OIG Top Management and Performance Challenges Facing the Department of Justice

November 10, 2015

MEMORANDUM FOR THE ATTORNEY GENERAL
THE DEPUTY ATTORNEY GENERAL

FROM: MICHAEL E. HOROWITZ
INSPECTOR GENERAL

SUBJECT: Top Management and Performance Challenges Facing the Department of Justice

Attached to this memorandum is the Office of the Inspector General's 2015 list of top management and performance challenges facing the Department of Justice (Department), which we have identified based on our oversight work, research, and judgment. We have prepared similar lists since 1998. By statute, this list is required to be included in the Department's Agency Financial Report.

This year's list identifies eight challenges that we believe represent the most pressing concerns for the Department:

- Achieving Balance and Containing Costs in a Significantly Overcrowded Federal Prison System
- Enhancing Cybersecurity in an Era of Increasing Threats
- Building Trust and Improving Police-Community Relationships
- Safeguarding National Security Consistent with Civil Rights and Liberties
- Ensuring Effective Oversight of Law Enforcement Programs
- Promoting Public Confidence by Ensuring Ethical Conduct throughout the Department
- Effectively Implementing Performance-Based Management
- Protecting Taxpayer Funds from Mismanagement and Misuse

We believe addressing the federal prison crisis and cybersecurity threats are particular challenges that will continue to occupy much of the Department's attention and require vigilance in the foreseeable future. In addition, we have identified a new challenge, *Building Trust and Improving Police-Community Relationships*, as an emerging issue where the Department must demonstrate leadership, provide support, and exercise oversight in its capacity as the federal agency charged with enforcing the law. Meeting all of these challenges will require the Department to develop innovative solutions and exercise careful oversight to ensure the effectiveness of its operations.

We hope this document will assist the Department in prioritizing its efforts to improve program performance and enhance its operations. We look forward to continuing to work with the Department to respond to these important issues in the year ahead.

Attachment.

TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE DEPARTMENT OF JUSTICE

Office of the Inspector General

Source: BOP website

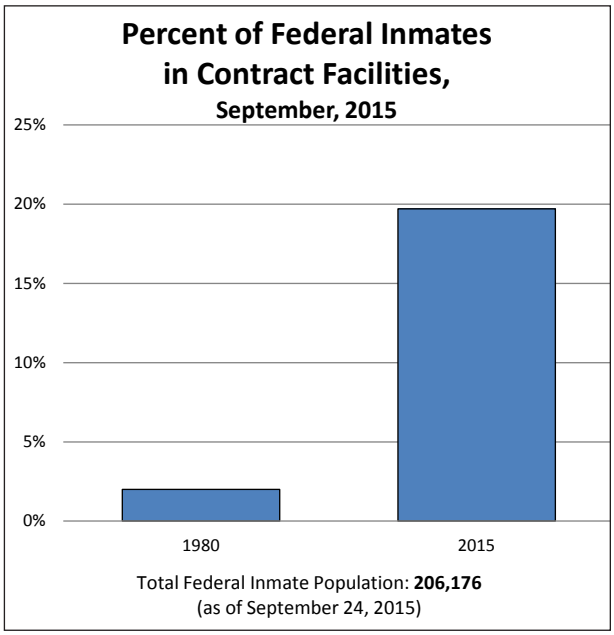
1. Achieving Balance and Containing Costs in a Significantly Overcrowded Federal Prison System

Though the number of federal inmates has declined for a second year in a row, the Department of Justice (Department or DOJ) continues to face a crisis in the federal prison system. Continued high rates of overcrowding both negatively impact the safety and security of staff and inmates and drive costs upward. While the Federal Bureau of Prisons (BOP) must ensure a secure environment and meet the medical and programming needs of its inmates, it must also balance these activities with regard to cost. However, meeting this challenge is complicated by the fact that the BOP exercises little control over the number of inmates it must house. The Department must therefore pursue a comprehensive approach to managing its federal inmate population, in order to find an appropriate balance that addresses the safety of the public, staff, and inmates in the federal prison system while holding costs to manageable levels.

