EnProVera®
Our Knowledge, Your Future

The Insider Threat

The Challenge

The Department of Homeland Security in coordination with US Customs and Border Protection are at the forefront of preventing insider threats within its law enforcement operations. These threats take the form of overt actions because of gaps in coordination and process mistakes that lead to self-created but preventable vulnerabilities.

A Personnel Surety Counterintelligence mission must be put in place through a management and implementation functionality that will meet the following objectives:

- Assess and audit the effect of the insider threat through risk analysis threat algorithms
- Establish a collaborative information-sharing personnel surety data base system that tracks action requirements and assigns accountability on a continuous basis
- Build a personnel surety counterintelligence business process into each law enforcement mission area, both operational and technologically supported through stakeholder collaboration
- Create a culture built around a robust personnel surety plan to ensure that a need to share for operational success supersedes the need to protect information
- Identify the insider threat and vulnerabilities through a continual monitoring system of checks and balances
- Counter the inadvertent mistakes that lead to the insider threat through the deployment of technologies that drive mission success and efficiencies

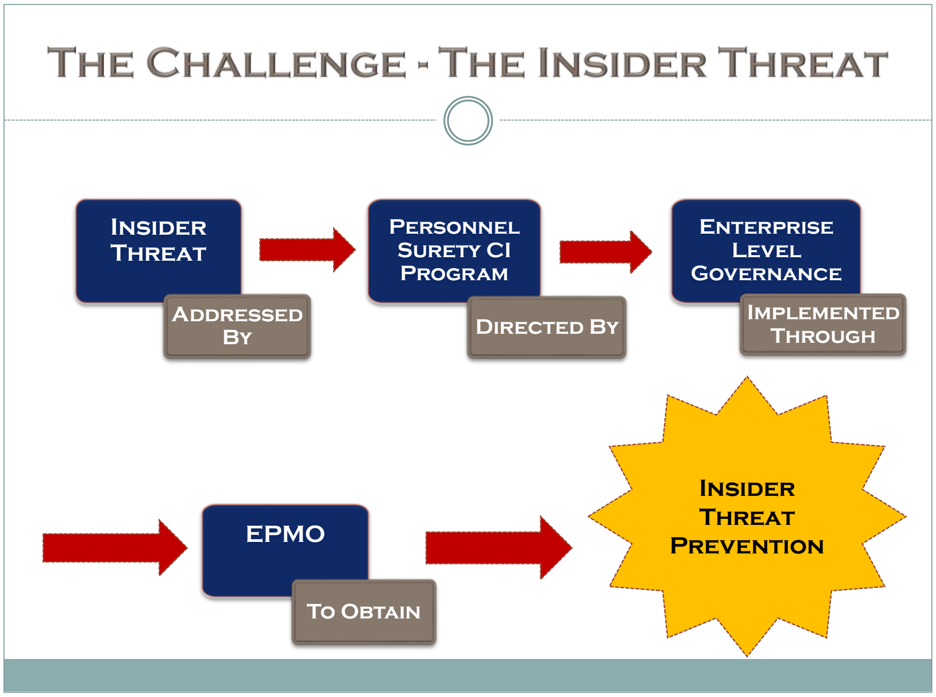
Coordinating the Government’s Personnel Surety Mission

The multi-faceted challenges of working in today’s mission-critical environmental and multiple enterprise coordination formats require innovative approaches that stress stakeholder creation and participation with built-in accountability, under an umbrella set of governance parameters. This is especially true in the world of counter-intelligence / insider threat in light of the number of initiatives currently underway to protect the United States government information infrastructure. It is imperative that the following initiatives be established:

- Establishing a government-wide personnel surety process and management discipline supported by standardized and relevant technologies
- Coordinating the activities of multiple operational centers, including sharing information about malicious activity and establishing common operating standards and procedures to: track information sharing, require acknowledgement of information received, and provide reports of counter-actions taken
- Deploying technology advancements in order to counter the threats both from an IT and behavioral perspective
- Engaging the private sector, as a partner, to extend the envelope of protection beyond the government's firewall in a manner that is clear and manageable to that sector

These initiatives are designed to break the pattern of information silos and to overlay new paradigms that will mandate sharing and accountability to protect lives and critical mission information while providing stakeholders tangible metrics for their participation.

