U.S. Department of Justice
Federal Bureau of Investigation

THE NEW
Field Intelligence

March 2008 – March 2009
Version 1.5

SET
Strategic Execution Team

ONE FBI – PROTECTING NATIONAL SECURITY

As we enter our 100th year, the FBI must continue to stand up to the challenge to protect the American people from an array of complex threats that are in an increasingly interconnected world. Our vision for what the FBI can be, and must be, to meet this challenge is neither radical nor insurmountable:

The FBI will protect the American way of life by staying ahead of national security threats to the homeland, acting at all times with obedience to the Constitution, fairness, compassion, integrity, and respect.

When we talk about "threats to national security," we are not focused only on terrorism, foreign intelligence, and weapons of mass destruction – although these are important priorities. A national security threat is one that tries to challenge the very foundations of American society, involving dangers so great that no local authority can handle them alone. It includes gangs that cause violence and disorder in cities, cyber crimes and transnational criminal enterprises that are borderless and have the potential to cause widespread disruption, white collar crimes that undermine the strength of our economy, and public corruption that tears at the fabric of our democracy.

The foundation of the FBI's strength will be the same in our second century as it was in our first – our core values, our tradition of excellence, our respect for constitutional rights, our support for our partners in law enforcement, our ties to our communities, and our ideals of fidelity, bravery, and integrity. And, let us not forget **leadership** and a sense of **FBI Family**.

At the same time we steadfastly embrace these qualities, we must be prepared to think and act differently when called upon to keep Americans safe from harm in our next century. Our adversaries are constantly adapting. We cannot afford to be set in our ways. We must be open to new levels of collaboration. As individuals, we must be willing to stretch ourselves beyond our comfort zones, to develop ourselves throughout our careers, and to adopt a posture of continuous learning.

We will continue to enforce federal laws, but we will choose our cases carefully, looking at the level of threat and needs of our local partners, and focusing on areas where we have unique capabilities or jurisdiction. The FBI is essentially the only member of the U.S. Intelligence Community with broad authority over the **domestic domain**. The American

people and our partners in the Law Enforcement and Intelligence Communities are counting on the FBI to use all of its tools to build a domestic security service capable of staying on the offensive against our greatest threats.

To do this effectively, we need to maximize all of the FBI's investigative and intelligence capabilities – what we know and what we *need to* know – in *every* program area to respond to national security threats to the homeland. If we base our knowledge only on what we learn through cases, we will be missing important parts of the picture.

It is more important now than ever before that we are **ONE FBI**. We cannot be "stove piped" in any way – not by field office, not by region, or not by program. We are one enterprise, consisting of skilled professionals working together. Aided by cutting edge tools and technology, we will build knowledge and develop insight that will provide strategic and tactical early warning, direct operations, create opportunities to further cases, and inform national security policymakers.

This document, "The New Field Intelligence," is a practical playbook to help us achieve this vision. It is not a policy document, but rather a communications tool to help all FBI personnel understand our strategy for intelligence activities in the field and their role in implementing that strategy.

I am proud of the work that went into this strategy because it reflects some of the best thinking across the Bureau. A Strategic Execution Team (SET) made up of almost 100 Special Agents, Intelligence Analysts, and other skilled professionals from field offices and FBIHQ examined the intelligence activities in each of our 56 field offices. The team identified optimal structures and processes for our intelligence activities from the best practices that were developed through trial and error in the field.

I ask you to be open to the changes that will be required and to do your part to help the Bureau succeed. Implementation will not be perfect, but where you see that things are not working, I ask you to work toward solutions. If we all participate, we will reach our full potential as a national security agency, and our families, communities, and country, will be safer in the years ahead as a result of your efforts.

Robert S. Mueller III

CONTENTS

INTRODUCTION

What is the purpose of our Intelligence activities in the field?

Simply stated, intelligence helps us do our jobs better, and helps our partners do their jobs better, so that, collectively, we are more effective at protecting our communities and our nation from harm.

Gaining intelligence and using it effectively helps us achieve our ultimate mission to protect the American people and enforce the federal laws. It enables us to better under stand the actions of our adversaries so that we can prevent threats from harming our communities and our national security. It informs our decision-making so that we allocate scarce resources where they will do the most good, focus first on the cases with the potential to neutralize the greatest threats, and recruit sources who have answers to our most pressing questions. When we share this intelligence with our partners, we share its benefits with them as well, making the entire homeland/national security apparatus more effective. We bolster the ability of everyone with a role in protecting the American people, from the patrol officer to the President, to make informed decisions.

Intelligence is not solely the responsibility of the Field Intelligence Group (FIG) or particular programs. The entire field office (FO) has a role in supporting the intelligence mission. All field office personnel, whether they are working on criminal matters or counterterrorism, and whether they are Special Agent (SA) or professional staff, will contribute to – and benefit from – the office's intelligence activities.

The field intelligence mission is:

To protect and preserve the national security of the United States and suppress crime, FBI field offices will integrate intelligence activities into all investigative efforts by:

- Systematically assessing their domain to identify potential threats, vulnerabilities, gaps in knowledge, and collection opportunities against national as well as FBI intelligence requirements, which support the broad range of FBI responsibilities;
- Pro-actively directing resources to collect against potential threats and other issues of interest to the nation and the FBI, and developing new collection capabilities where they are needed;
- Continuously validating collection capabilities to ensure information integrity;
- Deliberately gathering information against articulated priority intelligence requirements using all available collection resources;

- Expeditiously preparing collected information for dissemination and rapidly providing it to appropriate partners at the local, state, and national level; and

- Purposefully evaluating the collected information's implications on current and emerging threat issues.

Core Intelligence Functions

While intelligence is integrated into the work of the entire field office, it is the responsibility of the FIG to coordinate, guide and support the office's activities through five core functions:

- Domain management
- Collection Management
- Requirements based (sometimes non-case) collection - including human intelligence (HUMINT)
- Tactical intelligence, and
- Intelligence production and dissemination

These five functions will help the field office ask a series of questions about our adversaries and ultimately answer those questions with enough specificity to drive actions to dismantle them. Types of questions include the following: What is their leadership structure? How do they raise money? How do they recruit? Where are they present? How do they communicate? What are their vulnerabilities? Most organizations have these elements in common.

Do we have a diagram of how our adversaries work – their key management, fundraising, etc.– and is that picture assembled in one place? Where do we lack knowledge (typically acquired through human sources or wires)? Do we have a plan to address the gaps? And can we say, with consistency, that our dismantlement plans – our use of law enforcement tools – are based on a good picture of the target we're trying to take down? Or are they ad hoc?

The ideal field division, over time, should be able to answer the following questions:

1. Based on the Director's priorities, what are the key threats in your domain?
2. What are your collection efforts directed at this target?
3. What coverage do you have of those threats (leadership, finances, etc.)? What is your level of confidence in that coverage?
4. What collection plans do you have in place to ask sources about your gaps in knowledge?
5. Where you lack sources to answer key questions, what recruitment initiatives do you have to find sources who can complete your picture?
6. Have you disseminated what you know, so that anyone sitting with no knowledge of the target could understand what you know?
7. Are your cases drawn from this knowledge? Can you articulate and support why you opened one case and not another? And, are your dismantlement plans based on this knowledge?

When we have the answers to these questions, we should dissem inate what we know. This will enable the Bureau as a whole to analyze national and intern ational networks. Once we analyze and pull together what we know – what the national infrastructure of our adversaries looks like – we can then determine the best way to dismantle. For example, types of concerns include: What key players do we need to rem ove to cripple the organization? How can we eliminate their ability to raise funds? How can we ensure that our dismantlement plan will permanently disrupt the target?

The core functions that will enable the field office to answer these ques tions will require an investment in analytical, investigative, and collection resources. Investing in these intelligence functions will allow the FO to leverage all of its investigative and analytic capabilities to develop and maintain a common understanding of the threat issues they are currently facing, but also ensure the FO is able to identify emerging threats, assess those threats, and act against them.

Organization

All five of the core intelligence functions require the FIG to work seamlessly with the operational squads in order to be successful. Unfortunately, one of the biggest problems impeding our progress is poor information flow between the Special Agents collecting information and Intelligence Analysts (IAs) on the FIG. In many offices, we also see a lack of direction about the type of intelligence that should be collected. Our new model for field intelligence will help us improve these areas so that we can leverage all of our collection capabilities, in every squad and program, to meet our most critical Intelligence requirements.

This new model helps integrate tactical and strategic ***thinking*** by establishing a distinct intelligence leadership role at the ASAC or SAC level, and a central, strategic coordinating component for Collection Management and Domain Awareness. This new model will include a Chief Reports Officer, and in some offices cross-programmatic issue-oriented local Desks with clear links to a network of regional and national Desks. They will be supported by database administrators, Geographic Inform ation System (GIS) operators, and other professionals.

The field intelligence model also helps integrate tactical and strategic ***action*** by embedding analysts in operational squads, and by dedicating a group of Special Agents to requirements-based, cross-program collection. It fosters collaboration between the FIG and operational squads, and promotes the use of intelligence to inform decision-making at many levels, from executive management decisions about resource allocation to tactical operational planning in the squads.

Surveillance professionals and langu age analysts will be consolidated under a cross-program ASAC or SAC, and will play a critical role in supporting both tactical and strategic efforts. In field offices where these groups are not already consolidated, they will be placed under the SAC or ASAC for intelligence. This will help us leverage their capabilities to facilitate broad support for the entire field office.

The new structure and work roles will be supported by streamlined processes and new information technology (IT) tools that make it easier for all field office personnel to share information, identify the intelligence value of information, and produce and dissem inate intelligence products.

A New Mindset

The new field intelligence model challenges us to begin a new way of thinking about ourselves, and our roles and responsibilities for conducting domestic intelligence. We need to start thinking about ourselves as part of a national security organization. This is based on criminal events, including terrorist activities, that have impacted our nation's security and threatened its democratic principles. This is not the job of one "side of the house," but of the entire Bureau. Operational activities feed information into the intelligence process, and the intelligence process informs operations. We will use our interdependent operational and intelligence capabilities to protect the American people from threats – whether those threats come from criminals, terrorists, hostile foreign intelligence penetrations, corrupt public officials, or those who deny others their civil rights.

We must overcome the tendency to prioritize and handle resources in program silos. Many of the threats we face are regionally, nationally, or internationally networked and cannot fully be understood by looking through the lens of a single program or office. The FIG will help the field office and FBI Headquarters (FBIHQ) see the full picture, but only if it is supported by the entire FO.

So we must depart from thinking about sources and intelligence in terms of what case, program, office, or individual "owns" them and start thinking about where each can add value. Our strategy is to reduce hierarchical bottlenecks, and build stronger internal networks connecting personnel (and our collection capabilities) within field offices, across regions, and between individuals and FBIHQ. We also will build stronger external networks, including direct channels of communication between field offices, FBIHQ, other agencies, and the public.

We will build on our Strategy Management System (SMS) with performance dialogues that will cascade down from SACs to squads to help us track progress and share best practices. We will measure success by the relevance, accuracy, and speed of our intelligence reporting. It will also be measured by the degree to which information is actionable or informs decision-making, and ultimately by our ability to dismantle our adversaries' organizations, and prevent and suppress crime, terrorism, and other threats to national security. Along these lines, you are going to see new metrics for evaluating individual, program, and office performance, and a completely revamped inspection process.

ORGANIZATION

The creation of a FIG in every FBI field office was a critical step in developing our intelligence capabilities. Based on initial guidance, offices developed a wide range of FIG structures, staffing models, and workflow processes. Some had a great deal of success; others struggled. But in all instances, these 56 models taught us valuable lessons. Our next step is to apply those lessons to achieve our full potential in the intelligence arena.

Through an exhaustive analysis of FIGs and input from both field and FBIHQ personnel, we identified the elements that the most successful field offices have in common. Using these best practices, we designed the optimal model for intelligence in all field offices. We will now standardize all field offices according to this model, allowing for some variation in the size and complexity of the office. Implementation of the model will impact the office's organizational structure, what leadership positions exist and who fills them, work roles and responsibilities for personnel, the relationship between the FIG and operational squads, and coordination across field offices and with FBIHQ.

Common Elements

The structure and work roles for intelligence in the field are being standardized for two reasons. First, standardization will ensure that core intelligence functions (i.e., Domain Management, Collection Management, Collection, Production and Dissemination, and Tactical Intelligence) are being performed within each field office in a consistent and effective manner. Second, as employees move to other assignments within field offices, between field offices, or to FBIHQ, they will have the benefit of common roles, tools, practices, and procedures present at all levels of the organization.

The field intelligence model includes common elements that will be applied in all offices regardless of size and complexity.

- All field offices will have a distinct intelligence leadership role at the ASAC level or above.
- All FIGs will have a central, strategic coordinating component consisting of a Collection Management Coordinator (CollMC), Domain Management Coordinator (DMC), and Chief Reports Officer (CRO). This component will enable each field office to develop and sustain a holistic, cross-programmatic view of its domain, overlay collection capabilities based on the Domain Assessment, identify collection opportunities and intelligence gaps, assist the field office with articulating an overarching collection strategy and cascading collection plans, and ensure timely reporting of raw intelligence to our partners that is both relevant and of high quality. Depending on the size of the FIG, they will be supported by varying numbers of database administrators, GIS operators, and other professional staff.
- Embedded Intelligence Analysts will be supervised by the FIG, but will be physically co-located with operational squads and Resident Agencies (RAs).

- All FIGs will have a team of Special Agents dedicated exclusively to requirements-based source development and collection.

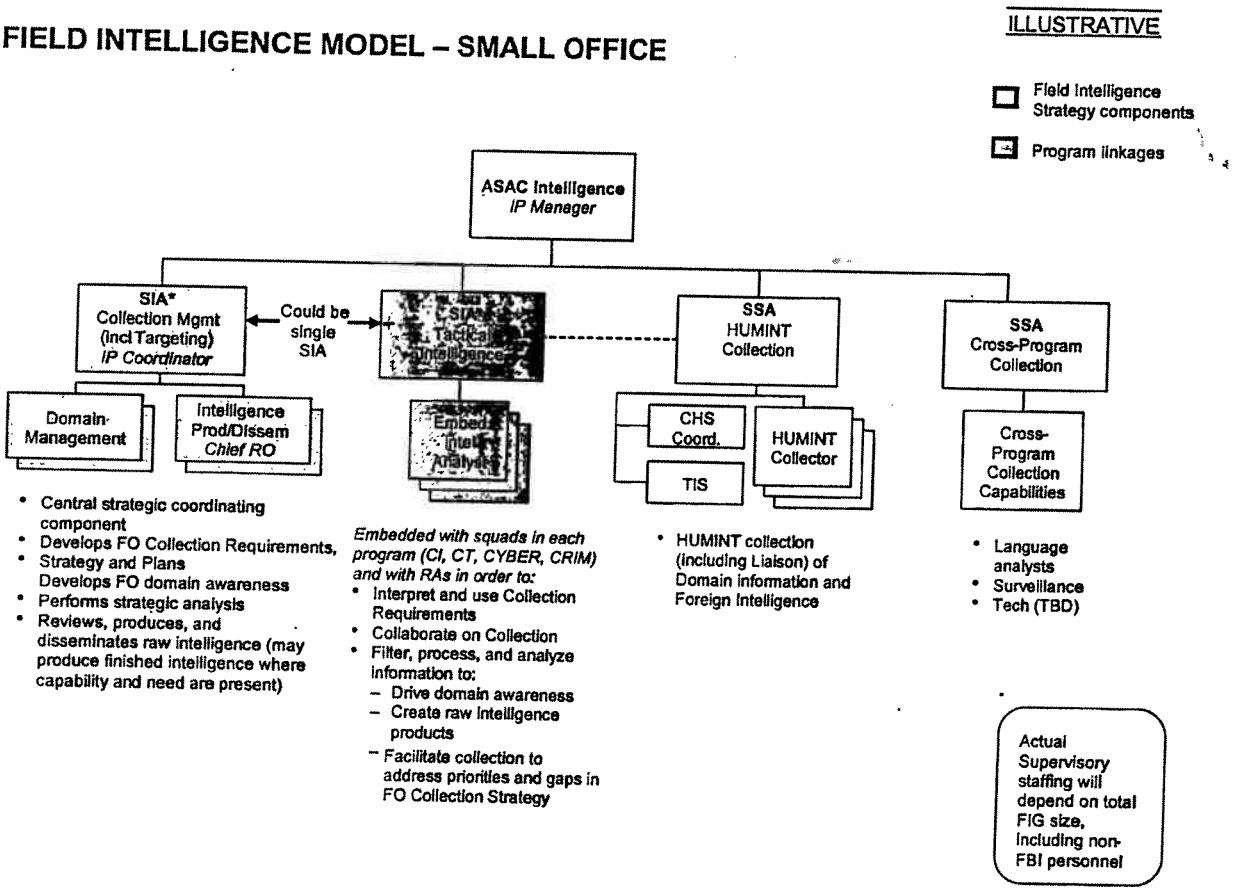
- Cross-program collection capabilities, such as SOG, SSG, and language analysts will be consolidated under the ASAC (or SAC) for intelligence to facilitate broad support for all squads and programs in the field office. If they are already grouped under an SAC or ASAC who is not responsible for an investigative program, the organizational structure will not be changed. An SAC or ASAC who is not responsible for managing any of the investigative programs, should be best positioned to help the SAC focus resources in a way that supports the Collection Strategy.