Improving Prison Safety and Security

Ensuring the safety and security of the BOP staff, inmates, and the public is critical. The BOP continues to face dangerous levels of overcrowding at its institutions, which poses threats to both staff and inmates. While the BOP has experienced some reduction in the inmate population in the past 2 years, the fiscal year (FY) 2014 Agency Financial Report has once again identified prison overcrowding as a programmatic material weakness, as it has done in every such report since FY 2006. Moreover, although overall overcrowding decreased from 33 percent in June 2014 to 26 percent in August 2015, overcrowding at high security institutions has actually increased from 42 percent to 51 percent. This presents a particularly significant concern because more than 90 percent of high security inmates have a history of violence, making confinement in such conditions especially problematic. In addition, the BOP has acknowledged that its inmate-to-correctional officer ratio remains undesirably high, and indicated that at times it has had to rely on non-custody staff to assist in covering security posts.

The difficulties in ensuring safe and secure incarceration of federal inmates apply not only to BOP-managed institutions, but also to contract facilities. As of September 2015, nearly 20 percent of federal inmates were housed in contract facilities, an increase from 2 percent of the inmate population in 1980. This total includes approximately 24,000 inmates housed in BOP's 13 privately-managed contract prisons. Although contract prisons may in some cases help to alleviate overcrowding of BOP facilities, contract prisons also can present safety and security risks for staff and inmates. For example, a riot perpetrated by approximately 2,000 inmates at the privately-managed Willacy Correctional Center earlier this year resulted in staff injuries and extensive property damage. Soon afterwards, the BOP cancelled the Willacy contract and transferred its inmates to other facilities. There have been riots at other BOP contract prisons in recent years, including one in 2009 and another in 2012 that resulted in the death of a correctional officer, severe injuries to both staff and inmates, and extensive property damage. The Office of the Inspector General (OIG) is completing a review examining how the BOP monitors its contract prisons and whether contract performance meets inmate safety and security requirements. The OIG will also evaluate how contract prisons and similar BOP institutions compare in an analysis of inmate safety and security data. The BOP and the Department need to ensure that contract facilities provide a safe and secure environment for inmates, staff, and the public, and that they do so in a cost effective manner.



Source: BOP

The use of segregated housing in both contract facilities and BOP institutions raises significant challenges. As mentioned in last year's management challenges report, the BOP underwent an independent assessment of its use of restrictive housing, including both single-inmate and multiple-inmate cells. The assessment, completed in December 2014, resulted in over 20 findings, including concerns regarding the use of restrictive housing for inmates with severe mental illnesses. The report also concluded that the BOP needed to improve its mental health diagnoses, offer more effective treatment, and provide sufficient psychiatric staffing. While the BOP uses restrictive housing primarily to confine dangerous inmates, it must weigh the use of this option, particularly for those with mental illnesses, given the potential negative psychological effects attendant with such types of confinement. The 2014 report recommended moving seriously mentally ill inmates into alternative units to reduce the number of inmates placed in restrictive housing. The OIG is currently conducting an evaluation of the screening, monitoring, and treatment of mentally ill inmates in BOP's restrictive housing units, evaluating costs and mental illness trends across several restrictive housing units. This review should help inform the BOP's efforts in this area, which implicate the difficult task of ensuring the safety and security of the facility while not undermining the mental health and rights of its inmates.

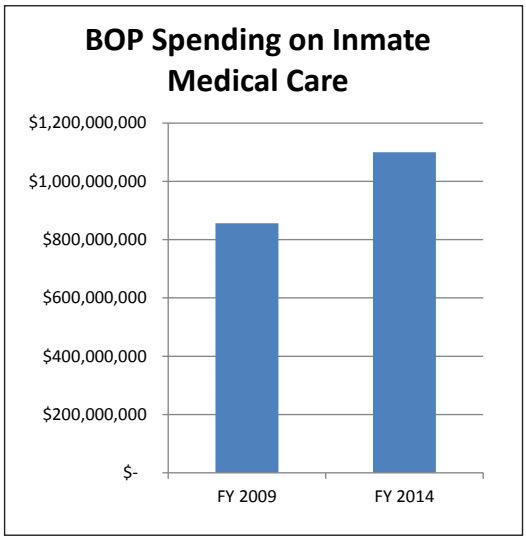
Preventing the introduction of contraband is another challenge to ensuring safety and security in BOP facilities. Cell phones are a particularly dangerous contraband item in a prison because inmates can use the devices to carry out criminal activities – such as coordinating additional contraband smuggling; threatening and intimidating witnesses, victims, and public officials; and orchestrating escape attempts. To help prevent the introduction of contraband, the BOP has introduced various technologies, including piloting in September 2014 the use of Millimeter Wave Scanners for contraband detection at six institutions. Also, in July 2013, over 10 years after a January 2003 OIG report recommended that the BOP implement a staff entrance and search policy, the BOP implemented new staff entrance and search procedures that authorized

