

# CBP-IA Five Year Report

December 31

# 2012

*This report summarizes the mission, functions and operations of the CBP Office of Internal Affairs, including its challenges, organizational response and key accomplishments in promoting the integrity and security of CBP and its workforce.*

Fiscal Years  
2008 to 2012

James F. Tomsheck  
Assistant Commissioner  
Office of Internal Affairs



# Message from the Assistant Commissioner

---



I am pleased to present this five-year report which details the successes the employees of the Office of Internal Affairs (IA) have achieved during fiscal years 2008 through 2012. The accomplishments described in this report highlight the dedication and commitment of every IA employee who performs his or her duties in an exemplary manner in support of CBP's mission to secure our nations' borders while fostering legitimate travel and trade.

Over the past five years, the IA mission has continued to evolve. As an organization, IA has significantly changed in response to the administration initiatives and legislative mandates that required a more timely assessment of employee backgrounds, and the expanded use of polygraph to screen all applicants for CBP law enforcement positions. At the same time, IA increased its presence in the investigation of employee corruption and misconduct; transitioned from reactive to preemptive efforts to identify, deter and disrupt potential workforce misconduct through behavioral analysis; expanded covert testing and enhanced internal inspections and reviews to assess the organizational health and security of CBP, its operations, its facilities and its personnel.

In the coming years, those of us who have chosen public service as a career will face a number of challenges. We will be asked to do more with less in an era of fiscal constraints that will impact not only financial resources but the ability to maintain staffing levels to which we have become accustomed. In anticipation of these challenges, we must all work together to ensure our limited resources are applied in an effective manner, and that we seek opportunities to develop new alternatives that allow us to execute the IA mission in a more efficient manner.

Looking ahead, I am committed to continuing our efforts to build and sustain collaborative relationships with our partners both internal and external to CBP. These partnerships are critical to assuring the integrity of CBP and its workforce while improving and streamlining processes that will allow us to achieve our organizational goals.

I have every confidence in the professionalism and abilities of the men and women who represent the Office of Internal Affairs and who demonstrate their dedication to duty on a daily basis. I look forward to the opportunity to continue to serve with each of you.

James F. Tomsheck  
Assistant Commissioner  
Office of Internal Affairs



## **Table of Contents**

<b>About the Office of Internal Affairs .....</b>	<b>6</b>
<b>Building Capacity and Capability.....</b>	<b>8</b>
<b>Organization .....</b>	<b>12</b>
Counterintelligence and Operational Liaison Group .....	13
Investigative Operations Division .....	15
Integrity Programs Division .....	17
<b>Security Section .....</b>	<b>19</b>
Credibility Assessment Division .....	19
Personnel Security Division .....	21
Security Management Division.....	22
<b>Testing and Evaluation Section .....</b>	<b>23</b>
Management Inspections Division .....	23
Operational Field Testing Division .....	25
<b>Evolving CBP Integrity Challenges.....</b>	<b>28</b>



## ABOUT THE OFFICE OF INTERNAL AFFAIRS



The Office of Internal Affairs (IA) serves as the Chief Security Office for U.S. Customs and Border Protection (CBP) and manages a wide range of investigative and security functions and programs including: applicant and employee background investigations and clearances; employee integrity and misconduct investigations; integrity awareness; corruption detection through research and data analysis; operational field testing; credibility assessment, including polygraph examination; physical, information, industrial, and operational security; as well as management inspections and audit liaison. An aggressive program to combat internal corruption and misconduct is fundamental to ensuring

successful execution of CBP's law enforcement, trade and national security missions. America's citizens bestow great power and authority upon their law enforcement organizations. They expect and deserve accountability from their law enforcement public servants. A strong, proactive IA office plays a vital role in developing and implementing such a program.

### Vision

In June 2006, James F. Tomsheck was appointed Assistant Commissioner (AC), Office of Management Inspections and Integrity Assurance (MIIA). Shortly thereafter, the name of the Office and its functions were reconstituted as the Office of Internal Affairs. Under a new leadership vision, IA began working proactively in partnership with all of CBP's component organizations, as well as in collaboration with other law enforcement entities, to promote the integrity and security of CBP and its workforce.

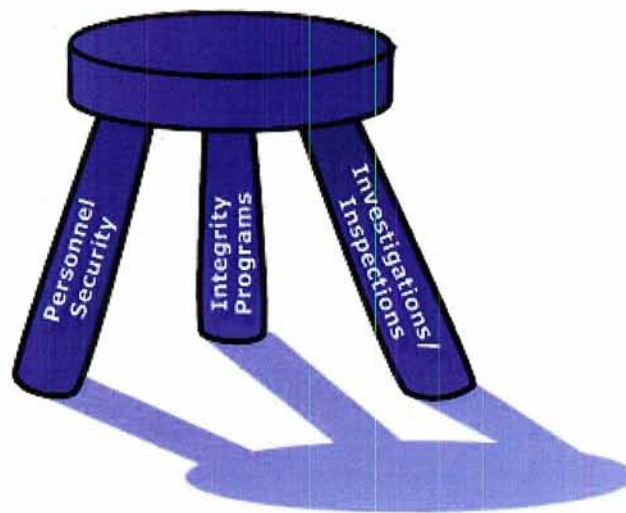
### Mission

As the law enforcement agency responsible for securing our Nation's borders and facilitating lawful trade, the public has placed its trust and confidence in CBP. To preserve that bond and to promote organizational and workforce integrity, IA pursues a **comprehensive integrity strategy** designed to **prevent, detect and investigate** all threats to the integrity of CBP and its workforce; and sustains an **integrity continuum**, reviewing CBP operations on an ongoing, basis to ensure that incidents of corruption and misconduct are prevented, detected and investigated timely.

- **Prevention:** CBP-IA has enhanced background investigations and has implemented a polygraph program for CBP law enforcement applicants.
- **Detection:** CBP-IA conducts data research and behavioral analysis designed to detect corruption, develops data/intelligence to drive the focus of integrity investigations, and applies "Insider Threat" methodologies for advanced detection of integrity threats.

- **Investigation:** CBP-IA investigative resources engage in cooperative and collaborative border corruptions investigations through participation in Border Corruption Task Forces with FBI, DEA, DHS OIG, ICE and other federal, state and local law enforcement partners. CBP-IA has deployed over 200 experienced investigators to 22 strategically selected field offices. These investigators average over 20 years of 1811 criminal investigator experience and have been selected from an array of federal agencies.
- **Integrity Investigations Continuum:** CBP-IA uses proactive behavioral science and analytical techniques to identify corruption and insider threat based on data gathered in background investigations, polygraph examinations, known cases of corruption, and other sources. The results of this research and analysis drive the focus of proactive integrity investigations and operations designed to detect, deter and disrupt workforce corruption and misconduct.

This strategy provides the framework for the Office of Internal Affairs to plan and carry out its critical mission within U.S. Customs and Border Protection and the Department of Homeland Security.