- The final common element is the implementation of management processes to ensure that intelligence supports effective decision-making across the field office.

Adapting the Model to Office Size

In the smallest 13 to 15 field offices, the field intelligence model will include all of the core intelligence functions, but some duties may be combined.

FIELD INTELLIGENCE MODEL – SMALL OFFICE

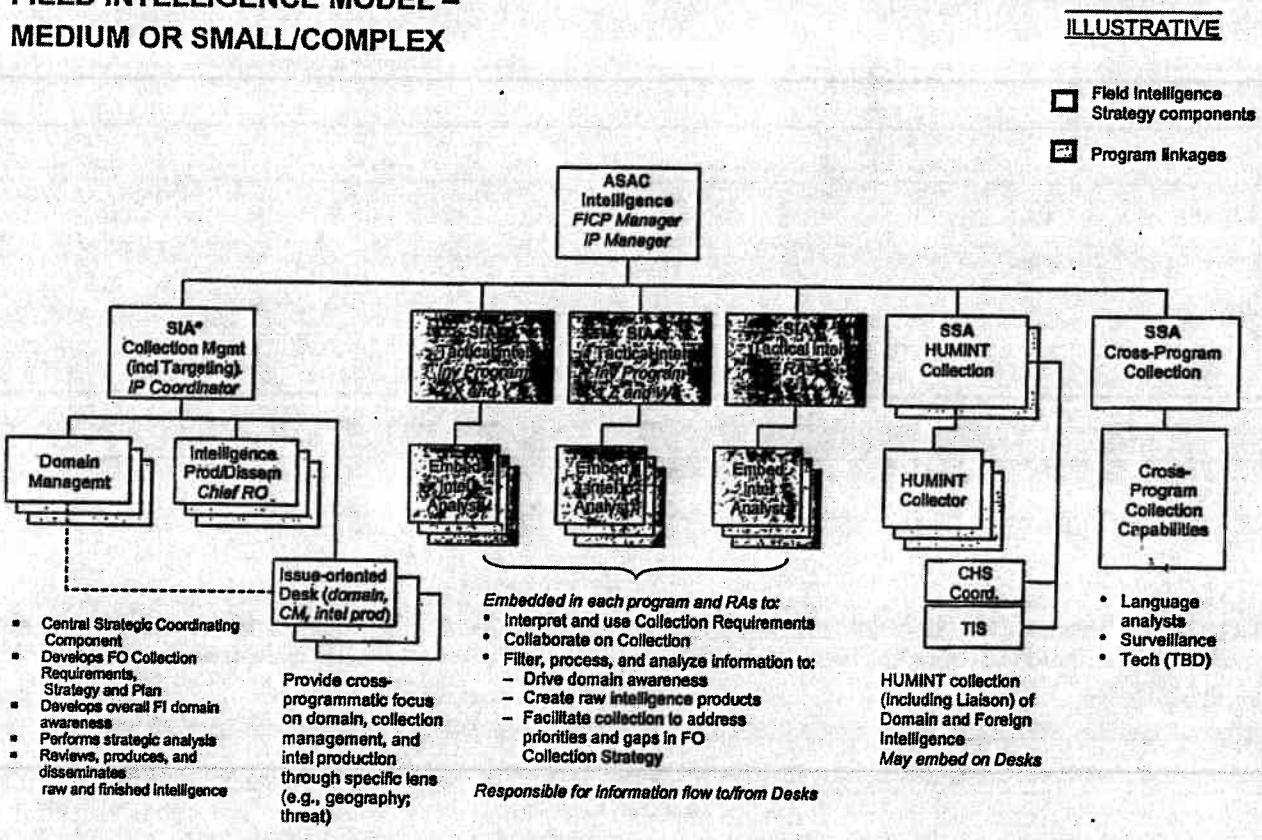


* In order to resolve short-term resource constraints, this position can be filled by an SSA. Currently St Louis, Richmond, Little Rock, Jackson, Mobile, Anchorage do not have SIAs

In the 38 to 40 field offices classified as medium or small/complex, the field intelligence model includes the core functions and some specialization against the highest priority local issues.

FIELD INTELLIGENCE MODEL – MEDIUM OR SMALL/COMPLEX

ILLUSTRATIVE

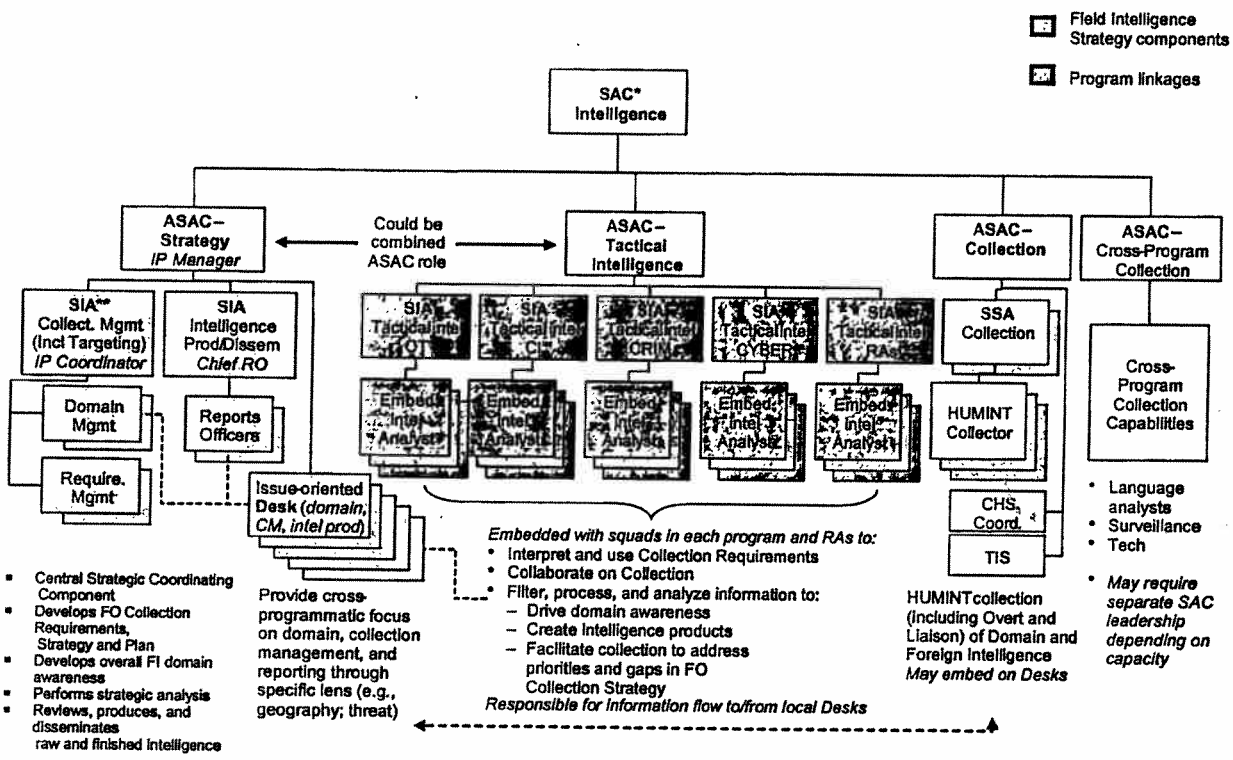


* In the immediate term, in order to resolve resource constraints, this position can be filled by an SSA.

In the largest three to five field offices, the structure includes a high level of specialization against highest-priority issues (most relevant geographies and threats) through both the Desk structure and specialized tactical components.

FIELD INTELLIGENCE MODEL – LARGE

ILLUSTRATIVE



* SAC or Associate SAC, depending on individual FO resourcing
** In the immediate term, in order to resolve resource constraints, this position can be filled by an SSA

Flexibility in Implementation

The field intelligence model has certain fixed requirements, but also includes flexibility to allow field offices to respond to local needs and obtain unique local intelligence. During the implementation, the SET leadership will sit down with the SAC to discuss any particular resource challenges in the office and develop a short and long term strategy for developing the core intelligence functions through the field intelligence model.

The model is a "build to" design that requires that first field offices invest in the central strategic coordinating component first. This component must have a Funded Staffing Level (FSL) of at least three, but should be larger based on the size of the field office and the complexity of its domain. Members of the Directorate of Intelligence and SET will work with each field office in advance of implementation to help identify personnel to fill key initial positions within the FIG, as well as help the office map a solution for full model implementation into the future.

Other rules for implementation:

- All offices should have distinct intelligence leadership role at the ASAC level or above. In offices headed by as ADIC, this position should be filled by an SAC-level executive.
- All field offices must have dedicated intelligence collection capabilities, but the staffing level should be determined based on the size and complexity of the domain.
- All offices must have a Chief Reports Officer, regardless of the size of the office.
- All offices must have intelligence analysts embedded with investigative program and Resident Agency (RA) squads. The responsibilities of these analysts must be consistent across all field offices. However, how many analysts are embedded and where they are assigned may vary based on specific field office needs.
- All field offices should consolidate cross-program collection capabilities (e.g. surveillance, language analysts) under the ASAC (or SAC) for Intelligence. Additional supervisory positions may be required to ensure reasonable spans of control, particularly in offices with a large number of language analysts.
- SET will work with each field office to determine the best way to apply the model to the RAs depending on RA size and the overall level of decentralization.

Desk Operations Team

Field offices will have a Desk Operations Team only in instances where a Domain Assessment, validated by FBIHQ, indicates the unique presence of a particular threat and it is determined to be a priority use of limited resources. Desk Operations Teams report to the ASAC in large offices. In rare instances where a Desk Team is required in a medium or small office, the team reports to the SIA for Collection Management.

Depending on its focus and size, the Desk Operations Team may be made up of:

- (Senior) Intelligence Analyst (Subject Matter Expert)
- Reports Officer
- Embedded Analyst (could be Operations Specialist)
- Language Analyst (virtual as needed)
- Collection Squad Special Agent (may be virtual)
- Investigative Squad Special Agents (virtual and as needed consistent with threat set)

The Desk Operations Team is effectively a task force that applies focused and unique subject matter expertise (geography, culture, language, political/governance, religion, military, economics, etc.) on key or critical threats (within a larger picture of threats and issues) and provides a unified effort of intelligence and investigative activities. This Team "goes deep" on a specific set of threats or issues while the field office's Domain and Collection Management "goes wide" to capture the fullest picture of known and emerging threats, indicators, vulnerabilities, and intelligence gaps.

Outputs of the Desk Team may include:

- Newly identified indicators and intelligence requirements
- Completed and tasked Target Recommendations
- Collection Strategies and tasks
- Intelligence Information Reports (IIRs), and finished intelligence reports
- Updated Common Operational Picture
- Threat mitigation strategies

Desk analysts are vital hubs in an information network. They work seamlessly with FIG collectors, investigative squads, Collection Management and Domain Management Coordinators, and the Chief Reports Officer, to contribute to an integrated national picture on the issue – one that can inform decision making at the highest levels of the Bureau and the federal government.

Desk officers' performance will be measured by:

- High-priority threats detected, penetrated and dismantled
- Volume and quality of reporting from collection platforms
- Quality and priority of Source Directed Requirements, Intelligence Information Need(s), Requests for Information (RFIs) and/or Notice(s) of Intelligence Potential met and generated by Desk
- High-priority, quality and timely responses to customer requests for collection (especially foreign intelligence)
- Depth and breadth of intelligence production (IIRs, bulletins, etc.) against priority needs
- Level of cross-program demand for participation in intelligence activities run by/from Desk

For more information, see the Field Intelligence Model How-To Guide.

ROLES AND RESPONSIBILITIES

This section provides an overview of the major field office work roles that will be created or significantly impacted by the new field intelligence model. This list is not intended to be all inclusive. Positions and work roles that are not described here generally will continue to exercise their current responsibilities.

It is the responsibility of employees in all career paths and programs to work collaboratively as a team and to support the field intelligence mission. All personnel should contribute to the FBI's efforts to stay ahead of threats by seeking out new knowledge, working to achieve their full potential, and helping others to do the same.

Leadership

Special Agent in Charge (or ADIC)

It is the SAC's responsibility to ensure that the field office is performing the basic intelligence functions effectively, that good collaboration is occurring within the office and that all personnel in the office understand their role (and the roles of the people they need to work with).

The SAC is responsible for ensuring that key positions and work roles are filled by personnel with the capabilities to perform those roles (as they are now defined) successfully. This will require strong leadership from the top and down to the squad supervisor level.

The SAC will interact with the FIG frequently to maintain and continually improve on the FO's understanding of the field office's territory, demographics, vulnerabilities, and primary threats. He/she must also be familiar with major intelligence requirements and the office's progress in satisfying those requirements. Based on this knowledge, the SAC will direct prioritization and resource allocation within the office. The SAC will receive, review, and approve, major products of the FIG, including the Domain Assessment, Common Operational Picture (COP), and FO annual collection strategy.

Through this regular interaction with the FIG, the SAC will send a strong message to the rest of the field office that intelligence is central to what we do, that the FIG is important to the FBI's success in achieving our mission, and that working on the FIG is career enhancing. Through actions, it is important that the SAC clearly convey this message.

The SAC has particular influence over the focus, mood, tone, and level of engagement in the office. The SAC will reinforce the necessary mindset by setting out clear expectations, and will reinforce this new message with strong, consistent communication to ensure that communication does not reinforce old ways of thinking. The SAC will ensure that new personnel coming into the office receive an appropriate and timely orientation that reflects new roles and responsibilities.

External communication is important as well. The SAC opens doors for the office through liaison with law enforcement and other federal partners and through involvement in a strong community

outreach program that builds trust and confidence in the FBI. The SAC must also support a proactive media relations program, participate personally in these efforts, and encourage personnel in the office to participate. This participation will inform the general public and key decision makers about the FBI's role in protecting Americans from threats to their way of life. Efforts will be made to promote positive stories about the FBI's intelligence efforts and national security focus.

The SAC will participate in bi-monthly review sessions with the Deputy Director, and then will cascade that process through the field office by holding quarterly progress reviews with supervisors. Ultimately, it is the SAC's responsibility to hold personnel in the office accountable for their contributions as individuals and members of a team.

Seven Questions SACs Should Be Able to Answer
(With Checklist for Finding the Answers)

What are my most important threats?

How to answer this...
- *Compare national prioritized threats with what is in my domain (e.g. what is important to local partners)*
- *Assess important open cases*
- *Assess Common Operational Picture of the domain*
- *Assess collection directives*
- *Observations of risks in AOR from Liaisons*

In order to answer this I need...
- *Prioritized set of threats from FBIHQ that are not strictly bounded by investigative programs*
- *Comprehensive case review*

How am I addressing these known threats?

What I would do to answer this...
- *Use a source survey to ensure all confidential human sources' access and placement has been analyzed in relation to requirements (examine utilization of sources)*
- *Catalog all technical collectors (FISA, TIII)*
- *Catalog all other collectors and their capabilities (SSG, SOG, Lookouts, Language Analysts, Undercover)*
- *Create a regular collection plan aligning threats with collection and liaison capabilities*

In order to answer this I need...
- *Access to source files/ELSUR files*
- *Comprehensive database with security controls*

What are my emerging threats?