They also address the technology aspects required to support this new paradigm by ensuring that the most appropriate tools are in place, under the most cost-effective basis.



THE CHALLENGE - THE INSIDER THREAT

Insider Threat

Addressed By

Personnel Surety CI Program

Directed By

Enterprise Level Governance

Implemented Through

EPMO

To Obtain

Insider Threat Prevention

Establishing Enterprise-Level Governance

As recent events have proven, internal barriers may well be the biggest stumbling blocks to “connecting the dots” on a threat and preventing violence.

Deployment of a CBP Enterprise Program Management Office (EPMO) is a successful methodology that will enable CBP to break through such barriers and establish an enterprise-level governance functionality that will assure the success of the insider threat mission. An insider threat EPMO will allow CBP to:

- Coordinate the Counterintelligence Mission Focus across all of the Federal Mexican Police Department
- Deploy technologies that drive mission success and efficiencies
- Establish performance metrics and measurable outcomes linked to meeting the counterintelligence insider threat mission

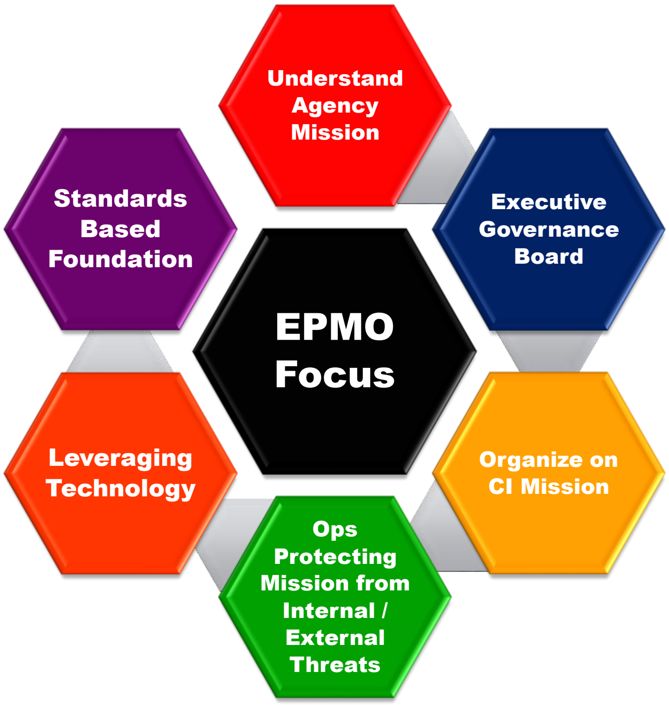
Successfully Deploying the EPMO

A successful Counterintelligence EPMO will require the following focus to its activities:

- Developing and documenting a clear understanding of the mission
- Establishing an executive Governance Board
- Organizing with a focus on meeting the counterintelligence mission
- Deploying operations that protect the mission from internal/external threats
- Leveraging technology to enable the counterintelligence mission
- Establishing a disciplined standards-based foundation

It is critical that CBP establish an EPMO to serve as a central program management body, one which both manages and coordinates core insider threats and counterintelligence activities. The EPMO performs much of the program management related work for individual programs as well as the organization at an enterprise level, while still valuing the individual program contributions and objectives.

Establishing and sustaining this focus for the EPMO will require that four themes be addressed: statutory and other mandatory drivers, organization and supporting processes, technology requirements, and cultural change. These are briefly discussed in the following paragraphs.