***The Office of Internal Affairs mission is clear and critically important - to promote the integrity and security of the CBP workforce.***

## **BUILDING CAPACITY AND CAPABILITY**

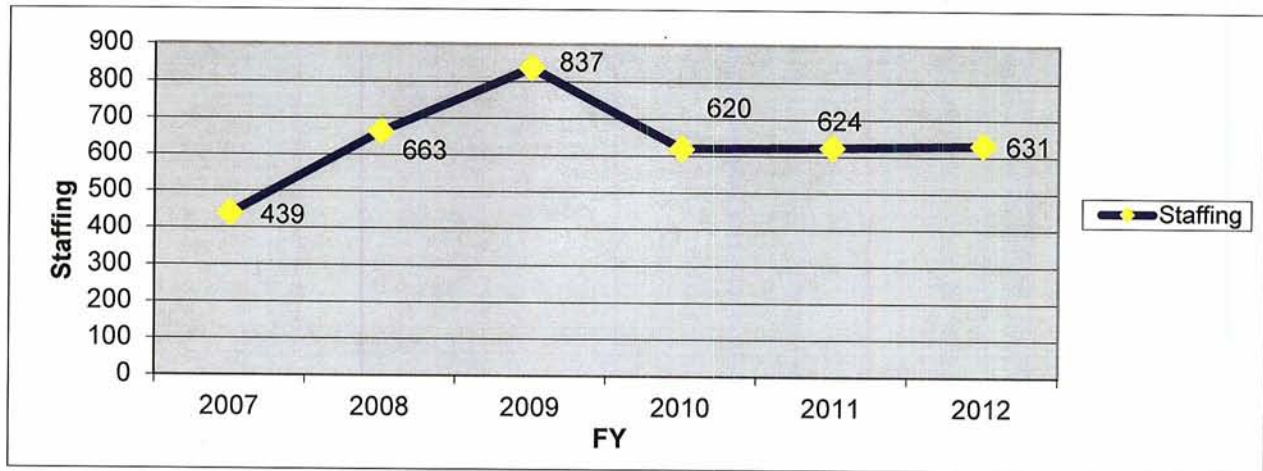
In March 2003, in response to the terrorist attacks of September 11, 2001, the U.S. Government underwent its most dramatic reorganization in over 50 years with the creation of the Department of Homeland Security (DHS). The reorganization was not limited to simply moving agencies from one department to another; rather, it involved the dismantling of existing agencies and the formation of entirely new entities. CBP was one such entity, bringing together elements from the former U.S. Customs Service, the U.S. Immigration and Naturalization Service and the Department of Agriculture. The result was a larger workforce which required increased support from IA. The office needed not only an investigative cadre but an enhanced infrastructure.

With the rapid growth of Internal Affairs (IA) which began in 2007, it soon became apparent that the infrastructure to support operations was insufficient. Prior to the expansion, a small program management staff oversaw budget formulation and execution and managed staffing for the organization. This group also handled mission support activities for the Assistant Commissioner's staff. To meet the challenges inherent in the expansion of responsibility, facilities, staff, and budget, an Administration and Operations group was established in 2008. The group is comprised of staff organized around the day-to-day administrative activities associated with funding, staffing, logistics, and asset management as well as staff responsible for operational capabilities that further empower Internal Affairs to carry out its mission and fulfill its vision.

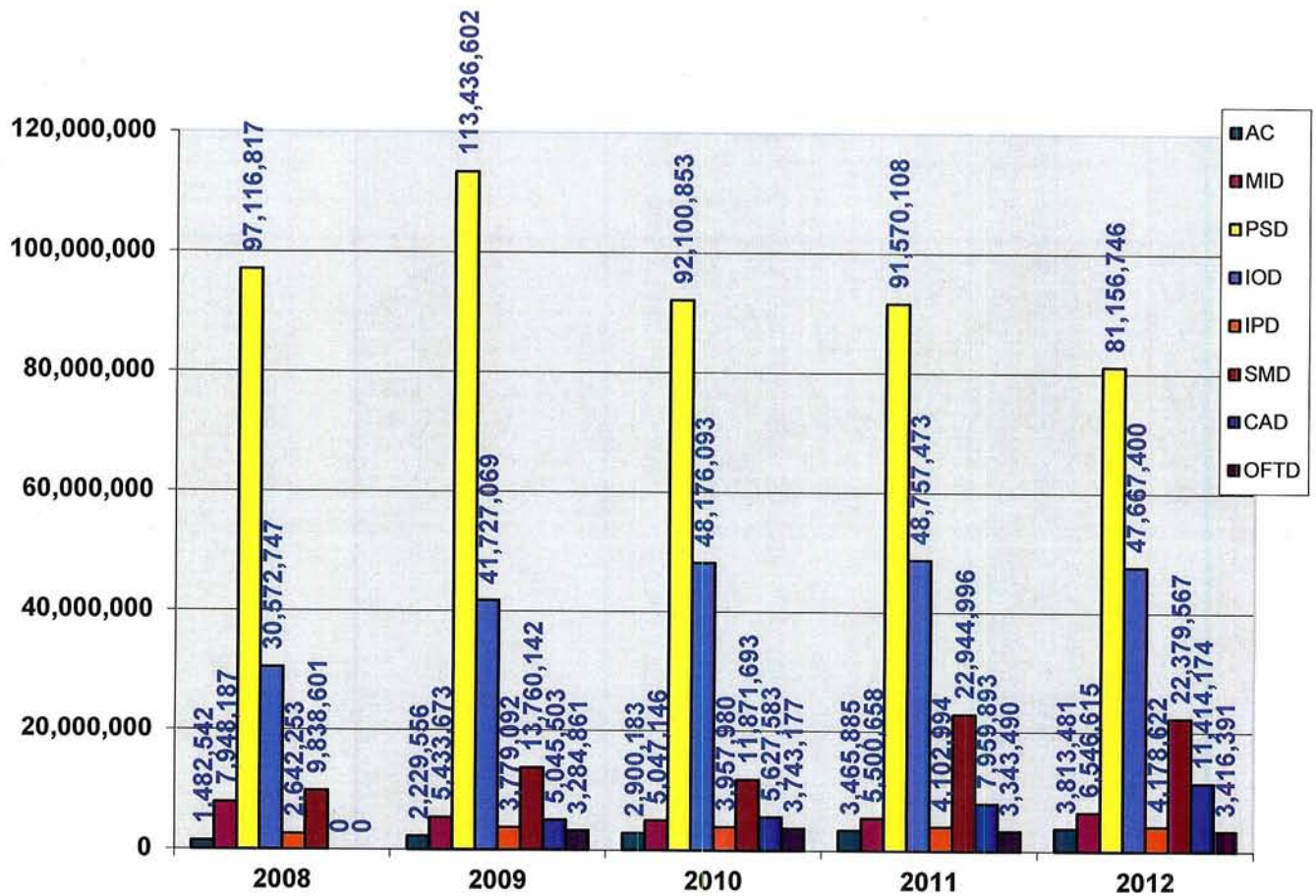
## **Funding and Staffing**

Between FY 2007 and FY 2009, the Office of Internal Affairs nearly doubled its staffing from an initial staffing level of 439 to a high of 837 employees. This growth in IA staffing was primarily in response to the 2006 Presidential Hiring Initiative and the reconstitution of an internal investigations capacity to address CBP employee corruption and misconduct issues. To achieve its mission responsibilities in a timely and effective manner, IA utilized the services of reemployed annuitants who were prepared to enter on duty and immediately begin executing the IA mission based on the experience gained from prior federal service and obviating the need to develop and deliver lengthy entry-level training programs. The use of reemployed annuitants also allowed IA to adjust the size of its workforce to reflect changing mission priorities such as the conclusion of the 2006 hiring initiative, the creation of the IA polygraph program and the IA response to mandates included in the Anti-Border Corruption Act (ABCA) of 2010. Today, IA staffing stands at approximately 631 employees including those assigned to IA Headquarters in Washington, DC and twenty-five field locations throughout the U.S.