What I would do to answer this...

- *Look for patterns and trends. Are there recurring events that do not quite reach the threshold for a case, but raise the possibility of an emerging threat?*
- *Maintain knowledge of current activities occurring nationwide and internationally (assassination, coup, mass protests, etc.)*
- *Determine whether national/international events or trends affect my AOR (i.e. Did the assassination of Benazir Bhutto in Pakistan have any impact on my domain?)*

In order to answer this I need...

- *Imagination and critical thinking*
- *Relationships in community that will inform on this question*
- *Baseline domain knowledge*
- *Access to sophisticated data research capabilities to identify patterns (e.g. "Targeter")*
- *Analytic capabilities to make optimal use of available data*

How am I addressing these emerging threats?

What I would do to answer this...

- *Extensive liaison with local/state law enforcement*
- *Extensive liaison with community; businesses, universities, defense contractors, agencies, etc...including new targeted liaison (not just existing relationships)*
- *Keep asking "What else can I do?"*

In order to answer this I need...

- *A broad network of contacts positioned to penetrate the threat*
- *Ability to recruit, develop, and retain sources for long periods despite their current lack of reporting*
- *An established centralized Liaison program and system to support inventorying partner capabilities and assets*

What are the highest priorities between my standing, local, and ad hoc requirements?

What I would do to answer this...

- *Assess ;*
  - *Cases*
  - *COP and Domain Assessment*
  - *JTTF and other task force issues, local policy makers concerns*
  - *Directors priorities*
  - *Standing requirements*
  - *Other (Amber alerts, local events, etc...)*
- *Determine whether local requirements rise to the level of a federal agency response*
- *Determine if the standing priorities exist in my territory*

- *Based on the strategy of "understand in order to dismantle", assess what you know of each threat with an eye toward prioritizing to address the most critical threats you know least about.*

In order to answer this I need...
- *Meetings with JTTF partners and local policy makers*
- *Tailored requirements*

What are my capabilities, speed, and confidence?

What I would do to answer this...
- *Leverage my collection capability assessment - an inventory of the source base and their access as well as HUMINT and other intelligence capabilities*
- *Build a Collection plan to align your collection capabilities with requirements.*
- *Assess the degree of confidence in sources' access and the capability of other intelligence platforms*
- *Assess the relationship developed by the Liaison group relative to my priorities*

In order to answer this I need...
- *More IAs dedicated to predictive and strategic analysis*
- *To assure individuals that they will not be punished if predictions turn out to be incorrect*
- *A database that stores existing capabilities of all collectors and partners*
- *A continuing knowledge of trends, technology and techniques*

What are my most critical knowledge gaps and plan of attack?

What I would do to answer this...
- *Targeting for the highest priority gaps*
- *Analyze existing and potential capabilities to determine who can most effectively collect against these gaps*
- *Identify other Field Offices' that may be capable of collecting in your domain*
- *Leverage Liaison capabilities*
- *Look at cross-program National Intelligence Assessments to see how they compare to your domain*

What I need to answer this...
- *Targeting process conducted*
- *Internal FBI requirements management system enterprise-wide*

Intelligence Program Manager

The IP Manager will lead the field office's intelligence program and be responsible for overseeing the functions of the FIG and ensuring that the field office succeeds in its intelligence mission. He/she will accomplish this through four sets of interactions.

- First, the IP Manager must interact routinely with the field office's executive management. The IP Manager will manage all SAC and ASAC briefings on intelligence matters, and inform the SAC on the intelligence performance of the field office. The IP Manager will lead efforts to use the domain management process to develop and maintain a COP and Domain Assessment. He/she will oversee annual delivery of the field office's collection strategy for consideration and implementation by executive management and will chair regularly scheduled executive intelligence review meetings regarding progress made against collections strategies and plans.

- Second, the IP Manager must interact with FIG personnel. The IP Manager has responsibility for operational and administrative oversight and is required to provide FIG supervisors and personnel with guidance and direction on all aspects of the field office's intelligence activities.

  The IP Manager will make personnel assignments for field intelligence functions, and is also responsible for helping members of the Intelligence Career Service in the field office to reach their full career potential. The IP Manager will arrange, coordinate, and deliver standardized intelligence training for all Intelligence Program personnel, identifying both internal and external training opportunities. The IP Manager must ensure that FIG personnel have the basic tools they need to get their jobs done.

- Third, the IP Manager must interact with field office personnel outside the FIG, particularly managers and supervisors, to integrate intelligence into the existing structure of the field office. This will require daily interaction with the ASACs over the investigative programs to ensure that operational squads are fulfilling collection plan requirements. The IP Manager will determine which intelligence functions require access to specific technology capabilities and other support services available within the field office.

- Fourth, the IP Manager will interact routinely with FBIHQ to receive guidance and direction as required. The IP Manager will then ensure that all appropriate members of the FO are knowledgeable of the intelligence policy guidance and other information produced by FBIHQ impacting the intelligence mission.

Qualifications: Candidates for this position should have served in a FIG. The candidate should have a degree or certificate from an ODNI-recognized intelligence training program or educational institution. The candidate should be very familiar with the intelligence structure at FBIHQ, process, and protocol) and ideally will have served in an intelligence program assignment at FBIHQ for at least one year).

Performance: The IP Manager's performance will be measured by: (1) quality of the field office's intelligence collection strategy and results; (2) number and quality of executive briefings/summaries concerning FO performance against collection plan; (3) quality and effectiveness of annual Domain Assessments to enable effective FO executive management

decision-making; (4) quality and results of Requests for Information (RFI's) sent to appropriate FBIHQ component or USIC or Law Enforcement partner.

The IP Manager will participate in monthly performance dialogues with the SAC.

Intelligence Program Coordinator

The IP Coordinator will be a full-time work role. In small offices, the work role may be combined with the functions of the Collection Management Coordinator.

The IP Coordinator will be a deputy and principal advisor to the IP Manager on functions related to Collection Management, Domain Management, production and dissemination. The IP Coordinator will be responsible for the effective coordination, operation and measurement of field intelligence activities within the FO.

The IP Coordinator will assist the IP Manager with some of the "nuts-and-bolts" management of the FIG. The IP Coordinator will monitor progress on intelligence plans and ensure that the FIG is producing actionable intelligence products. The IP Coordinator will interpret and apply organizational intelligence policy, directives, and provide guidance to ensure effective field intelligence function.

The IP Coordinator has a number of responsibilities related to performance management. The IP Coordinator will produce the Intelligence Semi-Annual Program Review (SAPR), monitor and interpret the field office's metrics and scorecards for executive management, and provide quality assurance of data across programs, reconciling data discrepancies where necessary. The IP Coordinator will prepare the SAC for Strategy Performance Session (SPS) discussions every 60 days and participate in those discussions. The IP Coordinator will organize monthly SAC SPS discussions with ASACs and Supervisory Intelligence Analysts (SIAs), and document and resolve issues/actions for those discussions.

The IP Coordinator also will serve as a principal point of contact between the FIG and the Directorate of Intelligence FIG Oversight Unit on matters related to intelligence unit policy, function, coordination, and metrics. The IP Coordinator will chair the Field Office Program Coordination Group composed of program coordinators from each operational component.

Qualifications: A successful candidate for this position must have demonstrated leadership skills and sound judgment. The IP Coordinator must have expertise with FBI intelligence functions, excellent oral, written communications, and liaison skills; strong teaming and organizational skills; strong data analysis/quantitative skills; familiarity with the operations, capabilities, and activities of other USIC entities.

Performance: Performance will be measured by: (1) quality and velocity of response to RFIs from FBIHQ; (2) documentation of intelligence management reviews, including agendas, participants, and outcomes; and (3) documentation of performance metrics and "proof of use" to enable informed decision making.

FIG Centralized Strategic Coordinating Component

SIA – Centralized Strategic Coordinating Component

Field offices will have a Supervisory Intelligence Analyst over the Centralized Strategic Coordinating Component. He/she will report to the IP Manager and will be responsible for leading, planning, directing, and reviewing the work of Intelligence Analysts engaged in Collection Management, Domain analysis, reporting and production. He/she will not supervise the analysts embedded in operational squads who report to the SIA for Embedded Intelligence. In smaller offices this SIA's responsibilities may be combined with the Collection Management Coordinator.

The SIA will oversee the field office's strategic efforts to detect indicators, trends, patterns, anomalies, and gaps in knowledge of known and potential threat activity. He/she will facilitate integration of domain awareness/analysis activities between the field office and FBIHQ/the USIC, and will advise the CollMc, field office executive management and FBIHQ on the strategic domain knowledge required for effective decision-making, including the allocation of field office and other resources to collect further intelligence about priority issues, topics, and threats of the most concern in the field office's domain, and to proactively identify and neutralize those threats.

Qualifications: This position must be filled by an SIA. It requires strong managerial capabilities, exceptional interpersonal skills, including the ability to coordinate with others to achieve work results and to coach IAs. Candidates should have broad knowledge of intelligence operations, knowledge of Collection Management, analytic techniques and standards, and reports tradecraft; familiarity with and the ability to facilitate the entire intelligence process; familiarity with USIC standard practices and resources and the ability to leverage external USIC partners; finally, project management skills, including planning and evaluation.

Performance: The SIA's performance will be measured by the quality of products and briefings coming out of the Collection Management and Domain Management processes as well as the overall quality, timeliness and responsiveness to requirements of other intelligence products.

Collection Management Coordinator

The CollMC will be dedicated to a full-time set of duties in all field offices. The CollMC will coordinate the collection management efforts of the field office through the development and execution of the field office's Collection Strategy, Collection Plans and Taskings, Collection Capabilities Assessment, Targeting efforts against collection gaps, and Collection Posture.

The CollMC has overall responsibility for evaluating efforts to meet the Collection Plan, and will coordinate the entire field office's intelligence collection efforts through the following process:

1. Examine the field office's prioritized requirements
2. Examine the field office's collection capabilities to determine the office's ability to meet the prioritized requirements with existing sources
3. Identify gaps between our requirements and our current ability to collect information to satisfy those requirements

4. Coordinate with internal and external partners to see if there are additional capabilities that we can tap into to help us satisfy requirements
5. Coordinate development of field office Collection Strategy
6. Develop Collection Plans that include leveraging existing sources and developing new sources
7. Ensure that intelligence that is collected is funneled back to the FIG as well as the requestor of the information and track overall progress on Collection Plans

The Collection Management process will require a great deal of coordination.

- The CollMC will work with the Domain Management Coordinator to prioritize requirements most important to the FBI field office (based on domain awareness).

- He/she must interact with FBIHQ to constantly remain updated on the latest national level requirements, and must also keep apprised of local requirements by collaborating with federal, state, local, and tribal partners; regional USIC partners; field office executive management; FIG personnel; and investigative squad supervisors to identify local intelligence information needs (IINs). Based on this input, he/she will consolidate, deconflict, and prioritize intelligence requirements, and provide a consolidated, prioritized list to field office managers to assist them in prioritizing collection activities and resource allocations.

- The CollMC will work closely with the Confidential Human Source (CHS) Coordinator to assess human source capabilities and to validate the collection capabilities assessment and prioritization of local requirements (i.e. quality, quantity, and capability of human source, technical, and physical coverage against its criminal and national security threats).

- To inform the collection management process, the CollMC will issue requests for information to appropriate FBI counterparts or USIC and law enforcement partners through FBIHQ when field office capabilities are inadequate to fill collection plan requirements.

- The CollMC will inform FBIHQ of the field office's collection capabilities and coordinate with FBIHQ on the implications of the overall national strategy for the local collection strategy.

- The CollMC will network with local, regional and national counterparts to appreciate wider trends, concerns, tactics, and resources.

The CollMC will prepare a Collection Strategy and Collection Plans. With approval from local executive management, the CollMC will then turn those plans into action through specific taskings that cascade through the ASAC chain of command down to operational squads and ultimately to individual Special Agents. The CollMC will manage targeting projects to develop new sources when existing sources cannot fill collection gaps. The CollMC will deconflict targeting projects and other FIG collection efforts with operational squads' cases and source development. The CollMC will also answer inquiries to provide clarification for investigative squads' collection plans.

The CollMC will compare raw reporting against existing requirements to monitor progress in collection. This will be coordinated through the CRO who will be the recipient of all raw

intelligence to be disseminated from the FO. The CRO will track the reporting for its velocity and throughput ratios while the CollMC tracks reporting in relation to requirements.

Finally, the CollMC will maintain and provide local executive management with metrics showing the performance of all programs, squads, and individual personnel in the implementation of the collection plans.

Qualifications: The CollMC position may be filled by an SIA. It requires a high-performing individual with strong knowledge of national and FBI requirements and local collection capabilities. It requires the ability to think strategically for the organization and support translation of strategy into action. He/she must have strong liaison and interpersonal skills in order to handle the extensive interaction with internal and external interests that the position entails, and the ability to command broad respect throughout the field office in order to be effective.

Performance: The CollMC's performance will be measured by: (1) achievement of clearly articulated strategic goals; (2) existence and quality of synthesized set of intelligence requirements for the field office, based on relevant domain knowledge and a documented methodology of prioritization; (3) incorporation of national and local requirements into field office collection plans; (4) existence/implementation of Field Office Collection Strategy and Collection Plans; (5) Documentation of FIG personnel and investigative squads' collection against Plans; (6) Quality and results of RFI's sent to FBIHQ or USIC or law enforcement partners; (7) Number and quality of executive briefings/summaries concerning field office performance against collection plans; (8) Timeliness and quality of responses to FBIHQ inquiries concerning the field office's collection efforts; (9) Quality of the office's targeting strategy and results.

Domain Management Coordinator

The Domain Management process and its products provide the basis for investigative, intelligence and management direction. The DMC has a full-time set of duties in all field offices. He/she will be responsible for implementing and operating a continuous, systematic approach to maintain a strategic understanding of the field office area of responsibility (AOR). This includes production of the COP and an annual Domain Assessment for the field office, including both regularly scheduled publications and continuous identification of issues that can be uniquely addressed by local capabilities. The DMC may manage or work with a team of analysts, depending on the size of the FIG, and will ensure adherence to data and methodology standards.

To develop products, the DMC must interact continually with FIG personnel and operational squads to seek, receive, consolidate, assess, vet, and synthesize locally-provided data, leveraging information that exists within the Bureau. The DMC will identify intelligence gaps (interacting with operational squads to solicit and receive input regarding relevant investigations) and manage strategic efforts to detect patterns and potential changes in patterns of threat activity.

With this information, the DMC will advise the Collection Management Coordinator, local Executive Management and FBIHQ on the strategic domain knowledge required for effective decision making, including the allocation of field office and other resources to proactively identify and neutralize threats.

The DMC will be responsible for facilitating the integration of domain awareness/analysis activities in the field office as well as across the region/nation. This will be the basis for finished intelligence products suitable for dissemination to the USIC and federal, state, and local law enforcement partners. The DMC will coordinate with regional and national counterparts, submitting the local domain assessment to drive broader context and receiving/processing information on the regional/national domain in order to drive more effective local domain awareness. The DMC will interact with local law enforcement and USIC partners to exchange or coordinate the exchange (by other field office personnel) with partner's relevant intelligence and analysis on threats, vulnerabilities, intelligence gaps, and capabilities in the domain. The DMC also will coordinate with liaison programs, such as InfraGard, Counterintelligence domain efforts, and Community Outreach, to deconflict and leverage efforts, and to facilitate the integration of domain awareness/analysis activities in the field office, as well as across the region/nation.

Qualifications: This position can be filled by an experienced Intelligence Analyst. It requires strong quantitative and qualitative analytical skills, critical thinking skills, as well as strong writing, editing, and oral communications skills. Familiarity with USIC analytic standards and an aptitude for database management and use of FBI IT tools (e.g. ArcGIS) is also required.

Performance: Performance for this position will be measured by: (1) existence and quality of a domain methodology and implementation as shown by documented use of domain data sets, tools, analysis; (2) existence and quality of a common operational picture for the territory; (3) number and quality of intelligence products; (4) the number and quality of executive briefings; (5) existence and quality of collection capabilities assessment; (6) quality/timeliness of responses to FBIHQ inquiries regarding domain knowledge; (7) documentation of field office variables/characteristics that influence FIG design and field office intelligence operations.