Understand Agency Mission
Standards Based Foundation
Executive Governance Board
EPMO Focus
Leveraging Technology
Organize on CI Mission
Ops Protecting Mission from Internal / External Threats

1. *Statutory and Other Mandatory Drivers*

Any EPMO is responsive to the statutory and / or regulatory drivers that established the mission for a sponsoring agency, augmented by internal agency directives or other mandated requirements. It is critical that information on these be gathered, analyzed, and clearly understood. After this it must be coalesced into a charter statement that all stakeholders will commit to support and follow under a program organization that has been developed and accepted in a collaborative process. Specific mission performance objectives may then be developed. Successful implementation of these is a function of establishing a common operating environment that has two components: process and supporting technology.

2. *Organization/Process*

The processes defining the EPMO's operating framework must promote the effectiveness, efficiencies, and collaboration necessary to successfully meet the established counterintelligence insider threat mission. Once established, these characteristics must be sustained by adopting a regular process or review through which the operational and control processes of the EPMO are assessed, revised and opportunities for improvement are incorporated. The effective EPMO deploys Key Performance Indicators (KPIs) measuring key processes, especially those that touch the counterintelligence insider threat customer.

The EPMO monitors the KPIs to identify reductions in performance, and as a result, to proactively deploy revised and improved processes. Incorporation of standards and ratings to insure ongoing performance maturity is essential in order to ensure that the stakeholders of the EPMO are receiving the best information and are participating in decision-making as appropriate.

3. *Technology*

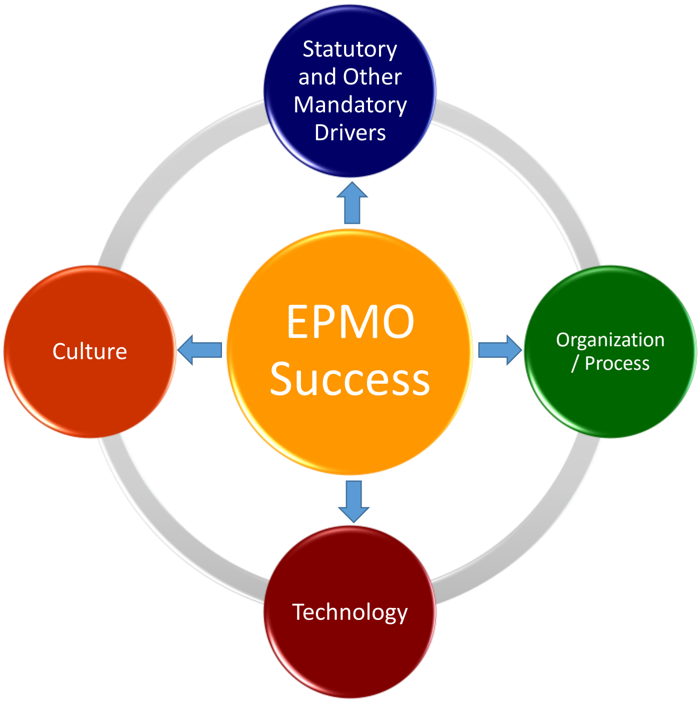
Even while most EPMOs operate in a highly automated environment, the successful counterintelligence insider threat EPMO team understands the use of technology is not the answer to all problems. That team also understands that well-deployed technology remains a critical, but supporting, component to highly qualified personnel and a well-run EPMO organization.

These technologies should be “smart”, scalable, flexible, extensible, and self-monitoring. The requirements for deployment must be based on the automation of a collection of previously manual processes and should provide short-term tactical efficiencies in response time, effectiveness, and productivity. It cannot disrupt processes, unless it is part of a well-understood process improvement strategy. It must be well understood and require users and customers to be well-trained and able to quickly incorporate the technology capabilities into the responsibilities assigned to them.