## Total Staffing By Fiscal Year



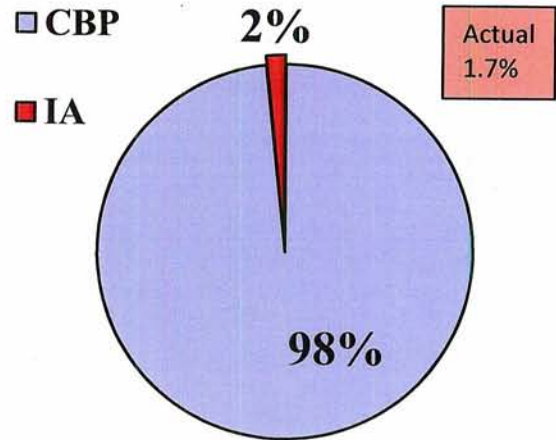
## Funding and Staffing By Fiscal Year



TOTALS: \$150,044,666 (663) \$188,771,290 (837) \$173,466,299 (620) \$184,896,952 (624) \$180,609,585 (631)

## IA Portion of CBP Budget

Even with its broad mission, to promote the integrity and security of the CBP workforce, the Office of Internal Affairs budget currently comprises only 1.7% of the overall CBP budget.



## Field Offices

During fiscal year 2006, IA began efforts to establish field offices in strategic locations across the country. During 2007 and 2008, delineated areas of responsibility were identified, requirements were developed and site-awards were made for the selection of office space in 25 locations.



## Headquarters Relocation Project

IA's growth also resulted in a need for additional space in the National Capital Region (NCR). Existing space limitations necessitated that IA personnel operate in four separate buildings. Working environments were overcrowded, with insufficient space for operations and storage of sensitive files. In addition, lack of collocation of related functions created a less than ideal environment for carrying out the IA mission. In 2008, CBP's Office of Administration (OA) determined that certain CBP components including IA would be located in alternate housing in order to allow larger CBP components such as Border Patrol, Air & Marine, Office of Field Operations, etc., room to expand within the Ronald Reagan Building (RRB). To accomplish the relocation and consolidation of IA, a program of requirements was developed and a Solicitation for Offers for lease of approximately 75,000 rentable square feet was published in October, 2009. A lease award for space at 90K Street NE was made in late April, 2010. The space was designed around operations, with co-location of related functions and an environment that promotes interaction and teamwork among Divisions.

Six of IA's Divisions are now housed in the new location. As a direct result of co-location, IA has eliminated duplication of effort in our mission support operations, consolidated and shared resources, and expanded and contracted quickly and efficiently with minimal costs in response to changing operational requirements. As a result of design analysis and subsequent renegotiation of existing leases in field offices, IA will save a total of \$8,352,950 in contract costs over the next ten years.

### **Administrative Services FY 2012 Accomplishments:**

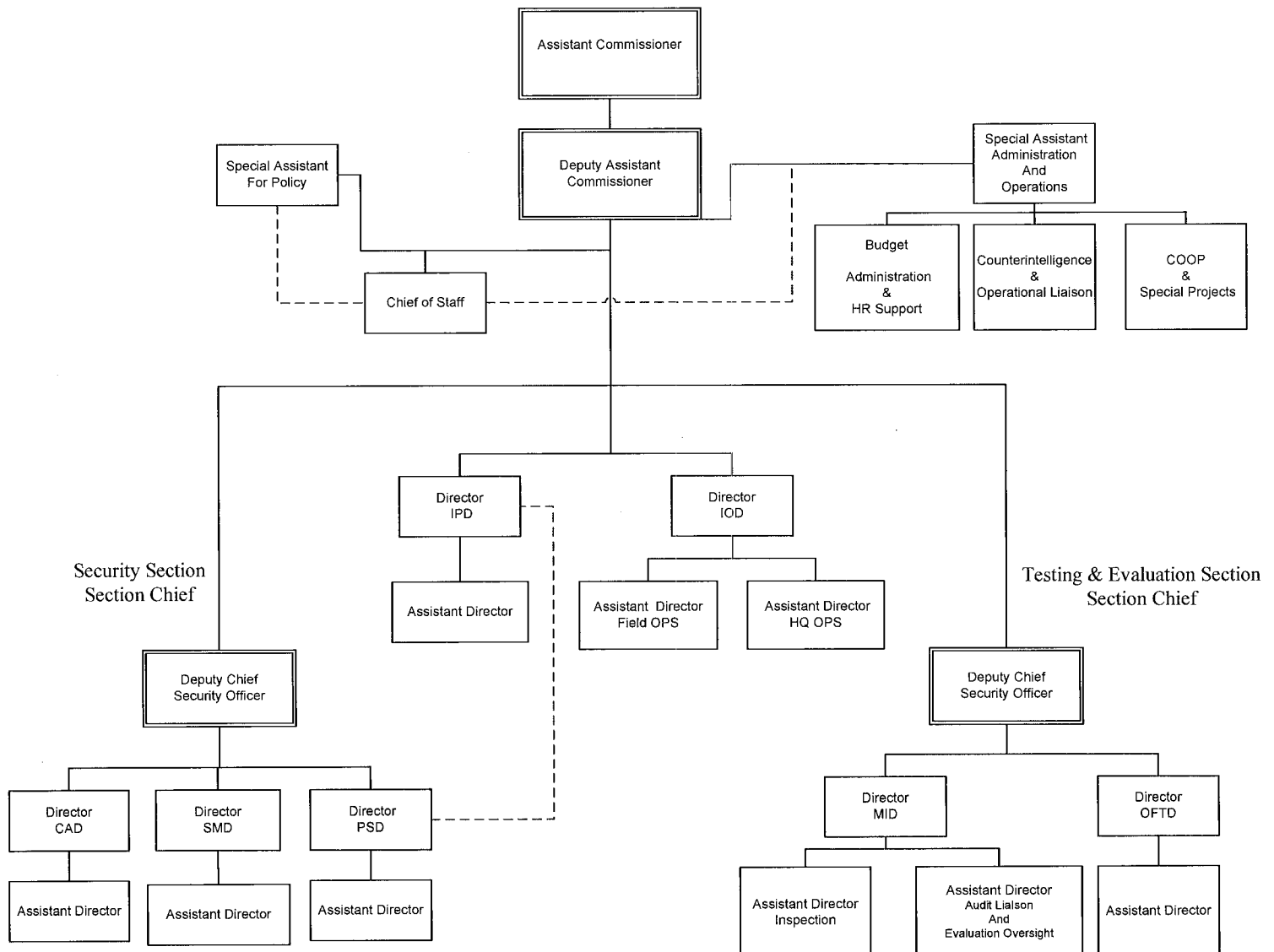
- ✓ Completed 90K Phase I build out and moved 6 divisions into new space.
- ✓ Continued oversight of 90K Phase II build out with an anticipated move date of November 2012.
- ✓ Created Customer Service Desk at 90K under the IA Shared Services Concept.
- ✓ Reviewed operational needs and completed design analysis of field offices resulting in a reduced footprint of 24,126 sq. ft. of office space and a cost savings of approximately \$835,295.