Chief Reports Officer

Every field office must have a full time, certified CRO. The CRO will be accountable for field office production of accurate, timely, and professional raw intelligence products. The CRO has several related areas of responsibility, related to the quality, prioritization, and analysis of raw intelligence in the field office. Upon completion of the CRO course, the CRO will be designated a Certified Release Authority (CRA).

First, the CRO should review raw intelligence products (IIRs) prepared in the field office to ensure that sources and methods are protected and USIC quality standards are met. The CRO is much more than an editor. He/she should add substantive value to IIRs to enhance their utility to the reader. The CRO will receive evaluation and RFIs from customers and produce follow-on source directed requirements and feedback for IIR drafter/reviewers. The CRO will ensure that sources relied upon in IIRs have been properly characterized (requires access to appropriate source files.) The CRO will also contribute to source validation efforts through Production Review.

To ensure ongoing quality, the CRO will mentor field office personnel on IIR development and writing. This includes working directly with investigative squads on all submitted raw intelligence to ensure accuracy, relevance, and quality and to help manage possible effects on case operations.

Second, the CRO should prioritize information dissemination based on knowledge of national and local collection requirements.

Third, the CRO contributes to the field office's Common Operational Picture by providing input to the DMC regarding trends identified based on review of multiple IIRs, including potential threats and vulnerabilities. The CRO also contributes to the field office's collection strategy and plans by providing input to the Coll MC regarding incoming intelligence against the Collection Plan, and potential source-directed requirements.

Fourth, the CRO receives, coordinates and reports on raw intelligence from collectors, embedded intelligence analysts and others, coordinating information flow in conjunction with the Coll MC. The CRO also coordinates with FBIHQ on regional and national production and Dissemination for IIR approvals.

Qualifications: This position can be filled by a Reports Officer or Supervisory Intelligence Analyst. The CRO must have exceptional written communications skills, with specific expertise on the policy and format requirements for IIRs. This position requires knowledge of the USIC, FBI, and locally generated requirements; strong knowledge of source lifecycle management; knowledge of source targeting. Excellent coaching, bargaining, and negotiating skills, and the ability to meet deadlines, are necessary as well.

Performance: Performance will be measured by:

- All IIR metrics, including the number of IIRs that address priority requirements (in the field office collection strategy), velocity rate, throughput rate, and any actionable results)
- Documentation of training and feedback for FIG personnel on IIR production
- Quality of source-directed requirements directed to field office

Who performs strategic analysis in the field?

Strategic analysis may be performed from anywhere within the FIG structure and by analysts assigned to any of the core intelligence functions. Analysts assigned to Domain and Collection Management functions perform strategic analysis as they work to assess the division's domain and collection capabilities. Reports Officers assigned as the Chief Reports Officer or assistant CROs also may perform strategic-level analysis as they work to understand and articulate reporting trends within the division and what those trends may mean. Analysts assigned to issue-oriented Desks would have strategic responsibilities associated with their assigned issues. Finally, analysts embedded with operational squads and Resident Agencies would have the opportunity to develop subject matter expertise in issues aligned with their squads' areas of focus.

Other FIG Positions

SSA – HUMINT Collection

The SSA for HUMINT Collection is a full time position in all field offices, reporting to the ASAC over intelligence collection.

The SSA for HUMINT Collection manages and directs HUMINT collection activities for the FIG. The SSA gets information from the CollMC on intelligence gaps which require non-case based collection, and feeds information from interviews and sources to the DMC to help inform the common operational picture. This involves enormous coordination with investigative squads to coordinate efforts to ensure deconfliction between investigative squad activities and FIG collection efforts.

Qualifications: This position must be filled by an SSA. It requires expertise in HUMINT tradecraft and policies and proven proficiency in source recruitment, debriefing, and handling (USIC certification is preferred). The position requires a strong foundation in the intelligence cycle as well as core agent investigative skills. This position requires an understanding of how to leverage all types of collection and be able to distinguish between the need for liaison and CHS operations. The position also requires appropriate subject-matter expertise and domain knowledge. The position will require interpersonal skills, including liaison skills to work with external partners, and the ability to effectively mentor and coach subordinates.

Performance: The SSA for HUMINT Collection's performance will be measured by:

- Percent of the squad's source reporting directly related to the field office's collection strategy and plan
- Tripwire coverage directly related to the field office's priority threats
- Number of jointly operated sources handled on the squad
- Satisfaction level of subordinates and fellow SSAs on substantive squads
- Percent of completed leads from Domain Management and Collection Management Team
- Recent and relevant training received

Special Agent HUMINT Collectors on the FIG

Each field office should have a minimum of three Special Agents who report to the SSA for HUMINT Collection. These Special Agents will use the full range of appropriate HUMINT tradecraft and operational skills to develop, recruit, and exploit sources and to leverage relationships with external partners in order to collect intelligence in the most critical field office collection gaps.

The HUMINT collectors' role is the exploitation of all HUMINT sources who provide intelligence which fills identified gaps as outlined in the field office's collection plan. They will work across all investigative programs in response to the FBI's priorities and collection requirements. They will identify potential Confidential Human Sources, assess their suitability and access, establish a relationship and recruit them, task them to collect against intelligence gaps and requirements, vet, validate, pay as appropriate, and end the relationship when appropriate. They may conduct

sensitive joint source operations with domestic and foreign partners. Along the way, they will generate IIRs based on CHS reporting to meet the needs of other squads and divisions, local partners, or the USIC.

HUMINT collectors on the FIG will coordinate the use of established and newly created liaison contacts as a HUMINT collection platform. There are several types of liaison relationships that will be leveraged. Some FIG Agents will serve in an official liaison role and coordinate with (and in some cases embed themselves within) federal, state, and local agencies to better understand their intelligence needs and to leverage non-FBI sources capable of collecting intelligence on our requirements (i.e. – local law enforcement partners). Other liaison relationships will be created one-on-one with private sector entities, non-governmental organizations (NGOs), academic institutions and other similar entities.

All Special Agents assigned to the FIG will work closely with analysts on the FIG to report observations indicating new trends in the local environment, and to spot areas and targets for source recruitment. FIG Agents will serve to facilitate the handling of cross-programmatic intelligence information obtained from CHS debriefings.

To do this effectively, HUMINT collectors on the FIG must have strong relationships with other collectors and embedded IAs on investigative squads in order to augment their collection abilities beyond reporting on the squads' investigations.

Qualifications: HUMINT collectors must have proven proficiency in source recruitment, debriefing, and handling. They also should have a strong foundation in core agent investigative skills, including an understanding of how to leverage all types of collection. They should be self motivated, independent thinkers, with the ability to recognize the demarcation between the need for liaison and CHS operations. They must have strong interpersonal skills, including liaison skills for working with outside partners. An enhanced understanding of the intelligence cycle and the FBI's integral role within the USIC is also required.

Performance: The FIG Special Agent's performance will be measured by:

- Volume and quality of internal and external disseminations
- Amount of source reporting directly related to priority requirements in the FO collection plan
- Significant contributions to domain awareness
- Effective operational testing of sources
- Effective establishment of "tripwires"
- Identification of additional intelligence gaps
- Recent and relevant training received

SIA – Embedded Intelligence

Every field office will have an SIA for Embedded Intelligence, and all but the smallest offices will have more. The SIA for Embedded Intelligence reports to the IP Manager and serves as manager and rating official for analysts embedded with operational squads. This position is a key bridge between strategic and tactical intelligence efforts in the field office.

The SIA for Embedded Intelligence should keep updated on collection plan requirements and investigative squad capabilities. The SIA collaborates with the operational squad supervisors and program managers to ensure that the capabilities of embedded IAs and squad SAs are leveraged to fulfill intelligence requirements.

The SIA for Embedded Intelligence reviews intelligence products created by embedded analysts for analytic value, quality, and source validation purposes, and then delivers them to Reports Officers for dissemination and to the central strategic coordinating component for strategic analysis. The SIA evaluates the appropriateness of analyst participation in source and detainee/arrestee debriefings and interviews (balancing value-add and safety).

In addition to these management responsibilities, the SIA pulls information together from across squads and programs to identify new issues, trends, patterns, intelligence gaps, and anomalies in FBI programs and cases, The SIA identifies the connections between subjects and persons of interest, and where appropriate, new targets (subjects and sources).

Qualifications: This position must be filled by an SIA. It requires strong managerial capabilities, including the ability to supervise employees in another location, mentoring junior analysts. It requires exceptional interpersonal skills, including the ability to coordinate with others to achieve work results, and to coach SAs and SSAs to effectively employ intelligence resources. Candidates should have broad knowledge of investigative operations and intelligence operations (e.g. knowledge of methods for collecting intelligence data), knowledge of collection, reporting, and Domain Management; familiarity with and the ability to facilitate the entire intelligence process; familiarity with USIC operations and resources and the ability to leverage external USIC partners; finally, project management skills, including planning and evaluation.

Performance: The SIA's performance will be measured by the contributions of supervised embedded analysts to the field office's Collection Plan and Common Operational Picture, as well as analysts' intelligence production.

Embedded Intelligence Analyst

Embedded Intelligence Analysts report to the SIA for Embedded Intelligence, but physically sit with an investigative squad. From this vantage, they act as a link to FBI operations for intelligence and investigative priorities. They coordinate and provide focused intelligence requirements to investigators for use in all investigative activities, as appropriate. They work directly with investigative personnel on the squad to ensure FBI operations fulfill intelligence requirements. They participate in and/or provide interview guides for source and detainee/arrestee debriefings, interviews and asset validations (balancing value-add and safety).

Embedded Analysts have multiple responsibilities. First, they aid the field office with close-to-real time reporting. Because they are present on the investigative squads and at the resident agencies, they are familiar with their squads' cases and sources, and are aware of the information those squads and cases are generating. This aids efforts to identify reportable information as early as possible and compress the amount of time it takes to move information from point of collection to dissemination.

The second critical activity of embedded analysts involves assisting the squad or resident agency, in partnership with the SSA or SSRA, achieve its intelligence collection responsibilities as detailed in the squad's portion of the division's Collection Plan, and to report the outcome of those efforts to the central, strategic coordinating component within the FIG on a day-to-day basis. Individual squads and resident agencies, based on their existing sources and case work, will have specified tasks assigned to them through the division's Collection Plan. The embedded analyst will help the SSA or SSRA ensure that the squad's results against those assigned tasks are assessed and reported when appropriate.

The third responsibility of embedded analysts is to identify and help the squad or resident agency capitalize on intelligence collection opportunities that have not previously been specified within the Collection Plan, but that present themselves during the course of day-to-day investigative efforts. For example, an agent investigating a drug matter plans on interviewing a cooperating subject located at a country jail, and the division has a concern about the potential for terrorist organizations or affiliates to radicalize and recruit inmates at that facility. The embedded analyst would be the person to alert the interviewing agent of the potential for the collection of information associated with prison radicalization and recruitment. Additionally, the analyst would provide the agent with only those additional questions that should be asked, and advise the central, strategic coordinating component within the FIG of the results of the interview. In summary, embedded analysts assist squads with the interpretation and use of intelligence requirements to maximize intelligence collection opportunities across programs.

Finally, embedded analysts analyze information developed during the course of investigations to help develop the FO's view of its domain, further ensure that reportable information is identified as quickly as possible, and add value to investigations by assessing how the squad's threat issues are evolving. Cases needing action, having gaps in knowledge and potential for impact from other cases or sources, will be highlighted.

Qualifications: These positions can be filled by an OS, AS, or RO. Embedded IAs must be skilled in hypothesis-driven analysis and problem-solving. Candidates should have familiarity with USIC operations and resources; ability to leverage USIC partners; subject-matter expertise in the field of intelligence operations (knowledge of methods for collecting intelligence data), deep target knowledge, as well as knowledge of a professional discipline such as international relations or military science. To succeed in a fast-paced operational environment, the embedded analyst must be able to work under pressure and meet tight deadlines. To function as a member of the team, they need excellent people skills and the ability to persuade and inform, verbally and in writing.

Performance: Performance will be measured by the number of IIRs against priority intelligence requirements, internal feedback in IIR quality and relevance, and new sources recruited and PIRs satisfied via targeting.

Staff Operations Specialist

The Staff Operations Specialist (SOS) will provide operational support to Intelligence Analysts and Special Agents who are involved in analyzing intelligence data. The SOS will be assigned to the FIG in support of the intelligence mission, and will report to the SIA or SSA of the FIG.

The SOS is an entry level professional position beginning at the GS-7 level with promotion potential to the GS-12 level. It is intended to provide the employee with the necessary knowledge, skills, and abilities to become either a Special Agent or Intelligence Analyst.

Qualifications: The SOS position should be filled by a recent college graduate (past two years) who received a GPA of 3.0 or better, and must be familiar with key FBI systems (ACS, Guardian, IDW, Telephone Applications) and commercial systems such as Microsoft Office applications, Lexis Nexis and Choicepoint.

Performance: [TBD]

Outside the FIG

SSA – Operational Squad

In addition to their existing responsibilities, squad supervisors will work with the FIG, particularly the SIA for Embedded Intelligence, to ensure that their squads' activities support the field office's collection plans, to fully leverage the squad's source base to address the most critical requirements.

In instances where a source may have the ability to provide intelligence that is responsive to an intelligence requirement, it is up to the SSA to ensure that the source's handler is familiar with the relevant requirements, asks the source appropriate questions, and reports any responses that may have intelligence value. The SSA, working with the SIA for Embedded Intelligence, will identify situations where it is appropriate for analysts to participate in interviews and debriefings. Where an SA must question or task a source on an unfamiliar issue, then the SSA should get assistance from Agents on the FIG or locate an appropriate subject matter expert to provide guidance or participate.

Finally, the SSA should conduct file reviews every 90 days that cover both case work and contributions to meeting intelligence requirements.

Case Agent

The case agent continues to conduct investigations to support prosecutions, but is better integrated into the field office's intelligence functions. Case agents will work more closely than in the past with the FIG, and will benefit from the assistance provided by the FIG's development of a COP and Domain Assessment which will be accessible to agents to help them better assess their operating environment.

SAs will perform source handling and documentation which is an integral part of the Collection Management process. If the agent has a source, then the source should be questioned to gain information for both the case and any intelligence requirements that the source may be able to address.

Community Outreach Specialist

The Community Outreach Specialist (COS) should be a full time position in most offices, reporting to the SAC. (In New York and Los Angeles the COS may report to the supervisor over public affairs.) In the smallest offices, the position may be combined with the functions of the EEO coordinator or media coordinator.

Under the new field intelligence model, the COS will continue to coordinate the Citizens Academy and Community Relations Executive Seminar Training (CREST), and serve as a liaison to the Citizens Academy Alumni Foundation. The COS will oversee Community Engagement Councils and Regional Advisory Councils, communicate with various ethnic and minority communities, and coordinate donations of abandoned property to organizations where entrée has been lacking. The COS may also coordinate programs in local schools when such outreach is determined to open a needed dialogue with a particular community.

While the COS is not, and should not be, under the umbrella of the FIG, the COS should coordinate with Special Agent Liaison Specialists on the FIG to "open doors" for the FIG and other field office components in the local community. The COS can leverage the Office of Public Affairs, Community Relations Unit's national level outreach to ethnic, religious, and other community-based groups and organizations. The COS can also leverage relationships built through the Citizens Academy, CREST and other outreach programs. The COS, who optimally has roots in the community, can also serve as additional "boots on ground" for the field office, particularly to establish a positive dialogue in insulated or isolated communities that may be distrustful of law enforcement.

The COS will also work closely with the field office's media coordinator to market and generate positive press coverage of the office's community outreach activities. The COS can serve as the public face of the office's community outreach program in instances where the FIG Liaison Officer wishes to keep a lower profile.

The COS's focus will be governed by national and local intelligence priorities. For instance, if MS-13 gang activity jumps in a particular area, the COS should expand outreach to Latino communities where MS-13 might be present.

Qualifications: The COS must have effective interpersonal skills and superior organizational skills. An ability to relate to people from varied ethnic and minority backgrounds is essential. The COS must possess self-control and maintain composure so that criticisms and disparaging remarks aimed at the FBI by groups frustrated by FBI action or inaction do not embroil the COS in public controversy. Proficiency in a foreign language would be a plus but would not be required.