random pat searches of staff and their belongings. However, as a result of a recent Federal Labor Relations Authority ruling that concluded, in substance, that staff search policies were not negotiated properly, the BOP rescinded the 2013 search policy and reinstated the prior procedures. The OIG continues to investigate and present for prosecution an ongoing stream of cases involving the introduction of contraband into BOP facilities, and we are engaged in an ongoing review of the BOP's contraband interdiction efforts, to include an evaluation of staff searches as well as physical security measures, including random pat searches and TSA-style body scanners. The results of these cases and our review should be instructive for the BOP as it continues to battle against new and innovative means of introducing dangerous contraband that threaten the safety and security of inmates and staff.

Containing the Cost of the Federal Prison System

While the Department faces the challenge of maintaining safety and security in the federal prison system, it must also look for ways to contain ballooning costs. As the costs to operate and maintain the federal prison system continue to grow, less funding will be available for the Department's other critical law enforcement and national security missions, making effective management of the federal prison system a significant challenge the Department cannot ignore. The BOP currently has the largest budget of any Department component other than the Federal Bureau of Investigation (FBI), accounting for more than 25 percent of the Department's discretionary budget in FY 2015, and employing 34 percent of the Department's staff. The BOP's enacted budget was nearly $7 billion in FY 2015, an 11-percent increase since FY 2009, despite a decline in the federal prison population from 214,149 in FY 2014 to 206,176 in FY 2015 – its lowest level in 6 years. Further, the BOP has requested an additional 6-percent increase for next year, despite projecting that its population will decrease by an additional 12,000 inmates.

The Department must isolate the chief drivers of these uncontrolled costs and consider innovative solutions that might help to contain them. As mentioned in last year's management challenges report, inmate medical costs are a major factor in BOP's overall rising costs and thus an area that must be monitored closely. In FY 2014, the BOP spent $1.1 billion on inmate medical care, an increase of almost 30 percent in 5 years. One factor that has significantly contributed to the increase in medical costs is the sustained growth of an aging inmate population – a 2015 OIG report found that the oldest BOP inmates cost an average of $30,609 each or 65 percent more than the youngest ones. As a result, we recommended revising the requirements that limit the availability of compassionate release for aging inmates. One consequence of the increase in the aging inmate population is BOP's increased need for inpatient treatment beds, which has grown by 67 percent since 2003. In addition, the BOP is spending significantly more to meet the needs of aging inmates with serious diseases.



Source: BOP

The Department must also assess the cost-effectiveness of the BOP's increasing reliance upon contract services to provide more facility space and supplement medical care. The BOP contracts with 13 prisons owned by either county governments or private prison companies to confine inmates who are primarily low security, foreign nationals with less than 90 months remaining in their sentences. In the past 5 years, spending for contract prisons increased by more than 30 percent, to $639 million in FY 2014. The BOP needs to remain vigilant in assessing the cost effectiveness of procuring contract services, particularly in light of reforms to reduce its overall inmate population. As the OIG's 2015 audit of the Reeves County,

Texas contract prison showed, the Department must conduct careful oversight of these contracts. In auditing that contract alone, we found nearly $3 million in questioned costs. Our work has also found that the BOP struggles to meet the medical needs of its inmates with its own staff and must use contracts to supplement the medical care it provides. According to BOP data, spending for inmate medical services provided by contract providers increased 27 percent from $258 million in FY 2010 to $327 million in FY 2014. The OIG is currently examining factors that contribute to BOP's medical staffing challenges as well as the financial impact of using contract medical care. We believe that this analysis should help the BOP identify ways to address this pressing issue.