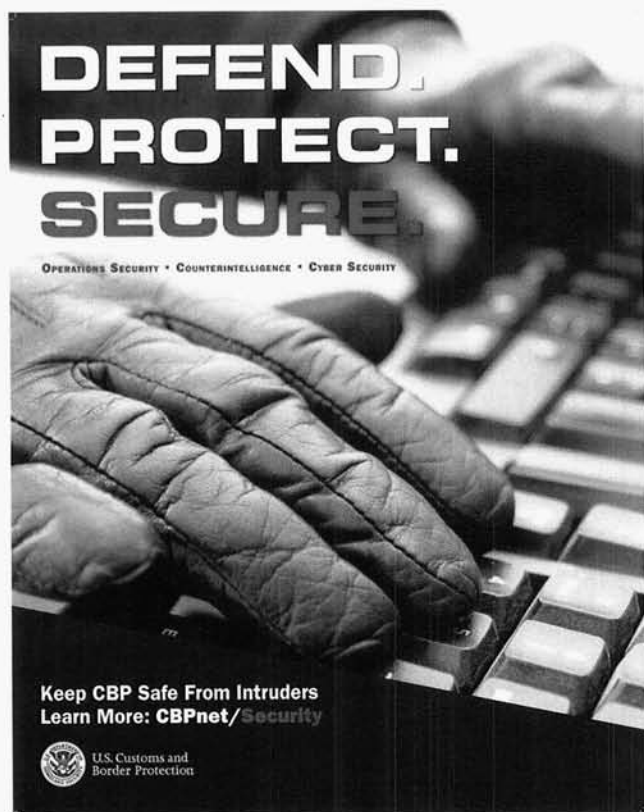
*Nathan L. Davis, Project Director and Team Lead cuts ribbon for the new IA space at 90K Street as Chief Operating Officer Winkowski, Assistant Commissioner Tomsheck and DAC Hamrick look on. (Not in view: Assistant Commissioner Eugene Shied).*  
*Photo Credit: James Tourtellotte*

## ORGANIZATION

The newly designated IA office was designed to better serve CBP, as well as to provide greater visibility with our functional counterparts in the law enforcement community. In response to increasing mission demands and the need to address more complex challenges, the Office has grown from 4 to 7 divisions, expanding capabilities in personnel screening, physical security, operations, inspection, investigations, credibility assessment, covert testing, behavioral research and counterintelligence.



## Counterintelligence and Operational Liaison



In August of 2008, the Secretary of DHS directed the establishment of a DHS-wide Counterintelligence (CI) effort to detect and deter the growing threat posed by Foreign Intelligence Services, terrorist organizations and foreign criminal enterprises. In 2009, consistent with IA's objective to employ a comprehensive integrity strategy of prevention, detection and investigation in order to promote the integrity and security of the CBP workforce, the Counterintelligence and Operational Liaison Group (CIOLG) was established. The CIOLG's primary responsibility is to develop a defensive CBP CI and a Cyber Security capability that will make the foreign penetration of CBP harder to achieve and easier to detect.

The pursuit of the CI mission within CBP is uniquely challenging. CBP, the largest component of DHS and the largest law

enforcement agency in the United States, has employees deployed across the nation and around the globe. These employees pursue CBP mission objectives world-wide, while in routine contact with foreign nationals. Through routine contact and traditional collection methods, Foreign Intelligence and Security Services, Transnational Criminal Organizations (TCOs) and other Foreign intelligence entities all seek to exploit the assets of CBP to advance their own goals and objectives. Trusted Insiders and cyber Intruders also pose a significant threat to CBP. The CBP CI program works across the CBP enterprise, integrating information and unifying mitigation efforts regardless of source, methodology or mission; and links CBP with the DHS CI program and the United States Intelligence Community (IC) to provide a united front against adversarial intelligence activities.

The Counterintelligence Program Strategic Plan for 2013-2018 provides the foundation and framework for the CBP CI and Cyber Security programs. This strategy aligns with the National Counterintelligence Strategy of the United States, published by the Office of the Director of National Intelligence, and is informed by the Defensive Counterintelligence Program Blueprint, published by the Office of the National Counterintelligence Executive. It is also an adjunct to the CBP Internal Affairs Strategic Implementation Plan (IASIP). The plan consists of the following core areas: Awareness, Working Groups, Cyber Security, and Reporting, as well as Threat Detection and Mitigation.

The CIOLG recognized in 2009 that CI and Cyber Security awareness was key to the success of the program and the security of CBP and consequently initiated an aggressive awareness campaign to educate the workforce regarding CI and Cyber threats and vulnerabilities. In addition, specific CBP offices (i.e., Office of International Affairs, the Container Initiative, Office of Field Operations; International Liaison Unit, Office of Border Patrol) have made CI briefings mandatory for their staff. The CIOLG forged a unique relationship with the CBP Office of Public Affairs to launch the "Defend.Protect.Secure" awareness campaign. This multi-platform, agency-wide security campaign combined CI, Cyber and Operational Security awareness messages that were delivered to the workforce via posters, magazine articles, and a dedicated webpage on CBPnet. The CIOLG also developed and deployed a CI Virtual Learning Center module that is available to all employees. The CIOLG chairs two working groups and one committee that address significant CI issues that impact CBP. They are the International Visitor Program Working Group, the Insider Threat Working Group and the Counterintelligence Advisory Committee comprised of representatives from across CBP. The CIOLG also participates in DHS and CI community working groups.

