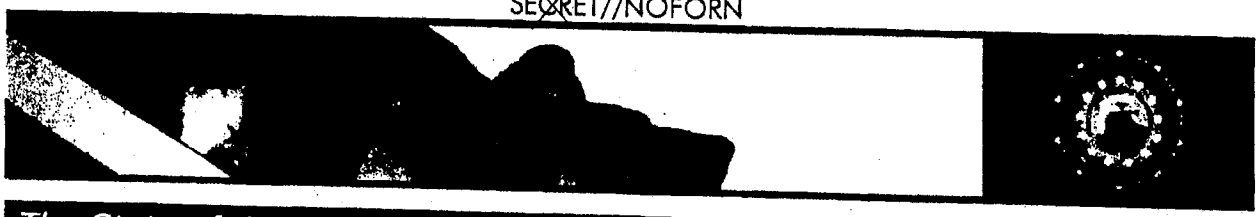
Archives

Contact Us

Top of Page ▲

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

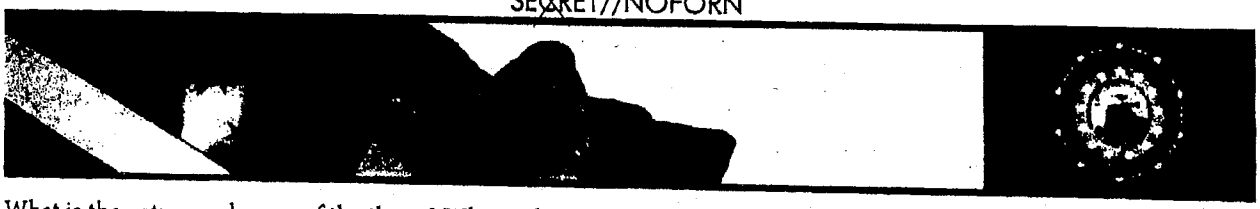
(U)

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:

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

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.

This Month's Hot Topic

(U) Revised Executive Order 12333 Assigns IC Duties

[redacted]

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 ▶