Properly Evaluating Other Department Programs and Policies Can Better Address the Prison Crisis

The challenges to the federal prison system cannot be corrected by the BOP alone, as it has only limited control over the number of inmates it is charged with safely housing. Instead, multiple Department-level efforts must come together if there is any hope of seriously addressing these safety, security, and cost concerns. To address these and other challenges, the Department launched the Smart on Crime initiative in August 2013, with the goal of reforming the federal criminal justice system by curbing reliance on incarceration for less dangerous offenders. The initiative proposes taking a comprehensive approach to the criminal justice process by focusing on five key goals: (1) prioritize prosecutions to focus on the most serious cases; (2) reform sentencing to eliminate unfair disparities and reduce overburdened prisons; (3) pursue alternatives to incarceration for low-level, non-violent crimes; (4) improve reentry to curb repeat offenses and re-victimization; and (5) provide "surge" resources to aid violence prevention and protect the most vulnerable populations. Proposed reforms include requiring districts to modify their guidelines for when federal prosecutions should be brought, limiting the use of mandatory minimums and enhancements for repeat offenders for low-level, non-violent drug defendants, and enhancing prevention and reentry efforts at each U.S. Attorney's office.

The Smart on Crime initiative also aims to explore cost-effective reforms to the federal prison system that will allow law enforcement to redirect scarce federal resources toward violence prevention. For example, a 2014 Government Accountability Office (GAO) report estimated that 370,985 beds and $4.1 billion could be saved in the next several years through retroactively reducing prison sentences for inmates currently incarcerated for certain drug offenses. The GAO found that other options, such as not bringing charges that carry mandatory minimum sentences in cases involving low-level, non-violent drug offenders, would have less of an impact, but still could provide relief for the federal prison system as well as redirect resources to crime prevention.

As an outgrowth of the Smart on Crime initiative, the Department established its new clemency initiative in April 2014. Under this initiative, the Department indicated that it will prioritize clemency applications for non-violent, low-level inmates who petition to have their sentences commuted or reduced by the President. In addition, as part of Smart on Crime, the Department has announced its intention to expand the use of pre-trial diversion and drug court programs to provide alternatives to incarceration and reduce recidivism. These two alternatives enable prosecutors, judges, and probation officers to divert certain offenders from traditional criminal justice proceedings into programs designed to address the underlying causes for criminal behavior or otherwise provide appropriate sanctions and remedies without the need in many cases for incarceration or even criminal convictions. The OIG is currently evaluating the use of these programs within the various U.S. Attorneys' Offices.

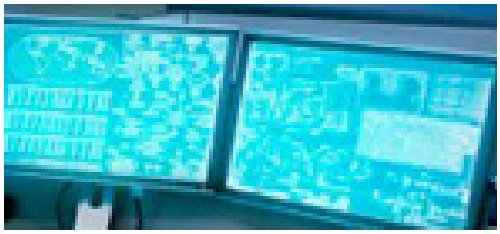
We have found that the Department could better utilize other programs and policies related to the goals of the Smart on Crime initiative. In August 2013, as part of the Smart on Crime efforts, the BOP expanded its Compassionate Release Program. This change allowed inmates age 65 and older to request a reduction in

sentence if they meet certain criteria. However, our subsequent report on the BOP's aging inmate population found that during the first year after the new BOP policy was implemented, only 2 of the 348 inmates who applied were released under the new provisions. The OIG found that the Department imposed several restrictive requirements, including a rule that inmates requesting a non-medical compassionate release must have already served 10 years and 75 percent of their sentences to be eligible for compassionate release. By excluding inmates with sentences of less than 10 years, this change significantly reduced the number of inmates who could apply and, as a consequence, excluded many who committed lesser, non-violent offenses. Similarly, in an August 2015 follow-up report on the Department's international treaty transfer program, the OIG found that the number of inmates transferred under the program had actually decreased, despite a substantial increase in both awareness of the program and the number of inmates applying for such transfers. The OIG's follow-up report recommended that Department leadership boost the effectiveness of this program by actively engaging with treaty transfer partners, including the Department of State and foreign government representatives.

Among the more difficult challenges that the Department faces is adequately measuring whether these various initiatives will ultimately meet its goal of reducing the prison population and containing costs. In many reports we have found that the Department needs better recordkeeping to be able to evaluate and direct its efforts. This was confirmed in a 2015 GAO report, which recommended that the Department modify its 16 Smart on Crime indicators to better track whether the program was having much success. In fact, the last BOP study on the overall recidivism rate for federal inmates occurred more than 20 years ago, which is concerning given the BOP spends hundreds of millions of dollars annually on reentry programs and residential reentry centers to improve rehabilitation efforts. As we describe more fully below, the Department must develop the capability to accurately assess its initiatives and programs in order to properly measure their outcomes and efficacy, and that is particularly true given the limited resources available to conduct law enforcement and incarceration efforts within the Department.