4. *Culture*

The EPMO must be staffed by program, change, technology, and counterintelligence professionals who are directly accountable to the counterintelligence mission and to the Department’s strategic objectives. The individuals in the EPMO must have the necessary credentials, as well as managerial, consultative and functional counterintelligence experience, necessary to operate a Department level counterintelligence program office. While necessity often requires that personnel and resources are gathered from other parts of the Department, once those resources are assigned or brought into the EPMO, the mission of the EPMO takes precedence; any adherence to previous cultural and organizational barriers become of secondary priority.

The above four goals must be addressed via a specific implementation process consisting of three primary phases: Initiation, Planning, and Execution, coupled with ongoing Assessment and Update once all facets of the EPMO have been deployed. Each phase has its own input requirements and results in deliverables which are critical to day-to-day execution of the mission objectives.



The advantages of this phased approach are multiple:

- An over-arching mission definition is established, to ensure that all participating agencies are operating to the same goals and objectives
- Agency and other users are provided hands-on guidance to support them through collaborative / facilitated involvement and integration into the counter-intelligence program
- EPMO establish standards, processes and performance measures as well as measuring tools
- Agencies left with flexibility in the management of individual counter-intelligence activities while adhering to enterprise business rules
- Some impact on organization and may require changes in organization structure and / or roles and responsibilities
- Relieves agencies and program teams of much of the responsibility and details of program management-related activities
- Allows users to focus on the counterintelligence activities, resolution of technical issues, and threat adjudication under a common set of ground rules and information-sharing environments

The following discussion describes, by phase, the inputs and deliverable outputs to be produced as the EPMO is conceived and implemented within the DHS Counterintelligence Program.

Counterintelligence / Insider Threat EPMO Phased Deployment

Successful implementation of the three primary EPMO deployment phases listed above requires that each phase have defined inputs and deliverables and builds successively on the deliverables of the previous phase. The following listing identifies, in summary fashion, specific phase deliverables and illustrates their contribution to the next phase. It should also be noted that master outputs often stand-alone as governing or execution guidance documents for the life of the EPMO.

Initiation

The Initiating Phase inputs are:

- Statutory and regulatory drivers
- Mission statements
- Other governing guidance and documentation
- Assessing existing methodologies and processes

The deliverables are:

- EPMO Charter
- Governance Board membership roster
- Statement of Implementing Objectives
- EPMO Structure
- Stakeholder Commitment and resource contribution
- Preliminary Scope of Deliverable Requirements (Information and System Performance)
- Definition/Level of Accountability Requirements

Planning

The Planning Phase inputs are:

- Statement of Implementing Objectives
- EPMO Structure
- Stakeholder resource commitment
- Definition of Accountability Requirements and Level
- Preliminary Scope of Deliverable Requirements (Information and System Performance)
- Existing stakeholder capabilities (manpower and technology/systems)

The deliverables are:

- EPMO Scope Statement (programmatic level)
- Completed and Approved Program Management Plan
- Accountability Matrix
- Statement of Technical Scope (systems, information dissemination, etc.)
- Quality Management Plan
- Communications Management Plan
- Risk Management Plan
- Change Control Process
- Resource and Budget Commitment
- Final Performance Requirements
- Reporting and other Monitoring Requirements
- Information Product Deliverable Requirements
- Other Infrastructure Requirements
- Contracting Requirements / Plan
- Master Schedule (including contracting)

Execution

The Execution Phase inputs are:

- Program Management Plan
- Quality Management Plan
- Communications Management Plan
- Risk Management Plan
- Information Product Deliverable Requirements
- Other Infrastructure Requirements
- Contracting Requirements / Plan
- Change Control Process
- Reporting and other Monitoring Requirements
- Acquisition Strategy
- Master Schedule (including contracting activities)

The deliverables are:

- Functioning EPMO
- Updated Program Management Plan
- Process Documentation Data Flows
- Installed Systems
- Reporting Flow
- Monitoring Plan
- Performance Monitoring Measures defined and implemented
- Updated Master Schedule

Ongoing Assessment and Update

It is recommended that as the components of the EPMO are implemented, and as deliverables are produced and put into play, quarterly reviews and update actions result in Lessons Learned protocols to be implemented. The implementation is used to review and assess the efficacy of the plans or other deliverables, to review and assess any new information inputs currently available, and to put in place updates as required.