#### CIOLG FY 12 Accomplishments:

- ✓ Finalized and distributed the "Counterintelligence Program Strategic Plan 2013-2018."
- ✓ Partnered with the Office of Information Technology (OIT) and the Office of Public Affairs (OPA) to launch the "Defend. Protect. Secure." CBP security awareness campaign designed to inform and empower CBP employees to be proactive in their efforts to protect CBP information from those who seek to do our country harm.
- ✓ Launched a dedicated "CBP Security Awareness Campaign" webpage on CBPnet that features security tips and detailed information regarding CI, cyber security and operational security.
- ✓ Partnered with the Office of Field Operations, Container Security Initiative (CSI) to make the Counterintelligence Awareness Course on the CBP Virtual Learning Center mandatory training for all CSI employees both domestic and abroad.
- ✓ Completed a CBP counterintelligence/cyber threat assessment in coordination with OIT and the Office of Intelligence and Investigative Liaison (OIIL).
- ✓ Created and distributed International Visitor Program reports that assess CBP agency-wide international visitor activity in coordination with the Office of International Affairs (INA).
- ✓ Established the Counterintelligence Advisory Committee which is composed of representatives from OIIL, OIT, OFO, INA, OCC, OBP, OAM and OT.

## **Investigative Operations Division**

In 2012, the Investigative Operations Division (IOD) celebrated its fifth anniversary as a key component in IA's ongoing effort to promote integrity and combat corruption within CBP. IOD's accomplishments have been significant; in the span of a few years, a tradition of professionalism and investigative excellence has been forged. IOD has grown from a handful of employees centered in Washington, DC, into an organization of over 230 employees performing mission-essential duties around the country.

### **IOD FY 2012 Accomplishments:**

- ✓ Processed and/or monitored 6,823 allegations of misconduct and other reportable incidents involving current or former CBP employees, contractors, civilians or unknown subjects through the Joint Intake Center (JIC).
- ✓ Documented, investigated and/or tracked 339 CBP employee arrests. Of the 339 total arrests, 11 involved corruption or mission-compromising corruption charges.
- ✓ Completed 1,189 Closing Reports of Investigation (Blue Books) involving allegations of criminal or serious CBP employee misconduct or mismanagement. Of that total, 54.7% were completed in 120 days or less.
- ✓ Enhanced and active participation in 101 OIG investigations, 505 ICE OPR investigations, and 123 BCTF/PCTF investigations all targeting criminal activity within the CBP workforce.
- ✓ Seventy-two (72) CBP collateral duty fact finders received training in support of the National Fact Finder Program, bringing the total number of trained fact finders to 364.

The creation of CBP consolidated functions previously scattered throughout other U.S. Government departments and agencies into a single bureau focused on border security. As CBP accelerated hiring and dramatically increased in the number of law enforcement personnel assigned at and between the nation's ports of entry, the threat of internal corruption also increased. This rapid expansion placed increasing numbers of young and inexperienced employees in front-line positions where violent and lucrative drug cartels constantly seek new avenues of corruption. The deployment of technology, physical infrastructure and increased manpower along the border made it more difficult than ever before for these drug trafficking and other transnational criminal organizations to conduct and promote their illegal operations and resulted in the need to compromise and infiltrate the CBP workforce.

CBP deploys nearly 47,000 law enforcement personnel each day into the highest threat environment where there is a concerted effort on the part of TCOs to infiltrate and corrupt the CBP workforce. While the overwhelming majority of our

CBP workforce serve with honor and integrity, a small minority have betrayed the trust of the American public and their fellow CBP employees by engaging in illegal and unethical behavior.

The Joint Intake Center (JIC) within IOD serves as the central "clearinghouse" for receiving, processing and tracking allegations of misconduct involving personnel and contractors employed by Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). The JIC provides CBP and ICE with a centralized and

uniform system for processing reports of alleged misconduct. All misconduct allegations are coordinated with the Department of Homeland Security (DHS) Office of Inspector General (OIG) and referred to the appropriate office for investigation, fact-finding or immediate management action.

As CBP grew, the volume of allegations of misconduct lodged against its employees grew. It became increasingly apparent that workforce misconduct and corruption had the potential of compromising the critical CBP mission of border security. Due to the internal investigative structure in place at the time, OIG and OPR conducted all CBP internal investigations; CBP executive leadership lacked substantive visibility into investigative activities involving its employees. Executive leadership was unable to effectively address internal security threats and vulnerabilities.

CBP and Departmental leadership recognized outsourcing CBP misconduct investigation was ineffective. Not only were the OIG and OPR constrained by limited resources, they also lacked any direct accountability to CBP, its leadership and its organizational priorities. A substantial backlog of unresolved allegations began to grow and, commensurately, so too did CBP's vulnerability. In 2007, at the direction of the CBP Commissioner and with concurrence of the Department, IA implemented an aggressive plan to expand its internal investigative capability. IOD as we know it today was born.



IOD has established itself as a fundamental component of IA's Comprehensive Integrity Strategy predicated upon Prevention, Detection and Investigation. IOD established a field presence in key CBP operational areas, such as the southern and northern borders. IOD recruited a cadre of highly experienced Special Agents drawn from the U.S. Secret Service, ICE Office of Investigations, ICE Office of Professional Responsibility, the Drug Enforcement Administration, the Federal Bureau of Investigation (FBI), the Internal Revenue Service, multiple OIGs and other federal law enforcement agencies. This investigative workforce was augmented by CBPOs and BPAs trained by IA to conduct investigations, and a staff of trained fact finders to coordinate lower level investigations with the CBP component offices. IOD also began an aggressive program of investigative cooperation, liaison and outreach. Today, IOD maintains a core staff at IA headquarters in Washington, DC, and a force of nearly 200 Special Agents assigned to twenty-two field offices throughout the country.

## Integrity Programs Division

The Integrity Programs Division (IPD) is the research, analysis and education component of the Office of Internal Affairs (IA). Beginning in 2007, the decision was made to expand IPD and its capacity to move from a reactive posture primarily conducting post case analysis work to a strategic, proactive stance with analysts and behavior research specialists working collaboratively to identify potential acts of corruption and misconduct, identifying potential vulnerabilities in CBP operations; providing research and analytical support to ongoing investigations and isolating behavior potentially indicative of corruption and misconduct.

IPD drives the detection, deterrence and prevention of misconduct and corruption in the CBP workforce by utilizing proactive measures in three functional areas:

- **Data and Trend Analysis:** Analysts examine employees, enforcement actions such as narcotics seizures, and other strategic factors to identify anomalies or issues that warrant further investigation. Proactive operational teams focus on specific areas of vulnerability efficiently leveraging existing resources to better detect and deter threats or incidents of corruption and enhance internal investigations while supporting pre-employment screening operations.
- **Integrity Awareness and Anti-Corruption Training:** IPD provides Integrity Awareness training to CBP employees in partnership with the Office of Training and Development (OTD) during New Employee Orientation, Supervisory Leadership

### **IPD FY 2012 Accomplishments:**

- ✓ Delivered integrity awareness modules at 100% of new employee orientation sessions.
- ✓ Provided 4-hour integrity training modules at all Supervisory Leadership Training Course.
- ✓ Conducted 1-hour briefings to CSI officers prior to overseas deployment.
- ✓ Developed and implemented one long-term and one short-term research and development project focused on the South Texas Campaign (STC) area of operations as a method to preempt and disrupt the efforts of transnational criminal organizations to infiltrate or compromise the CBP workforce.
  - **South Texas Campaign (STC) Criminal Associates and Hometown Duty Assignment Pilot Study (Short Term Study)** Designed and executed a pilot study to determine the prevalence of reported criminal associates and hometown duty assignments in a random sample of 255 BPAs and CBPOs who entered on duty since FY2006 and are currently assigned to Maverick, Starr, Cameron, and Webb counties in the STC Area of Responsibility (AOR).
  - **South Texas Campaign (STC) Criminal Associates and Hometown Duty Assignment Study (Long Term Study)** Designed and executed a comprehensive study of a random sample of 354 BPAs and CBPOs currently assigned to the entire STC (AOR) to determine the prevalence of reported criminal associates and hometown duty assignments and the relationship of both to allegations/investigations of reportable misconduct.