In sum, a multi-faceted approach is necessary to address the persistent crisis in the federal prison system. The Department has taken several steps by pursuing programs and policies including its Smart on Crime initiative. Yet, the Department needs to collect the correct information to continuously evaluate whether these initiatives are reaching their goals, and put in place policies and practices designed to achieve them. The BOP must also continue to work collaboratively with other Department components to develop better methods to fully utilize its own programs, prevent the introduction of contraband, provide effective management of contract services, and address staffing and other challenges to the safety and security of its facilities.

2. Enhancing Cybersecurity in an Era of Increasing Threats



Source: FBI website

The Department, working closely with its private sector, law enforcement, and global partners, must be persistent and innovative in defending the nation's cyber resources from intrusions and attacks. In September 2015, Director of National Intelligence James Clapper testified that cyber threats pose one of the gravest national security risks to the United States. Further, a September 2015 GAO report concluded that federal agencies' information and systems remain at a high risk of unauthorized access, use, disclosure, modification, and disruption, while also noting an increasing number of cyber incidents and breaches of personal information at federal agencies. As recent events have shown, increasingly sophisticated attacks can result in significant releases of information and potential damage to national security. The breaches of Office of Personnel Management (OPM) data compromised the personal

information of more than 22 million people, and resulted in the disclosure of fingerprints and other highly sensitive data from background investigations of more than 5.6 million current, former, and prospective federal employees and contractors. That, combined with reported cyberattacks on other government agencies, clearly demonstrates that the federal government is vulnerable. The danger to private industry and American citizens is equally clear and present: private and public organizations as well as individual citizens continue to be victimized by cyberattacks. For example, earlier this year, a publicly reported cyberattack on health insurer Anthem Inc., exposed private data, including names and Social Security numbers, of nearly 80 million people. Other reported attacks on Target, Bank of America, and Sony, among others, are all too regular reminders of the critical need to better shield our nation's Information Technology resources.

Source: DOJ OIG

Among the greatest challenges the Department faces in this area is that malicious actors are increasingly relying on encryption and other technological advances to remain elusive and thwart the government's efforts to isolate and mitigate cyber threats. FBI Director James Comey recently warned in testimony before the Senate Judiciary Committee that advances in encryption technology are allowing our adversaries to "go dark." The growing use of single-key encryption on smartphones and other devices restricts access and prevents communications providers from providing law enforcement with stored data, even if they obtain a court order. As it looks for ways to combat cybercrime and intrusions despite encryption technologies, the Department needs to find ways to assure citizens it will not violate their privacy rights – underscoring the inherent tension between cybersecurity, civil liberties, and national security. While strong encryption protects the right of Americans to communicate in private, free of government surveillance, allowing device users sole control over their data greatly limits law enforcement's ability to find and retrieve significant evidence that may reside on a smartphone, a tablet, or a laptop. This, in turn, has the potential to leave crime and national security threats undetected. The government must work with private industry to shape an encryption policy that strives to ensure that privacy and security can co-exist.

As it devotes increased attention, resources, and personnel to its cybersecurity efforts, the Department needs to maximize their impact by developing and implementing a cohesive strategy to tackle this problem. In its FY 2016 budget, the Department requested an additional $26.8 million to confront computer intrusions and cybercrimes and protect the Department's information networks from both internal and external threats. In May 2015, Assistant Attorney General Leslie Caldwell announced the creation of a new Cybersecurity Unit within the Criminal Division's Computer Crime and Intellectual Property Section. This unit is charged with assisting other government agencies and the private sector to develop and implement their cybersecurity plans consistent with federal law. This is in addition to the National Cyber Investigative Joint Task Force, run by the FBI under a presidential directive that makes the Department the focal point for coordinating, integrating, and sharing information on cyber threat investigations across 19 U.S. agencies and foreign partners. In October 2012, the FBI also launched its Next Generation Cyber Initiative (NextGen) and has requested nearly $500 million for NextGen and its growing capabilities for the upcoming fiscal year. The goals of this initiative include improving cyber skills for agency personnel and strengthening public and private partnerships. The initiative has narrowed the focus of the FBI's Cyber Division to work solely on cyber intrusions that pose the greatest threat to national security and on being proactive in preventing future attacks.