Performance: The performance of the COS will continue to be measured by the criteria outlined in the semi-annual report mandated by the Community Relations Unit. Those criteria include the number of Citizens Academies held, the number of CRESTs held, the amount of outreach conducted in ethnic and minority communities, youth initiatives, federal, state and local partnerships, participation in the Abandoned Property Initiatives, and the ability of the COS to achieve management support for the outreach program.

DOMAIN MANAGEMENT

Domain is the territory and issues for which a field office exercises responsibility. Domain is also known as Area of Responsibility (AOR).

Domain Awareness is the strategic understanding of national security and criminal threats and vulnerabilities, the FBI's positioning to collect against these, and knowledge gaps related to a specific Domain. An FO always has a level of Domain Awareness, but in the past, this Awareness was not regularly centralized, managed, and analyzed.

Domain Management is a systematic *process* by which we develop cross-programmatic Domain Awareness in the FO, improve that Domain Awareness, and then leverage it to enhance our abilities to anticipate and neutralize threats. With Domain Management in place, at any given moment, a DMC and the Domain Team of analysts can capture a snapshot of the FO's current level of Domain Awareness and provide it to customers, either within the FO or at FBIHQ.

The Domain Management process is based on four fundamental questions:

- *What do we already know about our domain?*
- *What don't we know about our domain?*
- *What do we need to know about our domain?*
- *What are we going to do about it?*

The purpose of these questions is to continually drive the DMC and the Domain Team's efforts to improve Domain Awareness. These questions are not meant to be answered once and forgotten. They must be constant analytical and collection drivers.

Domain awareness creates the capability for:

- **Proactive identification of threats** (helping us stay ahead of those threats)
- **Strategic management of current investigative activities** (putting resources where they can do the most good)
- **New opportunities for collection and prosecution** (furthering the efforts of every squad and program)
- **Setting tripwires in the community** (using targeted liaison to give us advance warning)

Domain Management will allow field office management to:

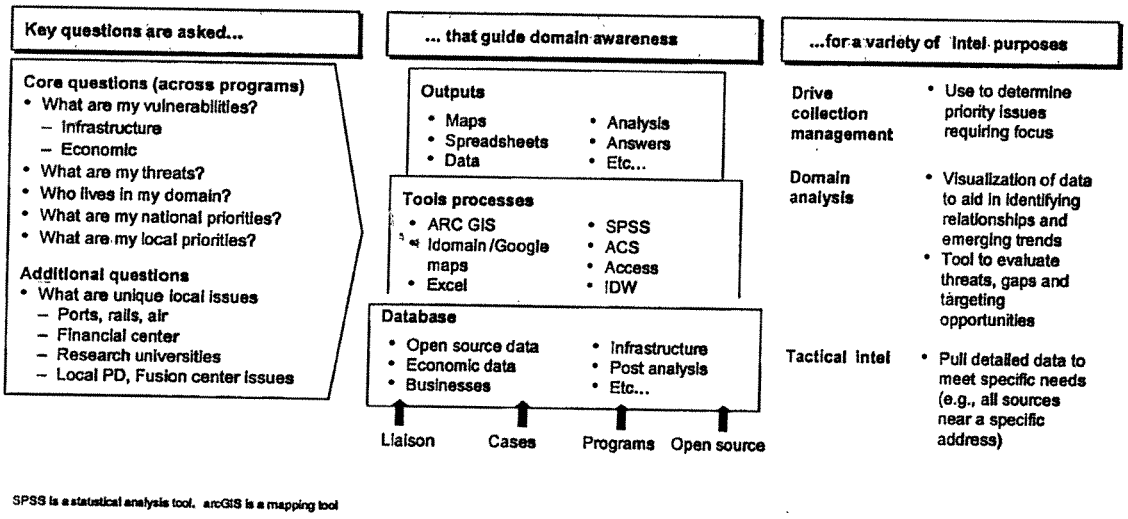
- identify and prioritize threats and vulnerabilities of the field office domain;
- conduct analysis/research on affiliated entities;
- engage entities through direct personal contact, with interagency/local cooperation;
- know timely and relevant threat information that could be provided to vulnerable domain entities, if appropriate;

- leverage domain entities for CT, CI, Cyber, or Criminal information and foreign intelligence;
- and conduct operational activities for filling FBI and USIC requirements, leads, case openings, etc.

Domain Management at the FO level will also enable Domain Awareness at FBIHQ, enabling the Bureau to develop a national awareness of threats and vulnerabilities. This national awareness will ultimately guide our national program management and inform decision makers at the highest levels of the federal government.

Domain Management must be cross-programmatic to be successful. Counterintelligence or criminal matters cannot be neglected to the "benefit" of counterterrorism, or vice versa. Only if our Domain Management gives equal attention to all programs are we positioned to see liaison and outreach efforts uncovering criminal cases and possible links to other programs. Without equal attention, such opportunities may be missed and every priority will suffer.

DOMAIN AWARENESS SUPPORTS THE FBI's MISSION



SPSS is a statistical analysis tool. arcGIS is a mapping tool

Baseline Domain Awareness in the field office

For years the field offices have had a variety of sources that have been collecting intelligence on the domain. In order for the Domain Team to determine what the FO already knows, in terms of its Domain, the Domain Team will conduct reviews with all of these sources, collecting both case-derived and non-case intelligence.

The team will conduct a program by program, squad by squad review of current case work and liaison in the division and analyze how these match FBI priorities. The baseline of domain awareness will begin with existing contacts in the domain. Questions include: How are you

currently interacting with the threats and vulnerabilities in your domain and what domain entities are of interest to your field office? All programs in the field office must be reviewed, including Counterterrorism (CT), Criminal Investigative Division (CID), Counterintelligence (CD) and Cyber. Each program should be reviewed to determine the priority threats and vulnerabilities, along with how the cases match up to the FBI priorities in those programs. Developing a full picture of our threats and vulnerabilities also will require review and assessment of information outside of our investigative programs.

During this analysis, the following factors must be considered:

- Physical factors: What priority targets must be protected in the field office domain pursuant to FBI priorities (identification of vulnerabilities for critical infrastructure);
- Social factors: What is known about the demographics and sociology of a domain through existing investigative work (social, organizational, and communication networks);
- Threat factors: People or organizations that wish to do harm, especially to priority vulnerabilities (knowledge of presence, capabilities, activities, intentions, motivations, and opportunity);
- Capabilities factors: Investigative or intelligence resources that can be applied to improve domain knowledge and defeat or neutralize threats (SSG logs, confidential human sources, other collection platforms, local police department mappings, etc.); and
- Current affairs factors: Investigative or intelligence resources that already exist (liaison, JTTF, Community Outreach, task forces, etc.) and must be used cross-programmatically.

This analysis will provide the following:

- Improved knowledge of division territories;
- The identification and location of intelligence capabilities against known or suspected threats;
- Priority locations in the field office that are vulnerable to threats and need attention;
- The allocation of requirements to appropriate sources;
- The identification of intelligence collection gaps; and
- The application of targeting analysis to improve collection against threats, vulnerabilities and gaps.
- Identification of emerging trends.

The baseline assessment should make a field office ready to answer the question: What do we already know about our domain? This question seeks to identify what is already known about a domain through pending and closed investigations, source and liaison coverage, and known threat activity as described above.

What is a threat? A threat is a foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and malicious intent of debilitating the defense or economic security of the U.S. A threat may be an individual, an organization, or nation. A threat can also be the capabilities, intentions, and attack methods of adversaries to exploit – or any circumstance or event with the potential to cause harm to – information or an information system. Threats include gangs, foreign intelligence services, etc.

What is a vulnerability? A vulnerability is the susceptibility of facilities, operations, activities, infrastructure or programs to exploitation by a threat. Vulnerabilities include infrastructure such as dams and bridges, locations that house dangerous materials such as chemical plants, research facilities and the technologies developed on-site, and locations that facilitate criminal activity.

Application of new tools, personnel, and processes

The field office must reallocate and secure resources to use new tools to establish comprehensive domain knowledge and capabilities. In addition to identifying a DMC, dedicated liaison officers, CollMCs, and personnel with expertise in geospatial mapping, the field office should establish regularly scheduled, cross-program, threat based working groups of agents, analysts, and CollMCs to share knowledge on topics, trends, and patterns for that threat, while establishing necessary cross-programmatic working relationships and social networks in a field office.

The field office should also establish and/or continue regularly scheduled external working groups with police and USIC partners to share knowledge on topics, trends, and patterns for threats and vulnerabilities, while establishing necessary working relationships and social networks outside a field office.

As new tools, personnel and processes arise in a field office, Domain assessments by program, issue, or the like can be drafted to capture information at any given time. Moreover, this information will provide executive management at a field office ready answers for FBIHQ and others seeking status about investigations, new trends, or filling requirements. This process will be repeated continuously, as a Domain is continuously evolving and changing.

Analyzing FO information using the Domain methodology

The next step is to answer two additional questions: "What do we need to know about our domain?" and "What don't we know about our domain?" Answering the first requires an understanding of vulnerabilities and intelligence requirements within, or related to, a domain. Vulnerabilities include critical infrastructure and technology that, if damaged, destroyed or stolen, would adversely impact the U.S. and its entities and may vary depending on the threat. Examples of vulnerabilities include, but are not limited to dams, bridges, chemical plants, nuclear plants, research facilities, and air and seaport facilities. Answering the second question entails carefully analyzing what the FBI already knows and comparing it to what the FBI needs to know. Responses to this question should lead to the emergence of information or intelligence gaps about the threat and domain that need to be addressed.

Completion of a Domain Assessment

The Domain Team will pull together information from inside and outside the FO and produce the Domain Assessment, a product that takes this synthesized data, adds perspective and context, and recommends specific courses of action. It answers the fundamental question: "What can we do about it?" Domain Assessments are annual products that identify and rank the priority threats in the Domain, identify key vulnerabilities in the Domain, and identify intelligence gaps from a Domain perspective. The purposes of a Domain Assessment are:

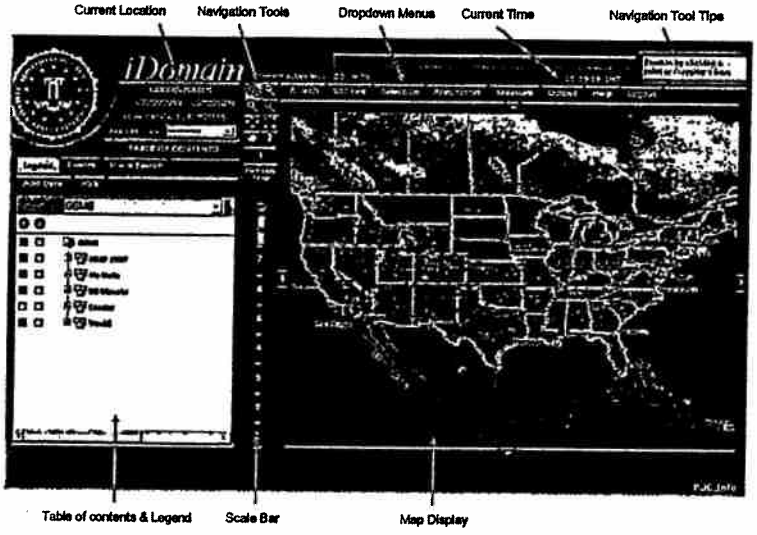
1. To provide a comprehensive analysis of the Field Office's area of operations, specifically its threats and vulnerabilities;

2. To describe the Field Office's key concerns and identify gaps in collection; and

3. To assist in the prioritization of collections, operations, and sources.

The Domain Assessment will include several Key Findings based on analysis of the FO Domain. These may include identifying new threats and vulnerabilities, new targets, and new cross programmatic trends. The Domain Assessment will also offer additional insight into current investigations and Domain intelligence gaps. As the Domain Assessment is being produced, the Domain Team will compare its findings to current FBI and FO priorities and provide this comparison to FO management in the event that FO priorities and resources need to be adjusted to meet the primary concerns in the Domain.

As part of this process, the team will produce Common Operational Pictures (COPs), which are maps that depict various layers of Domain intelligence on top of each other as it pertains to a given threat. For example, a COP may be created that displays known gang territories in a Domain, and then known drug activity may be overlaid on top of the gang territories to determine which gangs are dealing in which types of drugs.

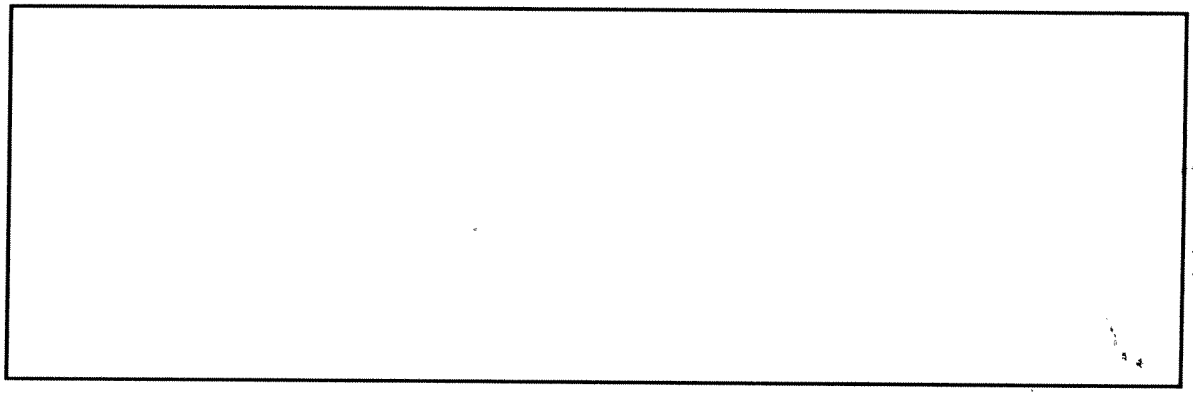


Improving and Applying Domain Awareness

Once the new tools and processes are learned and become part of a field office's basic functions, Domain Awareness will develop in the field office. Part of increased Domain Awareness is a better

understanding of intelligence gaps, a process that naturally occurs following the production of a Domain Assessment. A field office must begin to fill the knowledge gaps about its domain. Identification of these information gaps will require decision makers to address the last question: What are we going to do about it? Decision makers should reevaluate how their resources are allocated and deployed against the threats, vulnerabilities and knowledge gaps related to their domain.

Once the baseline Domain Assessment is completed, and new tools and processes are applied, a field office may now look across all programs in its domain and Collection Management can begin to initiate comprehensive collection plans for each. These plans will outline strategic and tactical outreach in the domain, along with keeping a finger on the pulse of a domain. Overlap between the programs should be welcomed and addressed by the Domain Management at a field office.



b2
b7E

"Domain Entity" Defined –

The phrase "domain entity" does not refer to a subject, but rather to something or someone that subjects are interested in. This can include targets (people or places that are threatened), tools (explosive materials or weapons), and people who could be tools (possible recruits for a gang or terrorist organization).

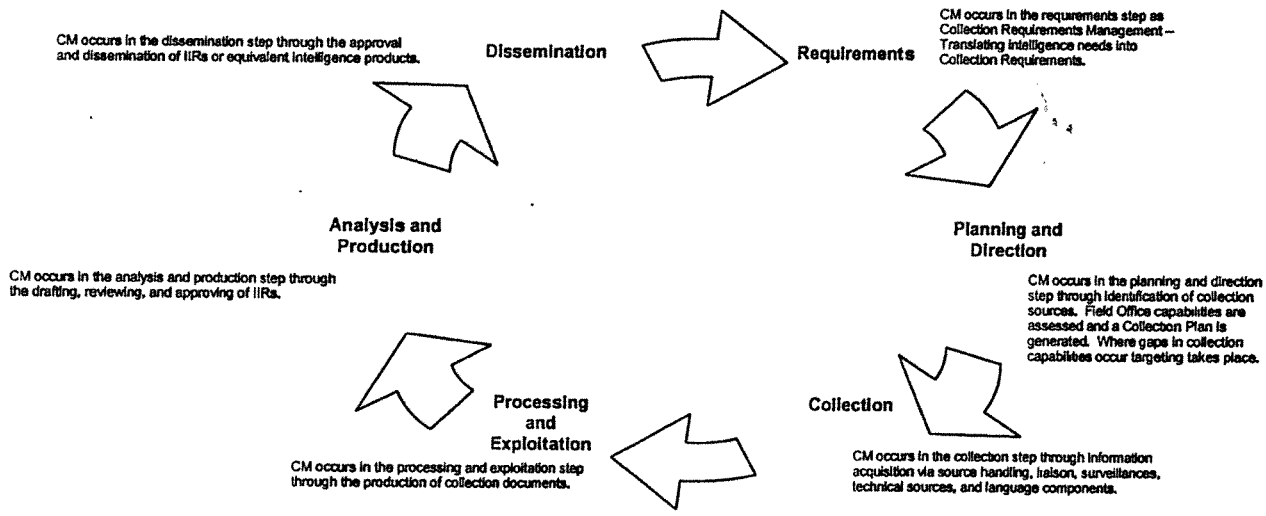
The fully mature Domain Management process will permit a continuous flow of: 1) receiving needs from operations, leads, FBIHQ, national requirements, internal requirements, local partners, field office management, etc.; 2) identifying pertinent factors within those requirements; 3) leveraging their domain for GIS (mapping) information), etc.; 4) filling knowledge gaps; 5) collecting information imported into a domain database; 6) generating new requirements and cases/operations; and 7) continuing the process over again. In short, knowing and acting on the domain.