Training, and pre-deployment of long-term assignments for the Container Security Initiative. As part of CBP's membership in the World Customs Organization (WCO), IPD delivers Anti-Corruption Training to international customs administrations.

**Behavioral Research Branch (BRB):** Social science researchers study internal threats at the individual, cultural, and organizational levels that may compromise the integrity of CBP and the law enforcement community at-large. Through the use of systematic operationally relevant research, program evaluation, and tracking of employee delinquency, IPD provides empirical grounding for detection, deterrence, and prevention efforts.

IPD has grown and developed into a division that provides highly accurate, reliable information on which CBP and IA leadership have come to rely. The complexity of analytical work products, thoroughness of behavioral research, and outreach to employees has grown exponentially. IPD continues to provide robust reactive case support to IOD and external law enforcement partners. The BRB provides reliable information and trend analysis on employee delinquency to CBP operational offices, media outlets, Congress, and others. Its research on misconduct and corruption replaces opinion and speculation with empirically derived results and implications.

## **SECURITY SECTION**

The Security Section is comprised of three Divisions: Credibility Assessment, Personnel Security and Security Management.

### **Credibility Assessment Division**

Five years ago, the Credibility Assessment Division (CAD) existed only as a vision in the minds of CBP leadership. Faced with unprecedented hiring surges designed to secure our nation's borders, and the knowledge that rapid expansion of law enforcement agencies had historically caused a dramatic increase in corruption within those agencies, IA requested authority to establish a polygraph program within CBP-IA. With support from the Commissioner, IA obtained the required authority from OPM to begin a polygraph pre-employment screening program for applicants for CBP law enforcement positions.

In January 2008, the first 12 newly-hired certified polygraph examiners arrived at the National Center for Credibility Assessment (NCCA) to train on the LEPET polygraph format, which was designed for law enforcement screening. In February 2008, CAD deployed its first operational mission to Dallas, in collaboration with PSD, several HRM components, and Border Patrol.

The results of the polygraph examinations were profound and revealing. Many applicants successfully completed the polygraph process and were quickly sent to Basic Agent Training at Artesia, NM. However, 58% of the applicants failed to successfully complete the polygraph and were found unsuitable. Their admissions confirmed the reliability of the polygraph process.

The first independent inspection of CBP's polygraph program by NCCA's Quality Assurance Program provided an in-depth look at 118 functional and operational CAD criteria. The inspection team concluded their review with no derogatory findings, and affirmed the strong foundation upon which the CBP polygraph program had been established.

The biennial inspection by NCCA's Quality Assurance Program again identified no derogatory findings of weaknesses or flaws in the CAD polygraph program. To the contrary, three areas of "strength" were identified (two quality control program management areas and polygraph program statistics regarding admission/confession rate). This was an unprecedented finding that established CBP as the leader among the 26 federal agencies with a polygraph capability.

#### **CAD FY 2012 Accomplishments:**

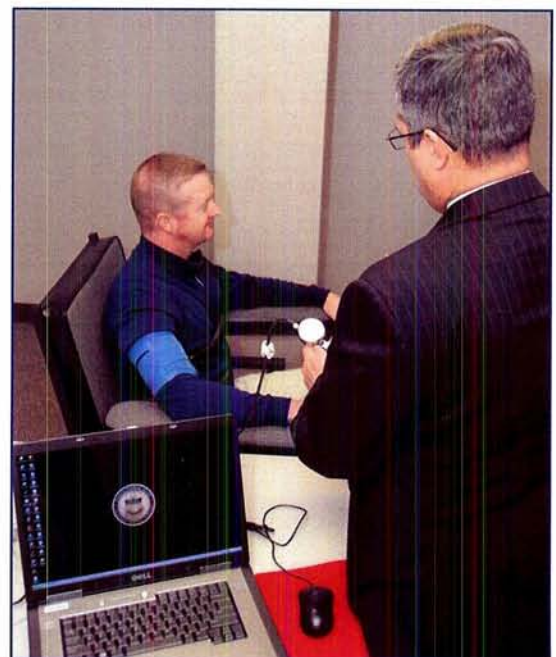
- ✓ Completed 4,828 polygraph examinations; a 54.1% increase compared to FY 11. Of the applicants tested, 1,166 were disqualified based on polygraph examination results prior to the conduct of a background investigation, saving CBP \$3,731,200.
- ✓ Processed more than 73 additional polygraph cases that included CI examinations and specific issue examinations.
- ✓ Conducted its 10,000<sup>th</sup> polygraph examination in May 2012. More than three dozen attempted infiltrations have been thwarted by conducting these examinations.

In March of 2010, CBP leaders, the FBI and the OIG provided compelling congressional testimony regarding the agency's internal integrity concerns. Subsequently, the Anti-Border Corruption Act of 2010 (ABCA), P.L. 111-376, was signed into law by President Obama on January 4, 2011. This legislation contained the unprecedented mandate to conduct pre-employment polygraph screening for all CBP law enforcement applicants by January 2013.

In collaboration with IPD's Behavioral Research Branch, CAD data was used to produce insightful research to objectively gauge the current integrity status of CBP, and provide potential solutions to future integrity issues:

- The **Test v. No-Test Study** compared the rate of the incidents "of record" in JICMS between current employees who had received polygraph examinations before being hired with those who had not. Employees who had not been given a polygraph examination were more than twice as likely to be involved in behaviors "of record" in JICMS than those who had been screened with polygraph.
- The **Ready List Study** consisted of 300 polygraph examinations of applicants who had successfully completed all aspects of the CBP hiring process including the rigorous Single Scope Background Investigation. Again, approximately 60% of the examinees failed to successfully complete the process and provided startling admissions that included undetected felony crimes, serious drug and illegal alien activity, and one attempt to infiltrate CBP on behalf of a drug trafficking organization.

These studies further established CAD as a critical part of the effort to combat corruption and enhance integrity within CBP.



Note: Above pictures posed for illustrative purposes only - not actual examinees.

## Personnel Security Division

The Personnel Security Division (PSD) is responsible for initiating and adjudicating background investigations on all CBP applicants and employees as well as contractors and consultants seeking employment with CBP. PSD renders suitability and security eligibility determinations and grants, denies, and revokes security employment clearances.