But even as it works to expand the ranks of its cybersecurity team, the Department continues to face challenges recruiting and retaining highly-qualified candidates to do this work, as detailed in our July 2015 audit of NextGen. We found that the FBI failed to hire 52 of the 134 computer scientists that it was authorized to hire, and that 5 of the 56 field offices did not have a computer scientist assigned to that office's

Cyber Task Force. Among other hiring challenges the audit identified were that the FBI's background investigations are more onerous than those used by many private sector employers, and it was difficult to retain top talent because private sector entities often pay higher salaries. Addressing these systemic challenges will be difficult, but it will be essential if the FBI and the Department are to play the leading role in combating this threat.

Building closer relationships with the private sector, state and local law enforcement, and global partners is another way the Department can work toward its cybersecurity goals. Despite the Department's emphasis in its FY 2014-2018 Strategic Plan on establishing successful relationships with other law enforcement agencies and developing strong private-public partnerships, it continues to face challenges partnering and sharing information about cyber matters with private sector entities, in part because of privacy concerns and a general distrust of government. Our July 2015 NextGen audit found that few state and local law enforcement agencies are motivated to join their local Cyber Task Force for a variety of reasons that must be addressed by the FBI in order to foster greater participation. The audit also found that although the FBI is working to develop strategies to enhance outreach to private sector entities, it continues to face challenges partnering and sharing information with these entities. The OIG is currently reviewing the FBI's strategy to mitigate cyber threats through an approach for identifying the perpetrators and their tradecraft, intent, capabilities, and affiliation. Those findings should help to further inform the Department's efforts in this critical area.

Given that those posing cyber threats know no boundaries, the Department has recognized the importance of working closely with other countries to boost cybersecurity. In September 2015, Attorney General Loretta Lynch announced that combating cybercrime was one of her top priorities and pledged that the Department was prepared to play a global leadership role in this effort. In remarks at Europol, in the Hague, the Attorney General highlighted Department efforts to improve global cooperation by (a) establishing permanent Cyber Assistant Legal Attaché positions in London, Ottawa, and Canberra, and adding five new temporary positions; (b) hiring 38 additional attorneys and 26 professional staff to the Office of International Affairs Mutual Legal Assistance Treaty Modernization project, with the goal of facilitating the transfer of information regarding international cyber issues; and (c) temporarily assigning a U.S. prosecutor to sit at Eurojust, the European Union's Judicial Cooperation Unit, and work with Europol's European Cybercrime Centre. The Attorney General also announced that the United States and the European Union had initiated the "Umbrella" Data Privacy and Protection Agreement, designed to enhance the ability of law enforcement and prosecutorial agencies on both sides of the Atlantic to combat crime and terrorism while protecting personal privacy. These are positive steps, but the Department must continue to push forward to develop and expand effective partnerships with private entities and state, local, and foreign governments, as they are all critically necessary partners in the Department's cybersecurity efforts.

While looking outward, the Department cannot lose sight of the critical need to make sure its own cyber defenses are robust. Following the OPM breach, the Office of Management and Budget (OMB) directed agencies to patch critical vulnerabilities, review and tightly limit the number of privileged users with access to authorized systems, and dramatically accelerate the use of strong authentication, especially for such privileged users. Following OMB's directive, the White House reported that federal civilian agencies increased their use of strong authentication (such as smartcards) for privileged and unprivileged users from 42 percent to 72 percent. The Justice Department, however, had among the worst overall compliance records for the percentage of employees using smartcards during the third quarter of FY 2015 – though it has since made significant improvements, increasing to 64 percent of privileged and unprivileged users in compliance by the fourth quarter. Given both the very sensitive nature of the information that it controls, and its role at the forefront of the effort to combat cyber threats, the Department must continue to make progress to be a leader in these critical areas.

The Department must also ensure that recommendations to address the security and operations of its systems are promptly implemented. Pursuant to the Federal Information Security Modernization Act of 2002 (FISMA), each Inspector General performs an annual independent evaluation of the agency's information security programs and practices. For FY 2014, the OIG provided 56 recommendations on five Department components' information security programs which included one classified, and five unclassified systems. For FY 2015, the OIG also reviewed the security programs of five Department components, which included two classified systems, and four sensitive but unclassified systems. We plan to complete reports evaluating each of these systems as well as reports on each Department component's information security program. Meanwhile, OMB has worked with the Chief Information Officers Council and the Council of the Inspectors General on Integrity and Efficiency to improve the reporting process and clarify FISMA reporting guidance for the inspector general community. We support the FISMA reform effort and believe it will help us provide more meaningful guidance to the Department on how it can be better prepared to prevent intrusions.