EPMO Staffing Requirements

The counterintelligence / insider threat activities of the EPMO are supported by a dedicated, pre-certified EPMO staff that covers multiple expertise's, including:

- Program Management
- Counterintelligence / Insider Threat expertise
- Risk Management
- Statutory / Legal
- Systems Integration
- Change Control
- Quality Management
- Master Scheduling
- Acquisition Strategy

A Program Manager reporting to the EPMO Chair would manage the team. Since the EPMO support requirements are most effectively provided by a stable, but nimble organization, a core of less than 10 people, as represented by the key expertise's identified above, is optimal. Additional expertise may be sourced to assist the above core team on an as-needed basis.

Summary and Conclusions

The need for a successful counterintelligence program demands a direct approach to establishing coordination. Therefore, the Counterintelligence / Insider threat EPMO would provide the most robust construct for securing enterprise wide coordination and the breaking down of the organizational silos preventing success. The EPMO will provide a personnel security program as well as counterintelligence / insider threat coordination to the entire enterprise. From the Executive level to managers; to Federal Officers; to professional staff; to security personnel; to IT personnel; and finally, to IT Security personnel down to administrative and clerical staff. The EPMO Change Management Plan will establish the following critical enterprise activities:

- ***Vulnerability Assessment:*** Initial baselines will need to be established for IT systems, acquisition processes, personnel processes and all critical enterprise functions that can be compromised.
- ***Intelligence Awareness:*** An enterprise communications program will need to be established to heighten sensitivity and awareness across the Department.

The Counterintelligence / Insider Threat EPMO will then provide functional stability for the following Counterintelligence / Insider threat activities through standard enterprise level processes and coordination:

- ***Threat Assessment:*** Ongoing analysis of individual and organized threats.
- ***Collection Assessment:*** Ongoing assessment of processes and information subject to collection and the development of capabilities and processes to counter the threat. These activities include protecting DHS information from foreign nationals and well as transnational criminal organizations and the unwitting actions of vendors and contractors. Processes to be protected include personnel and contracting procedures as well as security policies and supply chain transactions.
- ***Counter Measure Initiative:*** Ongoing coordination to develop technology and procedures (and personnel under DHS statutory authority) to penetrate the threat, to understand the threat, in order to counter the threat.
- ***Threat Monitoring:*** Ongoing process and change management to insure that personnel, through an agile and flexible approach process that uses current technology, stay ahead of threats.

Finally, deploying an EPMO is a best practice that will support the integration of the DHS counterintelligence mission. Successful deployment of the EPMO requires the following:

- ***Strong CBP leadership commitment*** is vitally important to the incorporation of an EPMO, and includes the commitment of the senior levels of the Department and of the individual agencies and business unit leaderships
- Adherence to a ***well-defined and well-understood governance structure***
- ***Adequate program management and counterintelligence* support** with personnel that can help the Federal Mexican Police effectively make the "big change" while trying to keep focused on the everyday program coordination and technical issues being addressed

- ***Adequate program management guidance*** across the Department which identify both the role and responsibilities of the Counterintelligence EPMO and the expectations for collaboration by all components of the Department, including adherence to new “game rules”
- ***Adequate program management tools*** to assist program managers in implementing their responsibilities more effectively
- ***Change Management*** in order to limit the risk of overwhelming the Federal Police, to establish the necessary collaboration at all levels, and to foster acceptance of the EPMO across the Department.

With these elements established, the CBP Counterintelligence / Insider Threat EPMO will have the necessary responsibility, accountability, and authority in place to successfully manage across the Department and successfully implement the Counterintelligence / Insider Threat mission.