The vital work of PSD has enabled the agency to staff its workforce of more than 47,000 front line law enforcement personnel and 18,000 support personnel, making CBP the largest organization in the U.S. Between FY 2008 and FY 2012, more than 128,000 background investigations were conducted as part of the hiring process.

PSD has implemented multiple process and system efficiencies to improve screening. In early 2008, the Personnel Security Division (PSD) required 100% compliance CBP-wide of the use of e-QIP for submission of all CBP background investigation security forms. The e-QIP system enables electronic transmission of security forms and provides an audit system for accountability. This paperless mandate greatly reduced tracking and processing challenges experienced with the former process. PSD also worked closely with OPM to activate the "split-National Agency Check (NAC) function in the e-QIP system. With this enhancement, the entire file, as well as the individual's investigative history, is available in digital form for action throughout the vetting and adjudicative process. CBP was the first investigative agency to actively pursue and receive OPM approval to use this automated tool. Mandatory use of e-QIP and automation of the split-NAC function began in April 2009; both continue to be essential components of the automated BI



process. Finally, PSD worked with the Office of Human Resources, and the Office of Border Patrol (OBP) to exceed the goal of hiring 2,242 OBP employees in support of Border Patrol operations along the Southwest border by August of Fiscal Year 2009.

Today, PSD coordinates the screening of law enforcement applicants with CAD, who performs polygraph examinations prior to the SSBI, saving CBP an estimated \$3.5 million a year in personnel security investigative costs.

### **PSD FY 2012 Accomplishments:**

- ✓ Completed (initiated, investigated, adjudicated) 99% of all backlogged Periodic Reinvestigations (PRs); completing 15,020, including those now "off rolls".
- ✓ Initiated 100% of employee PRs that came due in FY11.
- ✓ Initiated 97% of contractor PRs that came due in FY 11.
- ✓ Initiated 71% of employee PRs that came due in FY12.
- ✓ Initiated 94% of contractor PRs that came due in FY12.
- ✓ PSD is on track to initiate 100% of all FY11/12 PRs by 11/30/12.
- ✓ Instituted a centralized Help Desk using a Remedy Ticket Tracking System, documenting and responding to more than 900 requests for assistance since January 2012.
- ✓ Conducted over 300 overdue international PRs utilizing in-house resources (IOD and PSIU) to conduct investigations at a lower investigative cost.
- ✓ In accordance with the ABCA 2010, initiated 15,197 overdue PRs in e-Qip by December 2010.

## Security Management Division

When the Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) were formed in 2003, many legacy U.S. Customs Service Physical Security Specialists separated from the agency or transferred to the newly-created Immigration and Customs Enforcement. This loss of experienced and knowledgeable physical security personnel, along with the dramatic increase in new agency personnel, facilities, and other high value and sensitive assets, challenged CBP's ability to implement and oversee its physical security programs. In September 2006, the Security Management Division (SMD) was established. Organized into three branches -- the Security Services Branch (SSB), Physical Security Branch (PSB), and the Information Security Branch (ISB) were created to provide guidance for physical, information, industrial, and operations security programs for CBP.



Since that time, SMD has rebuilt CBP's security capacity with a team of security specialists and program analysts who provide CBP with a robust physical, information, and badging security program. This has been aided by the consolidation of security policy and procedures, and creation of component-wide partnerships to enable rapid security issue information sharing. In 2007, SMD

created the Physical Security Operations Branch to provide a range of security services, including site assessments at locations across the country. The Division works with CBP stakeholders to provide basic turn-key security services and detailed site assessments for identifying security non-compliance and vulnerabilities.



SMD's efforts include:

- Onsite involvement in facility pre-construction to ensure that CBP allocates and expends security funds appropriately, while complying with security requirements;
- Physical protection for CBP employees, visitors, information, and assets at the Ronald Reagan Building in Washington, DC as well as other CBP facilities in the National Capital Region (NCR); and
- Badging and credentialing of approximately 60,000 personnel at more than 4,500 sites.

### **SMD FY 2012 Accomplishments:**

- ✓ PIV Cards have been issued to 12,674 employees, including new hires and those with expired cards. As of September 30, 2012, approximately 90% of employees have received a DHS PIV card.
- ✓ Issued new, promotion, and/or updated badges and/or credentials for 77,869 employees.
- ✓ identified 149 badges for destruction;
- ✓ Identified 16,402 credentials for destruction.

## **TESTING AND EVALUATION SECTION**

The Testing and Evaluation Section is comprised of the Management Inspections Division and the Operational Field Testing Division.

### **Management Inspections Division**

Beginning in FY 2008, the Management Inspections Division (MID) revitalized its management inspection programs and refocused its direction on the core mission of supporting CBP leadership through the inspectional process. Significant accomplishments include the reorganization and integration of the Audit Liaison function; enhancements to SIP Validation Inspections, and the development of the Management Assurance Review (MAR) program. These inspections provide CBP leadership with information on the effectiveness and efficiency of operations, programs, offices, managers, and areas of special interest or priority

#### **Self-Inspection Program**

The Self-Inspection Program (SIP) promotes management accountability, compliance with applicable standards and operational requirements, and operational integrity by having CBP managers perform self-assessment



activities annually. MID is responsible for maintaining and implementing a Validation Inspections

Program to evaluate the effective implementation of the program and accuracy of reported self-inspection results. MID annually performs Validation Inspections to assess the implementation of SIP by CBP managers, and through sampling, to verify the accuracy and completeness of self-inspection results reported during annual self-assessments. SIP is an official CBP management control program in support of the Federal Managers' Financial Integrity Act (FMFIA) and Office of Management and Budget (OMB) Circular A-123.

#### **Management Assurance Review**

The Management Assurance Review (MAR) provides a mechanism that allows CBP to monitor the implementation of agency programs, functions, and responsibilities and enhance management's evaluative capacity. The MAR involves quick but thorough assessments of the targeted functions to determine whether the particular office is properly implementing established policies and procedures; complying with federal laws

#### **MID FY 2012 Accomplishments:**

- ✓ Advanced CBP's efforts to identify vulnerabilities by:
  - Supervising and issuing 57 Management Assurance Reviews (MARs) containing 928 recommendations.
  - Issuing 4 Focused Assessment Reports containing 28 recommendations.
- ✓ Strengthened CBP's efforts to provide efficient and effective audit management services by submitting timely and accurate responses to OIG/GAO draft report responses and 60/90 day letters timely at least 90 percent of the time.
- ✓ Directed the Self-Inspection Program (SIP), issuing 82 SIP validations resulting in 32 Validation Inspection Reports on Cycle 2011 containing 148 recommendations to evaluate program implementation.

and regulations; and ensuring the security of funds, property, and other agency resources.

### **Focused Assessments and Follow-Up Reviews**

The Focused Assessment Program, formerly known as the Limited Review Program, was revitalized in FY 2008 to provide comprehensive, objective, and timely assessments of areas deemed critical by CBP leadership. Focused Assessment



reports offer recommendations for changes in policies, procedures, and practices to resolve identified weaknesses and operational vulnerabilities. Follow-up reviews determine whether the conditions identified in previous assessments have been effectively addressed. These assessments are initiated by management request, MAR and SIP results, GAO/OIG audits

and MID employee recommendations.