For more information on Domain Management, see the Domain Management How-To Guide and Handbook.

COLLECTION MANAGEMENT

Collection Management is the process of receiving and then converting intelligence needs and gaps into questions (intelligence collection requirements), prioritizing how those questions will be answered, assigning the questions to collectors for resolution and tracking our progress in answering the questions.

Through Collection Management, the FIG helps the FO manage competing demands for intelligence collection, including the need to collect information to further case investigations, to follow threat leads, to conduct liaison and build partnerships, to help meet intelligence requirements from the Law Enforcement and Intelligence Communities, to complete our Common Operational Picture, to improve our understanding of a particular issue, and to support regional and national efforts. These requirements are consolidated and prioritized through a careful balancing of factors including an analysis of each case to determine the level of threat represented, national and regional priorities, vulnerabilities and knowledge gaps in the territory, and prioritized local requirements, and specific concerns such as requests from local law enforcement, or the high-profile of a particular case.



Elements of Collection Management

- Collection Requirements Management – The CollMC receives, analyzes, validates, and consolidates requirements received from the operational squad(s), FBIHQ, external agencies, and the FIG's DMC. Collection requirements will be prioritized with FBI requirements as the primary focus and then USIC or partner requirements (such as National HUMINT Collection Directives (NHCDs). Once completed, the prioritized set of collection requirements must be

validated by Executive Management. This set must be re-evaluated as local and national requirements change.

- Collection Planning and Direction – The FIG identifies and directs collection sources (human sources, surveillance components, technical sources, language analysts, etc.) to satisfy specific intelligence collection requirements. The individual performing this function in the FO analyzes the access, placement, and capabilities of all FO collection sources to determine which is the most effective and efficient resource to collect against a requirement. This assessment will be done using a methodology which tracks the full breadth and depth of actual, available and/or potential collection resources/capabilities by type (human sources, technical, SSG, SOG, local law enforcement, etc.) their access and placement against targets and intelligence requirements, availability, veracity, and dependability.

  The end products of the collection planning and direction process will be:

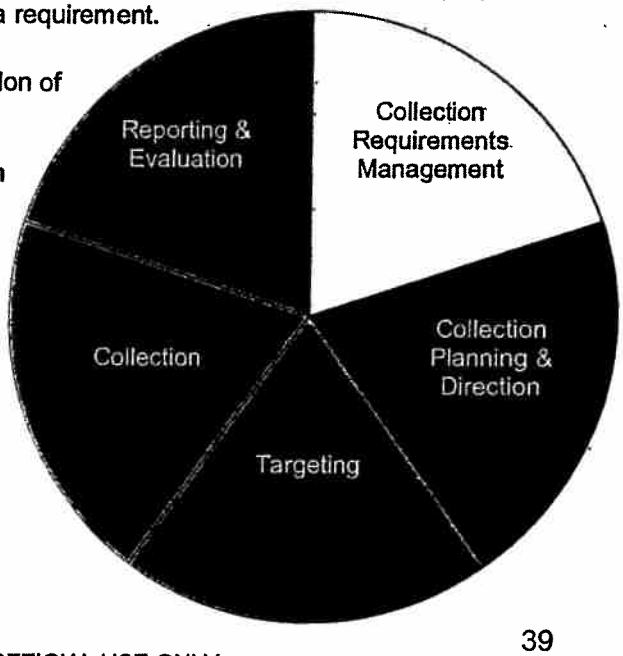
  A Collection Strategy is a periodic (annual) document articulating the field office's intelligence collection priorities and providing high-level guidance on the approach to achieve goals/objectives against these priorities. It provides the foundation for ongoing Collection Planning throughout the year.

  The Collection Plan assists the CollMC in allocating the field office's collection sources to address specific collection priorities. It considers the tasked collection requirements, their priority, and the collection capability and availability of sources.

- Targeting – When there are no existing or insufficient collection capabilities identified that can respond to a requirement, the FIG may produce a Target Recommendation providing the results of the analysis performed to find a new potential source or contact with the appropriate placement and access to possibly respond to a requirement.

- Collection – This element involves the acquisition of information from source handling, liaison, surveillances, technical sources, and language components. The end product of the collection process will be collection documentation.

- Reporting and Evaluation – The final step is to communicate the results of our collection efforts. This element involves the drafting, reviewing, approving, and disseminating of an IIR or equivalent intelligence product and then evaluation of reporting through the CRO. Another end product of this process will be a Collection Posture report by the CollMC to document and account for requirements which have been addressed in a FO and those requirements which are still considered gaps.



A standardized and centralized Collection Management function will give the field office the ability to leverage program sources and knowledge, and expose gaps in coverage for future targeting efforts. It will provide Executive Management with a planning document for deciding allocation of local resources against prioritized threats. It also will facilitate FBI-wide strategic coordination by providing a nationwide understanding of the threats (current and potential future) that are posed to the US and its interests, collecting intelligence to address those threats, and reporting relevant information to facilitate any warranted action.

For more information on Collection Management, see the Collection Management "How-To" Guide.

HUMINT COLLECTION

As outlined above, the Domain Management process will help the FO identify national security and criminal threats to its AOR. The Collection Management process will produce a plan for responding to intelligence gaps. This section is about how we fill those identified gaps by developing and fully exploiting HUMINT sources. Our strategy has several parts: leveraging case-based HUMINT collection, collecting HUMINT specifically to address requirements, liaison, and vetting and validation of sources.

Leveraging Case-Based HUMINT Collection

The vast majority of the FO's intelligence collection occurs outside of the FIG. If we are to fully leverage our existing source base, it is essential that all SAs and their supervisors develop a working knowledge of the FO's collection plan and related requirements, and must know how it relates to the squad's investigations and source capabilities.

All sources have the potential to meet intelligence requirements.

Does the Agent who is talking to a source know the requirements that this source could potentially address?

SAs on operational squads outside the FIG should proactively identify intelligence which is collected during the normal course of duties – either through investigation or source handling – that is pertinent to the FO Collection Plan. They are also responsible for ensuring this intelligence is forwarded to the appropriate entity within the FIG.

Where staffing levels permit, investigative squads will be assigned an embedded IA who will report to one of the field office SIAs and will ensure that intelligence collected during the squad's normal course of duties is funneled appropriately to the FIG for either dissemination, domain awareness or gap identification. This embedded IA will be an extension of the Domain and Collection Management functions in the office. The IA will help agents on the squad identify potential opportunities for sources to provide information that is responsive to an intelligence requirement (that may or may not be outside the scope of the case for which that source was recruited). The IA will identify and define priority collection requirements the squad's human sources may be able to fill. The IAs will identify, develop, and provide relevant questions and taskings to be used in source debriefings.

Dedicated Special Agent HUMINT Collectors

To distinguish from case agents, the FIG Agents are dedicated full-time to HUMINT. They will not work on cases, but will provide cross-program support by recruiting and handling human sources with access to intelligence that can address priority requirements. They may coordinate with CHS handling agents to facilitate the flow of intelligence information when the intelligence being provided reaches beyond the investigation on which they are reporting.

The FIG Agent should know the field office's intelligence gaps and collection requirements and priorities established by the CollMC. With this knowledge, they will develop liaison contacts and

spot, assess, develop, recruit, and handle human sources dedicated to creating non-case collection opportunities. Alternatively, a FIG Agent may be provided a targeting package relevant to a specific requirement.

Because FIG Agents will only be responsible for source operations and liaison, it is expected that they will develop high level expertise in the use of tradecraft as well as the operational skills necessary to spot, assess, develop, recruit and handle HUMINT sources. This expertise will be achieved by actively participating in the appropriate training programs and through constant practice while on the job. FIG Agents will, in turn, actively participate in mentoring and coaching other less experienced Agents in these areas.

Case Agents and HUMINT Collectors Each Add Unique Value to the Field Office's Capabilities

Case Agent	HUMINT Collector
• Expertise managing cases driving toward usable intelligence and/or prosecution	• Full-time spotters, developers, recruiters, and handlers of sources
• Source spotters and handlers for operational matters	• Dedicated to creating non-case collection opportunities and fresh streams of reporting
• Able to handle multiple cases and leverage program expertise	• Skilled in USIC-standard tradecraft practices designed to protect sources and agents
• Work in conjunction with embedded IAs to identify investigative approach	• Capable of working joint operations when necessary
• Subject-matter expertise	• Skilled in validation techniques for testing sources' reliability
	• Subject-matter expertise

Liaison

Liaison relationships provide the assets and controls necessary, essentially the "eyes and ears," required to blanket a community and establish a proactive posture against threats to the U.S. In this role a FIG Agent conducting liaison has the responsibility of educating the liaison contact regarding the vulnerability. As these vulnerabilities in domain entities are identified, liaison allows "tripwires" to be set in order to alert us to impending threats. There are several other benefits which can be realized from a strong liaison program. First, it creates valuable opportunities for spotting and assessing potential CHSs within the liaison entity. This is especially valuable when the information available from within the entity requires a confidential relationship in order to be extracted. Additionally, a strong liaison relationship will ease the entry for others (eg. Case agents) needing access to the entity with whom the liaison is maintained.

To ensure this critical mission, the FIG HUMINT squad will serve as the coordinating hub of all FO liaison activities. It is important to note that the FIG will not be taking away established relationships existing outside of the FIG, but these relationships will be centrally coordinated to

ensure common messaging and deconfliction of multiple requests for similar information from the same entity.

Two Platforms Used by the FIG Agent

CHS Operations

- Proactive Collection
- Focused & Targeted
- Tradecraft
- Vetting and Validation

Liaison

- Passive Collection
- "Eyes and Ears"
- "Tripwires"
- Education
- Spotting and Assessing

Value of two platforms

- Expands flexibility and options
- Expands collection opportunities
- Extends FBI reach and ability to "monitor" the domain

Risks of two platforms

- Over exposure of individuals to the public
- Overlap and de-confliction
- Management burden

	CHS Operators	Liaison
How do I present myself?	Confidential relationship	Open and public relationship
Who do I focus on talking to?	Individuals with specific access to information the FBI needs	Entities in the domain with vulnerabilities to threats
What is my purpose?	Develop a CHS (including access agents) to: • Gather intelligence • Set discreet tripwires	Develop contacts to: • Set public tripwires • Spot potential CHS • Gather intelligence
Where do I report information?	CHS report	Contact report

Vetting and Validation of Sources

We will create standardized mechanisms and practices for validating sources. Up until now, the processes utilized to vet and validate human sources have focused primarily on compliance issues.

While these efforts are important and will continue, we must also vet and validate sources for three other purposes:

1. To ensure field offices are operating viable and valuable sources in a secure manner;
2. To ensure the source is fully leveraged to respond to the field office's Collection Plan priorities; and
3. To provide a confidence level to intelligence provided by the source.

Where the purpose of HUMINT sources is to provide information to be used by the FBI in fulfilling its national security and law enforcement missions, the operation of sources requires the FBI to ensure the sources and the intelligence they provide are authentic, reliable and not subject to external control.

Validation is an ongoing process intended to continually re-establish the authenticity, reliability and control of a HUMINT source. It requires FIG and Case Agents to constantly assess the source and to use a number of tools and techniques for vetting and operational testing to verify or check the accuracy of available information about the source. Although it is essentially impossible to "prove" that a HUMINT source is valid, vetting and ops testing should provide the agent a high degree of confidence as to the source's authenticity, reliability, and whether they are under external control. Vetting and ops testing of the source are intended to gather information responsive to four key questions:

- Is the source really the source?
- Does the source have the access claimed?
- Is the source acting free of external control?
- Has the source provided valuable information to which the source has legitimate access?

Enhancements being made to work specialties in the FIG, specifically the CHS Coordinator, will greatly benefit agents in the validation, vetting and ops testing of sources. The CHSC will have the expertise and experience to provide guidance on ops testing and vetting of sources according to policy, legal guidelines and USIC requirements. However, an agent's use of tradecraft and regular assessment of his source will help in validating and ops testing the source.

Regular, standardized use of validation and ops testing provides increased credibility for the FBI within the USIC and with domestic and foreign liaison partners. Our use of tradecraft for recruiting and handling sources, as well as its attention to assessment and vetting of sources, increases opportunities for greater inter-operability of sources. This inter-operability of sources provides more collection opportunities to address the FBI's intelligence priorities at home and abroad. For example, an agent can better represent the FBI's interests in inter-agency coordination meetings when the Agent can provide a detailed assessment of the source's motivation for cooperating. Similarly, a tested and validated source is more acceptable for joint operation or turnover to another agency for handling, again enhancing the FBI's opportunities to collect priority intelligence.

For more information on HUMINT collection, see the HUMINT How-To Guide.

TACTICAL INTELLIGENCE

Tactical Intelligence refers to the integration of FBI investigative and intelligence operations through the dedication of critical front-line intelligence resources to investigative programs.

Embedded analysts from the FIG work directly with operational squads and their investigative programs to coordinate taskings to ensure unity of purpose and action consistent with field office priorities. They interpret collection requirements and collaborate with case agents on the collection, filtering, processing, and analysis of information to drive domain awareness, satisfy requirements, and create intelligence products.

The IA's role as part of the Collection and Domain Management processes is described in more detail above.

Targeting

IAs both on the FIG and embedded in operational squads also assist with targeting projects to develop new sources when existing sources are unable to fill collection gaps. They work with HUMINT collectors on the FIG and with operational squads outside the FIG to assess potential source capabilities, determine vulnerabilities, and recommend the most appropriate point of action or exploitation in a targeting product such as a Target Recommendation. The Target Recommendation provides direction to field office collectors (including HUMINT collectors, case agents, SOG/SSG, and Language Analysts).

In putting together a targeting strategy, the IA will draw from Collection Plans from the CollMC. The IA will access domain knowledge, collected information, finished intelligence and case data to discover potential sourcing and intelligence exploitation opportunities.

The IA may issue requests for information to regional counterparts and coordinate with FBIHQ on the implications of local targeting strategy and targets for overall national strategy. The IA will also network with local, regional and national counterparts to get a better awareness of wider trends, concerns, tactics, and resources.

PRODUCTION AND DISSEMINATION

We will implement several measures designed to enhance the quality, relevance and timeliness of FBI intelligence production and dissemination. Other measures will help enhance the focus of our intelligence production to ensure the appropriate intelligence product is created at the proper level for the right consumer. FBI intelligence products, both raw and finished, serve a wide audience including national level policy and decision-makers, intelligence agencies, warfighters, state, local and tribal law enforcement, and the FBI itself.

FOs, in addition to producing IIRs, should concentrate their all-source analytical production efforts on Intelligence Bulletins and Situational Intelligence Reports which focus on the needs of state and local organizations for intelligence that identifies threats, targets, and tools. However, Intelligence Assessments of a strategic nature may also be done in the field office when appropriate.

Raw Intelligence / Chief Reports Officer Position

A Chief Reports Officer will be established in every FIG to enhance the quality and timeliness of IIRs. The CRO's responsibilities include: review of all IIRs prepared in the field office to ensure that each appropriately protects sources and methods, adherence to USIC quality standards and FBI priorities; substantive review and guidance on the content of IIRs (does it satisfy a validated requirement, comply with other reporting criteria, e.g. new, detailed, authoritative etc.?); ensure field office accountability with measurable and objective performance standards; support for the development and maintenance of the field office common operational picture, collection strategy and collection plans; determine whether an IIR meets the criteria for direct dissemination; determine whether an IIR requires a substantive review at FBIHQ; and tracking of internal field division IIR production metrics. The CRO will also coordinate with Collection Management and provide Source Directed Requirements as appropriate.