In an era of ever-increasing cyber threats, the Department will be challenged to sustain a focused, well-coordinated, and robust cybersecurity approach for the foreseeable future. The Department must continue to emphasize protection of its own data and computer systems, while marshalling the necessary resources to lead the effort to combat cybercrime, identify and investigate perpetrators, and engage the private sector and its state, local, and global partners in this crucial effort.

3. Building Trust and Improving Police-Community Relationships

Source: OJP website

Among the most pressing challenges facing the Department is determining how it can most effectively assist in the vital task of mending the apparent growing divide between some of the nation's communities and their police departments. The recent riots in Ferguson and Baltimore following the deaths of unarmed African-Americans during encounters with police – as well as several attacks resulting in the deaths of law enforcement officers in Houston and Brooklyn – highlight the tension and the potential erosion of trust between law enforcement officers and the people they serve in certain communities across the country. This tension and a resulting lack of trust has the potential to negatively impact the ability of law enforcement to function effectively, thereby affecting the safety of those communities, and possibly trigger other undesirable collateral consequences, including the loss of police morale that could further endanger public safety. As Attorney General Lynch recognized in remarks earlier this year, the country has seen "too frequently how relationships between communities and law enforcement can grow strained; how trust can be broken or lost; and how simmering tensions can erupt into unrest." In order to provide leadership fighting crime, the Department must be able to rely on strong partnerships with state and local police departments. Only then can it gather street-level intelligence and benefit from the assistance of those officers closest to emerging threats. But if communities lose trust and confidence in their local police, or the police lose trust and confidence in local leaders, that will inevitably impact the ability of federal agents and prosecutors to join with local law enforcement to protect the citizenry. Further, if police experience lower morale due to a lack of support – perceived or otherwise – and deteriorating relationships with citizens in their communities, they may fear retribution or otherwise be less likely to aggressively fight crime. Recognizing this, Attorney General Lynch toured the nation earlier this year stressing that "restoring trust where it has eroded," while fostering relationships between police and the communities they serve, is one of her top priorities as Attorney General. The Attorney General also has emphasized the critical role police officers play in ensuring public safety and stressed they merit the Department's full support.

As the federal agency charged with enforcing the law, the Department can play a leadership role through cooperative law enforcement operations, grant funding of state and local efforts, knowledge and information sharing, and framing national discourse – not only with its own federal law enforcement components, the FBI, the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and the U.S. Marshals Service (USMS), but also with state and local police. These partnerships will, in turn, help the Department be a more effective leader in protecting Americans from both domestic and international threats, thereby creating and maintaining safer communities across the country.

The Department's task then is to determine how best to assist in solving a problem that is largely local in nature, when it has limited resources to share, limited jurisdiction upon which to act, and limited control over most aspects of crime fighting. We believe there are at least four areas where the Department can play a critical role: (a) providing leadership in improving the national dialogue between law enforcement and their communities; (b) offering and coordinating federal grants and guidance to local police departments to fund equipment, training, and reforms; (c) monitoring and assisting with the reform of police departments that are found to have engaged in a pattern or practice of unlawful misconduct, to include violating their citizens' civil rights; and (d) investigating and prosecuting law enforcement officers, whether local, state, or federal, who violate federal civil rights laws.

Source: DOJ OIG

In its leadership role, the Department must find ways to use the tools it has to help guide and oversee changes needed at the community level. Shortly after the events and protests in Ferguson, the Department launched a national initiative to build trust between law enforcement and local communities. Through a 3-year $4.75 million grant, the National Initiative for Building Community Trust and Justice, launched in September 2014, the Department designed "a new approach to training, policy development, and research geared toward advancing procedural justice, promoting racial reconciliation, and eliminating implicit bias." The Attorney General has pointed out that an increased effort in leadership and police-community partnerships led to a collaboration that has "transformed" certain cities. Additionally, the President signed Executive Order 13684 to establish the Task Force on 21st Century Policing to focus on improving policing practices. The task force recommended further research and suggested action items for law enforcement agencies, stakeholders, and the Department. Among its recommendations were that law enforcement agencies establish a culture of transparency and public trust by creating a more diverse workforce and making all department policies available to the public. These initiatives suggest a path the Department can follow to lead a national dialogue to develop and promote proactive solutions in this area.