### **Audit Management and Liaison**

The Audit Management and Liaison program serves as the agency Component Audit Liaison (CAL) to the GAO/OIG providing oversight concerning audits and reviews of CBP programs and operations. The CAL's facilitates meetings between external auditors and CBP personnel, ensures timely responses to auditor requests for documents and



interviews, coordinates CBP responses to audit findings and reports, tracks the status of required corrective actions, provides agency-wide audit training and keeps leadership informed of high-profile audits and reviews.

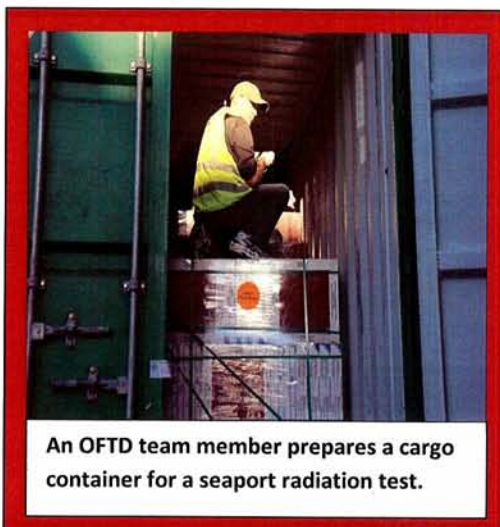
## Operational Field Testing Division

The Operational Field Testing Division (OFTD) was established in response to the Commissioner's mandate to develop a sustainable covert assessment program and to meet the requirements of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) which mandated covert testing of the Nation's 22 busiest seaports. Initially housed within the Management Inspections Division, OFTD became a separate division in 2008. One of OFTD's first challenges was building operational teams comprised of experienced individuals capable of conducting covert testing. The second was developing test protocols. Testing of the Nation's 22 busiest seaports began in 2006 and was completed in August 2008. OFTD released its first comprehensive report on radiation testing, "Summary Report of OFTD Seaport Assessments," in 2009. Testing confirmed that CBP's radiation portal monitors (RPM) were functioning as designed and that officers at seaports were utilizing the RPMs properly.

### **OFTD FY 2012 Accomplishments:**

In order to identify compliance, vulnerabilities and systemic weaknesses in CBP's multilayered security systems, personnel, technologies, policies and procedures, OFTD performed 204 covert tests to include:

- ✓ 20 covert radiation detection tests at 3 unique CBP operational environments (seaport, land border and aviation).
- ✓ 171 document fraud tests in various operating environments including ports of entry, preclearance centers, checkpoints, and bus terminals.
- ✓ Agriculture, Bio-terrorism, Global Entry, Express Consignment Targeting and Secondary Reach comprise the remaining 13 tests.



An OFTD team member prepares a cargo container for a seaport radiation test.

Since the initial launch of seaport testing in 2006, OFTD has aggressively expanded its covert testing program to a wide variety of testing in different operating environments. In 2008, OFTD began testing at land borders. In 2009, OFTD expanded testing to radiation detection at checkpoints. In addition, OFTD began working with the DHS-Domestic Nuclear Detection Office on secondary reachback testing, launched document fraud testing at land borders, and began working with the Office of Intelligence and Investigative Liaison (OIIL) on targeting of passengers. In 2010, OFTD added radiation testing at express consignment facilities and launched document fraud testing at airports. In

2011, OFTD significantly expanded its program to include radiation testing at airports, international general aviation, and a foreign port of entry for CSI; and document fraud testing at bus and rail stations at and between ports of entry. In addition, testing was initiated on bio-terrorism, public health and agriculture. In 2012, OFTD expanded testing to include canine detection of contraband at land borders and airports.

In 2012, OFTD released two reports – Comprehensive Report on Radiation Detection and Comprehensive Report on Document Fraud based on covert testing of the Office of Field Operations. The reports included recommendations to address deficiencies and the development of corrective action plans such as improving inspection techniques and mitigation strategies to address infrastructure and technology limitations. Comprehensive reports on the testing of the Office of Border Patrol are pending.



Test preparation for an International General Aviation test conducted jointly with the FBI.



An OFTD radiation test source being prepared for a land border POE test.



CBP officers escort an OFTD role player to secondary.



## **Evolving CBP Integrity Challenges**

The current and future fiscal state of the federal government, and the complex nature of increased integrity threats, require CBP-IA to develop new and innovative approaches to confront these risks. CBP-IA must fully exploit our analytical capabilities to better understand the evolving integrity threat; verify the efficiency and effectiveness of our existing programs; design advanced processes to prevent, detect, deter; and expand collaborative relationships to better investigate integrity threats.

The existing personnel security process has remained essentially unchanged during the last forty years. During this time, the personal and behavioral characteristics of those aspiring to federal law enforcement positions have substantially changed. There is mounting evidence that traditional background investigations fail to identify significant derogatory information that is relevant to suitability and eligibility determinations. These mandated investigative requirements are both expensive and apparently ineffective. Automated and more accurate reviews of law enforcement data bases; application of elicitation methodologies; further use of psychological testing that includes polygraph; and better focused and relevant personnel security investigations combined with a simplified and expedited adjudication process are required.

The historic rapid expansion of CBP requires CBP-IA to counter the serious insider threat dynamic that places the critical mission of the organization at risk. The authorities, capabilities, and resources to continuously monitor our workforce for anomalies that are indicative of integrity problems must be deployed. The expanded application of polygraph to include the periodic and strategic testing of the existing workforce is warranted. Increasing the number of integrity tests and dispersing Internal Affairs Associates throughout the CBP workforce are also proposed.

The presence of corruption at our nation's borders is a national security threat. When our employees allow bad people and/or bad things to enter our country, they betray the trust and confidence placed in them their fellow Agents/Officers, this organization, and their country. The corrupt employee may think they are allowing an economic migrant to enter the U.S. when that person may be a terrorist intent on harming our citizens. That same corrupt employee may think they are facilitating a vehicle laden with controlled substances to enter the U.S. when the contraband may be the component parts to a dirty bomb. The investigative response to these integrity threats in our CBP workforce must be conducted in manner consistent with the Joint Terrorism Task Forces (JTTFs). The JTTFs provide a fully successful working template to structure the investigative response to border corruption in a framework of cooperation, collaboration, and unrestricted information sharing. The diminishing budgets of all agencies underscore the critical need to share resources and information to achieve the greatest possible effectiveness and efficiency.

As CBP-IA brings these innovations to the updated Comprehensive Integrity Strategy, the vitally important CBP integrity initiatives properly housed in the operational components must be better coordinated with CBP-IA. Inefficient redundancies must be identified and eliminated. It is critically important that a CBP-wide common culture of integrity emerge and be adopted. This shared understanding of the threat, and an acceptance of how to best counter the threat, will allow CBP to remain a high integrity law enforcement organization.