Raw Intelligence / IIR Training

The SET has outlined a tiered IIR training program for all Intelligence Analysts, including Reports Officers and Chief Reports Officers to enhance the quality of all IIRs – ultimately affecting all other aspects of the IIR production. In addition, the CRO will have the expertise to train and mentor other Reports Officers concerning all IIR content issues, as well as other measures of quality such as technical tradecraft, standardization, and substantive accuracy. SET field office training will provide all members of the FIG with the general content of the IIR process, the need for requirements-driven intelligence dissemination, and the role of the CRO.

Limited Direct Dissemination of IIRs

In order to improve the timeliness of our raw intelligence reporting, the FBI will transition towards a limited form of direct dissemination of IIRs from field divisions to the USIC, Law Enforcement partners, and other consumers. Any reports disseminated directly from the field, regardless of the volume, will result in a commensurate number not needing to be processed at FBIHQ. The

objective is to improve IIR timeliness by allowing for a number of direct dissem inations from FBI FOs while simultaneously ensuring that IIRs forwarded to FBIHQ for substantive review prior to dissemination require only minimum review and coordination. A significant number of intelligence reports would continue to be forwarded from the field divisions to FBIHQ for coordination prior to dissemination to the USIC.

This hybrid approach of disseminating intelligence is contingent upon the establishment of a CRO in the FO and the FIG's ability to consistently produce high-quality IIRs. The CRO will serve as the quality control mechanism in the field. The intent is to apply a quality control check an d to ensure required coordination is effected at the lowest possible level and i n the most expedient manner, while at the same time, retaining a process that provides a mechanism for the necessary substantive reviews and authorizations to be performed at FBIHQ.

IIRs Requiring FBIHQ Dissemination

The following categories of IIRs m ust continue to be sent to the respective reports unit at FBIHQ for coordination and review prior to dissemination to the USIC:

1. Foreign Disclosure
2. Legal Review
3. Marked Originator Controlled
4. Limited Dissemination
5. Joint Source
6. US Policy
7. Attachments

The CRO certification program includes in-depth training on the specific inst ances that require FBIHQ approval or coordination.

IIRs Requiring FBIHQ Coordination

The following categories of IIRs m ust be coordinated with the respective repor ts unit at FBIHQ prior to being disseminated from the field office to the USIC:

1. National Level Activities – This includes national level activities or content associated with a nation-wide organization or activities affecting more than the field office's Area of Operations (AOR). In these cases, the CRO ens ures, in addition to the opera tional coordination with F BIHQ, coordination is effected with the respective FBIHQ reports unit. The purpose of this coordination is to leverage the subject m atter expertise of the reports units at FBIHQ which are responsible for following issues in a specified geographic or functional area and ar e expected to have a national or intern ational perspective.

2. Foreign Intelligence – If a report contains foreign intelligence or concerns foreign bas ed activities, the IIR should undergo th e same coordination procedure as fo r National Level activities and be coordin ated with the appropriate FBIHQ reports unit.

3. Technical/Substantive review – Technical/substantive review includes the follow ing:

- Any time an intelligence officer is identified
- Content concerning foreign military technology acquisition or programs (e.g. high-tech procurement or major hardware initiatives)
- Content concerning technical aspects of Weapons of Mass Destruction (WMD) or WMD precursors

Direct Dissemination – The CRO makes the determination whether an IIR qualifies for direct dissemination from the field division or is required to be forwarded to FBIHQ for additional coordination and review.

FBIHQ Dissemination – If the CRO determines that the IIR is in one of the seven excepted categories requiring FBIHQ approval, the report will be forwarded for coordination and approval. FBIHQ will accomplish any legal or Designated Intelligence Disclosure Official (DIDO) authorization that has not been delegated to the field, review IIRs with non-standard addressees or with special handling instructions, review reporting with U.S. policy implications or attributed to joint sources, and facilitate technical procedures such as posting attachments.

CRO IIR Metrics – The field division will be graded on three primary metrics. The first is FO velocity, measured from the date the IIR is created by the field office in the FBI IIR Dissemination System (FIDS) to the time the IIR is submitted via FIDS to FBIHQ or directly disseminated to the USIC. The second measure is the throughput metric. Throughput is the percentage of submitted IIRs that are subsequently disseminated to the USIC. A field office's throughput will decrease if FBIHQ rejects their submitted as 'non-disseminable.' The final metric is a new measure of throughput called first-time throughput. First-time throughput is the percentage of submitted IIRs that are subsequently disseminated to the USIC *and that were not returned to the field for additional edits*. A field office's first-time throughput will decrease not only when an IIR is rejected or not disseminated by FBIHQ but also when FBIHQ sends an IIR back to the field for edits – even if that IIR is then resubmitted and sent to the USIC.

Finished Intelligence Production and Dissemination

Field offices should refine their finished intelligence analytical products to a set number of products so as to standardize their products across the enterprise and create brand recognition with consumers at every level. While there are a number of local-use intelligence products, such as Intelligence Notes and Domain Assessments, the following finished products are the focus of SET standardization efforts because they are externally disseminated and should adhere to USIC standards. Finished intelligence products that are disseminated to external organizations can be grouped into five major categories:

1. Assessments
   (a) Intelligence Assessments (IA)
   (b) Special Event Threat Assessments (SETA)
2. Intelligence Bulletins (IB)
3. Situational Intelligence Reports (SIR)
4. Letterhead Memorandums (LHM)
5. Briefings

Assessments

Assessments are finished intelligence products containing evaluated all-source information that address intelligence requirements or identify threats and trends. Some are intended to be released to local customers of FBI FOs while others will be released at the national level to our intelligence community and law enforcement community partners.

Intelligence Assessments are finished intelligence products containing evaluated All-Source intelligence. Assessments may address tactical, strategic, or technical intelligence requirements. They are written when there is a need to identify threats or trends in any FBI investigative program and should always be responsive to FBI and/or USIC intelligence requirements.

Special Event Threat Assessments analyze the attractiveness of a special event for terror targeting, as well as, assessing the known and potential threats to an event. A Special Event Threat Assessment provides FBI personnel, other law enforcement agencies, and the event security planners with analysis to better monitor potential threats and to maintain a safe and secure event environment.

Intelligence Bulletins

Intelligence Bulletins disseminate information on significant criminal or national security developments or trends of interest to the intelligence or law enforcement communities. In most cases, bulletins are one to three pages long and contain brief analysis which supports at least one specific product judgment. FOs should produce Intelligence Bulletins that are locally oriented and pertain to the FO's territory. Intelligence Bulletins may be classified but should be prepared at the lowest level possible to ensure the broadest dissemination.

Situational Intelligence Reports (SIR)

The Situational Intelligence Report (SIR) is a finished intelligence product produced by FIGs to disseminate relevant, localized intelligence to state and local law enforcement. The SIR conveys information of specific interest to local audiences regarding previously disseminated national-level information that needs to be highlighted for the local audience or locally derived information that is largely of interest only to the local audience.

Letterhead Memorandum (LHM)

The Letterhead Memorandum (LHM) is often used to transmit information to Foreign Law Enforcement and/or Foreign Intelligence Services in response to official requests as well as other case specific uses. The LHM is a memorandum on letterhead stationery and should normally require a cover communication for transmittal.

Briefings

Intelligence briefing is an integral part of intelligence analysis tradecraft. Effective briefing requires proper planning, organizing and delivery skills. Intelligence briefs are presented at every level of the FBI from case analysis summaries at squad meetings to preparing for the Director's daily brief.

Intelligence briefings, whether delivered formally or informally, fall into one of five USIC intelligence briefing categories:

1. Basic Intelligence
2. Current Intelligence
3. Estimative Intelligence
4. Warning Intelligence
5. Operational Intelligence

Collection Management Products

The products specific to the new Collection Management process are specified in the Collection Management sections of the training materials.

For more information see the Production and Dissemination How-To Guide.

MEASURING AND TRACKING PERFORMANCE

If the FBI is to become the world's premier national security agency, the Bureau must instill a high-performance culture and standardize certain management practices to be able to measure its progress in becoming an intelligence-driven organization. One of these management practices relates to the ongoing process of monitoring and improving the organization's *performance* in executing its intelligence mission. An enhanced, strategic, and standardized performance management system will enable the FBI to monitor and clearly articulate its successes in delivering on its intelligence mission.

The SET performance management implementation is designed to achieve several objectives:

- **Motivation**: Encourage behavior that improves overall Bureau intelligence
- **Transparency**: Increase transparency and accountability, with clear performance standards at all levels
- **Continuous Dialogues**: Institutionalize a culture based on regular coaching and feedback, driven by hard data

The performance management system will focus on a strategic set of performance metrics that will drive the right set of behaviors in the organization and lead to continuous improvement of the FBI's intelligence program. At the same time, the system takes into account that not everything can be packaged neatly in numbers. A significant aspect of a field office's intelligence program is knowledge of domain and the understanding threats and gaps to be able to collect against those threats and gaps. In terms of measuring one's performance in this arena, a *qualitative*, creative approach must often be employed.

The numbers never tell the whole story, but they provide an important beginning. The first step is to install a reliable performance metrics tracking and reporting process across the Bureau. It is important that if Headquarters intends to monitor and drive performance that both Headquarters and the field work from the same data.

Think of it this way: intelligence collection, analysis, dissemination – and where applicable – action should be at the heart of what your field office does. So the metrics are your pulse. Is your office's heart rate slow or fast, and based on your domain, what should it be? Now, to take this metaphor one step further, the fact that your field office turns out a million IIRs, SIRs or IBs may show a very fast pulse rate, but not necessarily a healthy heart. The way to determine the true health of your intelligence program is to ask questions that go behind the numbers. Aside from the volume of reporting, what is the quality of the reporting? Is it actually useful when measured against the FBI's intelligence requirements, the intelligence community's requirements? Does the reporting help to fill a gap? Are we prioritized? Are we collecting against what we already know, or are we asking those provocative questions that identify the presence of risk that was not really on our radar before? What are the unknown threats and what am I doing to hunt for them? Are we using our mapping capabilities to get not just the intelligence information about our domain, but literally a

snapshot out what it looks like and how one collection stream, or one threat relates to another geospatially?

This qualitative component will be captured through regular performance dialogues among senior leaders in the field and at FBIHQ. The starting point for these performance reviews will occur with enhanced Deputy Director's Strategy Performance Sessions (SPS) with SACs from regional offices. The SPS dialogues will cascade to the field office level, where the SAC will conduct monthly intra-office SPS performance reviews with his or her management team. These reviews will be similar in concept to the CompStat performance system common in law enforcement. CompStat (short for comparative statistics) is a performance management system introduced in 1994 by the NYPD. The policing application of SPS works by counting crime reports and measuring them against arrest and summons activity and then mapping all of that. The concept is "to put the cops on the dots" or, map where the crimes are happening and deploy the police to those locations quickly so there is a higher likelihood of catching the bad guys the next time they strike. The FBI application – SPS – is slightly different in concept. We are not applying the CompStat model so we can get to where the crime is and catch them the next time, but so that we have a better chance of identifying threats beforehand and we are in the best position to prevent the threat from being carried out at all. In addition, whereas CompStat tends to be more operational and tactical in nature, SPS will be at a more strategic and focused level.

In the near-term, the performance management implementation will:

- Determine initial scorecard metrics for IIRs; expand metrics through 2008 and 2009
- Implement regular performance dialogues at the top levels of the organization
- Not set targets as part of SAC PARs in 2008, but in 2009
- Link inspection processes, SAC PARs, and file reviews with SET results/implementation
- Be driven by a manual process with some automation

The end state, or long-term vision, takes this a step further:

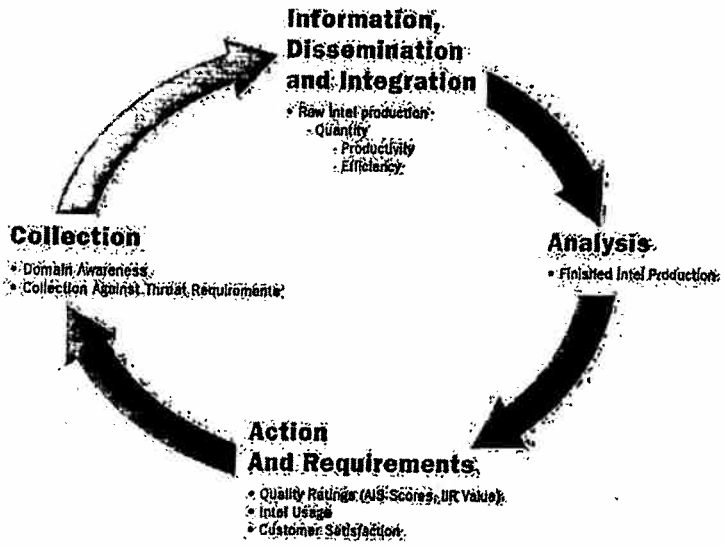
- Enterprise scorecard system that can be populated from Headquarters or the field, is automated and reliable
- Clear targets, both short-term and stretch targets
- Strategic, focused performance discussions regularly occurring among top FBI leaders and at all levels of the organization
- Inspection process, SAC PARs, and file reviews fully integrated with performance management process

Performance Data, Metrics, and Scorecards

Ultimately, the FBI measures success by how well we prevent and disrupt crimes and terrorist acts, and our ability to bring criminals and terrorists to justice. But to help us achieve this, we need to track and measure our success in the activities that help us get there. For intelligence, we have four key measures:

1. Speed
2. Quality
3. Accuracy
4. Actionability

This graphic illustrates the four core intelligence processes, and provides some examples of the types of metrics that will be captured at each stage.



Field offices will be expected to focus on a small set of metrics for "Phase 1", the first six months, based upon what can be collected currently. Phases 2 and 3 will provide FBI leadership with an updated set of metrics to track, as shown in the table below.

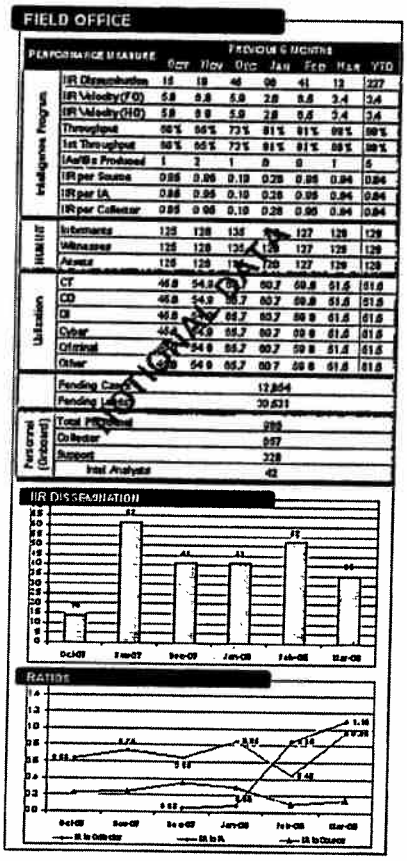
Phased Matrix of Performance Metrics

Intelligence Process	Phase 1 Metrics *(Next 6 Months)*	Phase 2 Metrics *(6-12 Months Out)*	Phase 3 Metrics *(12-18 Months Out)*
Collection	▪ # of IIRs by collector ▪ # of IIRs by source	▪ % of IIRs that hit priority 1 or 2 NIPF requirements ▪ % of IIRs that hit FBI requirements	▪ # IIRs hitting priority requirements by Confidential Human Source (CHS)
Info dissemination and integration	▪ # of IIRs ▪ # of IIRs by IA ▪ IIR Velocity (HQ to dissemination) ▪ IIR Throughput	▪ IIR velocity o Field velocity (collection to HQ) o HQ velocity (HQ to dissemination) ▪ # of IIRs by RO ▪ # of IIRs pending ▪ IIR quality rating	▪ IIR velocity o Field velocity (by immediate, priority, routine)* o HQ velocity (by immediate, priority, routine)*
Analysis	▪ # of IAs ▪ # of IBs ▪ # of SIRs ▪ # of Briefings ▪ Analytic integrity standards (AIS) score	▪ # of IAs ▪ # of IBs ▪ # of SIRs ▪ # of Briefings ▪ Analytic integrity standards (AIS) score	▪ % of IAs to analysts on-board ▪ % of IBs to analysts on-board ▪ # of SIRs ▪ # of Briefings ▪ Analytic integrity standards (AIS) score
Action & requirements		▪ Intel usage to determine quality % of IIRs used in internal (FBI) executive products	▪ Intel usage to determine quality ▪ Customer satisfaction score ▪ Identified trends and threats ▪ Investigations initiated ▪ Neutralized threats ▪ % of IIRs used in external executive products

Headquarters, through the Resource Planning Office (RPO), will continue to track other key metrics, such as resource utilization (i.e., TURK) and Funded Staffing Level (FSL), but the focus of FBI leaders will be on intel-related metrics.

Data Collection, Analysis and Reporting

The data collection process will continue to be manual and labor intensive, and will be led by the DI's Performance Analysis Unit (PAU) at Headquarters, in collaboration with the Resource Planning Office (RPO). Much of the data will be fed into the Compass system, and displayable via a common SAC "dashboard." Below is a snapshot of the view SACs will see when they open Compass and click on the "Intel" link from the Compass homepage:



The field's role will be limited in terms of data compilation and scorecard assembly; that role will be performed by a team of analysts in DI PAU in close collaboration with RPO. However, the field IP Coordinator, along with the IP Manager, will have a significant role in reviewing the data, as well as interpreting the data and explaining trends.

With regard to automation, the near-term deployment of enterprise systems will add an element of automation to the process, making it easier to collect existing and some new metrics.

Performance Dialogues

For an organization's leaders, periodic performance reviews are where the ongoing process of strategic management really comes together. The meetings generate strategic conversations and insights, inform decision-making, enhance performance management, and instill a culture of accountability to enable the organization to achieve performance breakthroughs. Historically, in the most successful organizations, the chief executive sets the tone and cadence by establishing regular strategic performance discussions among his executive team. The purpose of these reviews is not to monitor ongoing operations – those are separate meetings – but rather to monitor the strategic pulse and direction of the organization. These performance reviews or dialogues must then be cascaded down through the organization in a ripple effect in order to instill the behaviors that will drive the organization to desired results over the long-term. Since late 2006, Director Robert Mueller has assembled monthly and quarterly with his executive team to conduct strategic performance reviews focused on a small set of metrics and key enterprise initiatives. Known as the Strategy Management System or "SMS," the Director has cascaded this approach to the Headquarters divisions; the Assistant Directors of most HQ divisions also meet regularly to engage in strategic performance dialogues with their leaders. The process is far from perfect, but a foundation has been laid to expand the process to the field in a coordinated manner.

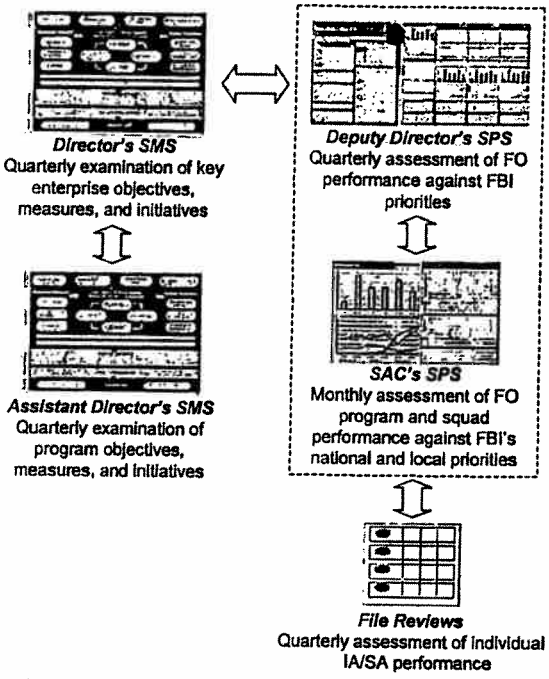
Beginning in February 2007, in an effort to cascade certain elements of the SMS to the field, Deputy Director John Pistole initiated a HQ-to-Field dialogue process called the "Strategy Performance Session." An extension of the SMS process, SPS created a forum to engage top field leaders in these existing strategic discussions originated by Headquarters. Held quarterly, Deputy Director Pistole and branch executives conducted a secure video teleconference (SVTC) with five to seven SACs at one time, focusing on a specific theme or topic (e.g., domain). Each SAC presented a set of common metrics (e.g., TURK, IIRs), whereupon the Deputy Director and his Executive Assistant Directors would then ask a series of follow-up questions, both quantitative (why did you only have five IIRs last month?) and qualitative in nature (what are you doing about a certain threat in your area?).

While a number of SACs likely initiated a version of their own "SMS/SPS," a formal structure or process did not exist that could position the field for success in its dialogues with HQ, or get it to focus its intelligence program. The graphic below shows the long-term FBI performance review structure at a high level, driven by bottom-up execution from the field and capped off by the Director's SMS reviews.

Deputy Director SPS with SACs

Beginning in May 2008, the Deputy Director will reconstitute Strategy Performance Sessions with his executive team and the Special-Agent-in-Charge from six field offices from a particular region. The SPS reviews will last two hours, giving each SAC 20-30 minutes with the Deputy Director and his team.

The SPS will draw from quantitative data captured in Compass as a starting point for discussion and build on that with qualitative questions. The full menu of qualitative questions can be found in the Performance Management "How-To" Guide.



The first SPS sessions will occur in late May and include the Wave 1 field offices: Washington Field Office, Baltimore, Norfolk, and Richmond. Wave 2 offices will begin their SPS reviews with the Deputy Director in July, along with the second sessions for Wave 1 offices. The calendar below provides a proposed review schedule through 2008.

Through 2008, each "Wave" will participate every 60 days. The SPS schedule will be re-set in January 2009 and focus on nine groups organized generally by regions (as opposed to SET waves). The chart below provides a sample SPS schedule for 2009. SPS frequency will depend on field office performance and scheduling availability.

SAC SPS with ASACs and Supervisors

SACs will meet on or around the third week of every month to conduct the field office version of the Deputy Director's SPS. Why the third week? First, because the metrics data are generally available in the second week of every month, when it is compiled and fed into the Compass system. By waiting until the third week, the SAC can ensure the latest data. Second, each SAC will participate in the Deputy Director's SPS at the end of every third month, so by conducting regular, internal field office reviews one week prior to the SPS, the SAC and his/her management team will get into a rhythm.

In conducting his/her SPS, the SAC should use the same menu of qualitative questions that are used for the Deputy Director's SPS.

Supervisor File Reviews with Agents/Analysts

Each supervisor will continue to conduct a file review with agents on a ninety-day cycle. These performance reviews are not meant to depart significantly from the current file review process in place, although some adjustments will be required. The existing file review template will be supplemented with an additional section that exclusively focuses on intelligence production (e.g., IIRs initiated by agent). Individual case review sheets will be modified to include key questions, such as:

- Was the investigation initiated as a result of strategic intelligence? (Yes/No)
- Was the investigation enhanced as a result of tactical intelligence? (Yes/No)

These questions mirror page 11 of the new Intelligence Program SAPR.

Supervisors will also conduct file reviews with Intelligence Analysts every ninety days. The Human Resources Division is currently developing a standard Intelligence Analyst file review process, much in the way Special Agent file reviews are standardized.

Link to Inspections and SAC PARs

Inspections and SAC PARs

In the summer of 2007, the Inspection Division (INSD) developed a Strategy Management System (SMS) as part of the FBI-wide SMS recently implemented to make sure the Bureau aligns all of its resources and activities to properly support our post-9/11 mission. In the traditional inspection process, inspections were generally based on a three year inspection cycle. All programs in a field office or headquarters section were inspected from top to bottom on this cyclical basis. In November 2007, INSD interrupted the 'traditional' inspection cycle in order to begin the Inspection Reconstruction Project (IRP). The IRP is nearly complete.

Under the new inspection model, the primary document utilized by the Inspection Division will be the newly designed SAPR. The questions contained in each program SAPR have been directly aligned with the SMS and the SAC PAR. Data analyzed by INSD will include the SAPRs, FBIHQ SAC program rankings, results of the leadership climate survey and results from the annual outside contacts survey. INSD will compile and analyze this data and prepare the Inspection Risk Assessment Matrix (IRAM) during the last quarter of each year. The IRAM will be used to determine the inspection schedule for the following year.

SAC PARs

A number of intelligence metrics that are part of the enhanced performance management rollout are also included in the SAC PARs for FY 2008, as it relates to **O3 – Expand Information Access and Sharing Internally and Externally**, including:

- Measurable Result 1 (MR1): IIR Dissemination over IA Capacity Ratio
- Measurable Result 2 (MR2): IIR Dissemination over Collector Capacity Ratio

- Measurable Result 3 (MR3): IIR Velocity Rate
- Measurable Result 4 (MR4): IIR Throughout Rate

Of note, SAC PARs for FY 2008 will include a question on what the SAC is doing to create an intelligence-led field office and ensure the overall SET Intelligence Operations recommendations (FIG, CM, DM, HUMINT, Production & Dissemination, Performance Management) are implemented in their offices, and how effectively they are working.

In addition, for FY 2009, SAC PARs will include a few additional intelligence-related metrics, including for example, a metric "IIR First-Time Throughout Rate," which will measure the percentage of IIRs that get through cleanly to dissemination on the first try.

For more information, see the Performance Management How-To Guide and Menu of Qualitative Questions.

IMPLEMENTATION

The new field intelligence model will be implemented in all 56 field offices between March and December 2008. This will be a phased approach that will be rolled out in "waves" beginning with the Washington Field Office, Baltimore, Richmond, and Norfolk.

The first step is preparation. This begins prior to the "wave" when the SET arrives in your office:

- A Prep Checklist and baseline assessment will be provided prior to SET's arrival to each field office to assist in its implementation. Each field office will be expected to have all items completed on the Prep Checklist prior to SET's arrival.

- A baseline assessment of each field office will be conducted prior to SET arriving. Based on this assessment, it will be determined what type of SET model could be successfully configured to that office. Field offices should also plan to staff core "functions" of the FIG.

- Any initiatives that are inconsistent with the SET initiatives should be discontinued. The SET plans to role out FBI-wide changes that incorporate lessons learned from each successive wave. As a result, making changes before the SET arrives at your office would be counterproductive. If you have a specific issue, contact the SET for guidance.

The second step begins when the SET arrives in your field office.

- SET members will work side-by-side with field office personnel to refine and improve the changes as they are implemented. The rollout will also provide guidance, training, and tools for enhancing domain awareness, Collection Management, and raw and finished intelligence production and dissemination.

- SET will initially be on the ground in your office for approximately two weeks to provide baseline training. The exact amount of time will vary depending on the size and complexity of your office, and how close your current structure is to the new field office model.

Step three: After the initial rollout, you will be left to act/execute (work on collection plan) for a few weeks. Some SET members may stay behind to provide on-site assistance. The SET will return at a later date for another two weeks to deliver more advanced training. SET will also check on your process and see what lessons learned can be used to improve the process and/or implementation in other offices.

The final step will be ongoing follow-up and support. This will be provided by the DI and other FBIHQ components. To ensure that FBIHQ is aligned to interact smoothly with the new field structure, the DI and the SET are assessing the alignment between the DI and the field and between the DI and other FBIHQ elements. Enhancements will likely be made to the current FBIHQ structure.

On a parallel track, the SET will rollout changes in the area of human capital. Some of these efforts, including recruitment of analysts, are already underway. SET members, recruiters, and IAs piloted our new recruiting approach at four campuses: George Washington University, Columbia University, the University of Maryland, and the University of California, Los Angeles. Additional recruiting activities are ongoing at other campuses and potential sources of candidates, including military bases. Rollout of all human capital initiatives will continue throughout 2008.

The Training Division is heavily involved with the SET efforts. They are developing specialized training courses, including Virtual Academy courses, for all aspects of the intelligence operations rollout. For example, they are preparing to deliver a Chief Reports Officer training course prior to the rollout in most field offices. They are also producing training materials and job aids.

To support longer term efforts, the New Agent training curriculum has been completely revamped and will be revised again in six months to reflect the SET initiatives. Training Division is also very engaged with development of advanced training options for Special Agent and IA career paths.

CONCLUSION

Our mission is to provide domestic security for the United States – to understand threats to this country well enough to dismantle those threats, whether they are from gangs, organized crime, or al-Qa'ida. Intelligence allows us to understand. Law enforcement authorities allow us to halt and dismantle those threats.

Many of the threats we face are regionally, nationally, or internationally networked. They cannot be understood by looking at them through the lens of one squad, program, or field division. Until we look beyond these "stove pipes" to the entirety of the organizations that threaten us, we cannot ensure that the law enforcement tools we use are optimally employed against the best targets. We are not fully succeeding in our mission if we simply disrupt organizations that our capabilities can and should allow us to dismantle. If we miss important threats, we are not succeeding at all.

The new field intelligence structures and processes outlined in this document are designed to help us maximize all of the FBI's investigative capabilities to protect our communities, our country, and our various ways of living. The capabilities we must harness exist within the organization now, with our dedication to duty, unyielding perseverance, and unwavering fidelity of purpose, we can, will, and must succeed in this endeavor.

SET
Strategic Execution Team

STRATEGIC EXECUTION TEAM – PROJECT AT A GLANCE

A Strategic Execution Team (SET), made up of Agents, Intelligence Analysts, and other professionals from the field and Headquarters, completed an exhaustive assessment process to examine the strengths and weakness of our intelligence efforts. They also looked at what is working well, and used what they learned to create a multi-faceted plan to enhance the FBI's intelligence our capabilities.

	Identified Weaknesses and "Pain Points"	Initiatives Underway
Production and Dissemination	• Constrained flow of information from collector to rest of FBI • Slow dissemination of Intel Information Reports • Low throughput of IIRs leads to wasted time/effort • Limited awareness of customer preferences	• Put in every field office a certified Chief Reports Officer accountable for consistent high-quality production and dissemination of raw intelligence • Deploy the Collections Operations and Requirements Environment (CORE), a SharePoint-based tool to help us generate raw intelligence that is responsive to requirements and track how we are doing in meeting those requirements. • Delegate authority lower into organization to approve IIRs • Enhance feedback process
Collection Requirements	• Collection requirements not widely understood • Requirements flow not centralized	• Establish Collection Management Coordinator in each field office to develop and maintain a comprehensive local Intelligence Collection Strategy and cascading Collection Plan based on field office prioritized requirements and collection capabilities • Embed intelligence analysts with operational squads
Human Sources	• Insufficient volume and quality of sources • Low utilization of sources	• Improve processes and incentives to better leverage the capabilities of sources opened for specific cases • Establish in all field offices a HUMINT collection program of Special Agents dedicated full-time to acquiring new sources and exploiting existing sources • Create standardized mechanisms for validating sources • Create a HUMINT liaison program to expand and exploit relationships with external partners for purposes of collecting intelligence
Collaboration	• Structure of Field Intelligence Groups (FIGs) not conducive to collaboration	• Standardize 56 diverse FIG structures along best practices to increase collaboration between intelligence and operations, coordination across field and with HQ, and accountability for intelligence gathering, analysis, use and production • When justified by a validated Domain Assessment, establish cross-programmatic local Desks to develop local expertise on priority issues, and establish clear issue-oriented communications channels across the nation
Domain Awareness	• Limited domain awareness restricts strategic resource allocation	• Establish central strategic coordinating component with Domain Management Coordinator to: – Provide comprehensive view of domain across all programs – Develop an integrated, comprehensive intelligence collection strategy that leverages all collection capabilities against priorities
Human Resources	• Variable quality of analysis of finished intelligence	• Execute targeted recruitment strategy for analysts • Improve analyst selection process to consistently identify candidates who will succeed in the role. • Strengthen career paths and training for analysts and agents • Make improvements to performance systems
Management and Accountability	• Ideas developed are not fully exploited • Inspection process misaligned with strategy • SSA/SIA approval process is slow	• Establish standard processes to ensure intelligence supports effective decision making across the field office • Establish metrics for collection, information dissemination and integration, analysis and action; tie to rewards and appraisals • Launch COMPSTAT-like review process; cascade to all levels • Reengineer Inspection process