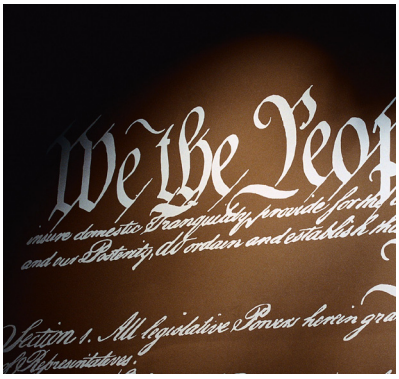
Another of the Department's challenges is to use available resources to foster partnerships with state and local law enforcement agencies in order to support law enforcement and oversee improvement at the community level. DOJ components such as the Office of Justice Programs (OJP) and the Office of Community Oriented Policing Services (COPS) provide federal leadership and coordination in developing the nation's capacity to prevent and control crime, administer justice, and advance public safety through community policing. These grant-making components can direct funding for training, equipment, and support to law enforcement entities across the country in furtherance of Department goals. The Department recently announced grant funding for its Smart Policing Initiative, with the goal of helping local law enforcement agencies reduce crime and earn the confidence of the citizens they serve. In September 2014 COPS also announced $124 million in awards to fund 950 community policing officers at 215 law enforcement agencies across the country. COPS subsequently released a resource guide for police

agencies highlighting training, leadership, and initiatives available for local communities. In addition, in May 2015, the Department announced a $20 million Body-Worn Camera Pilot program administered by OJP and designed to fund such programs in 73 local and tribal agencies across the country. The program's goals are to improve safety, reduce crime, and build community trust through the purchase of body-worn cameras, training and technical support to the recipient agencies, and identification of best practices.

Along these lines, to help evaluate what steps the Department can take to help reduce violence in local communities, the OIG has begun a review of the Department's violent crime initiatives. This review will evaluate the Department's strategic planning and accountability measures in combating violent crime, including coordination across Department prosecution, law enforcement, and grant-making components.

But as the Department wrestles with where and how it should invest to achieve the greatest impact with grants to local police departments, a major impediment is that it lacks complete and accurate data on issues driving the circumstances facing local law enforcement. In February 2015, FBI Director Comey stated that "the first step to understanding what is really going on in our communities and in our country is to gather more and better data related to those we arrest, those we confront for breaking the law and jeopardizing public safety, and those who confront us." Currently, complete figures on the number of "justifiable homicides" are unavailable because law enforcement agencies only voluntarily report this data. The FBI cannot completely track data on the number of incidents in which force is used by or against police officers. Without complete and accurate data, the Department and the American people do not have a complete picture of the nature of the problem, which undermines the potential effectiveness of any steps developed to address it. The Department has taken some early steps to help address this issue. In October 2015, the Attorney General announced that the FBI and the Bureau of Justice Statistics, in collaboration with major policing organizations, are working to expand and standardize relevant data collection. Going forward, the Department must improve the collection and analysis of data from local law enforcement agencies to determine the true nature of violent crime, "use of force," and officer-involved shootings.

In addition to providing supportive resources to police departments, the Department, through its Civil Rights Division (CRT), plays a critical role in ensuring that police departments use their powers consistent with the Constitution. CRT has investigated law enforcement agencies nationwide to address allegations of excessive force; unlawful stops, searches, or arrests; and discriminatory policing. Through these "pattern and practice" investigations, CRT endeavors to create models for effective and constitutional policing nationwide. The reforms sought by CRT at the departments it investigates can provide significant, systemic relief; increase community confidence in law enforcement; and improve officer and agency accountability. For example, after a CRT investigation showed that officers regularly used excessive force against Latinos in East Haven, Connecticut, city officials took steps to improve police-community relations. Among the reforms they adopted were requiring all officers to wear body cameras, holding regular community meetings, having school-based officers check on children, and creating a citizens' police academy. The Attorney General singled out the city's efforts as a model for improving relations between police and the community.



Source: DOJ

In the past 6 years, according to the Department, CRT has opened "pattern and practice" investigations in 22 police departments across the country. CRT and U.S. Attorneys' Offices also criminally prosecute law enforcement officers across the country for violating individuals' civil rights. Ultimately, civil rights investigations of police departments and criminal prosecutions of police officers are only two tools to help build trust in local law enforcement, and the Department needs to evaluate what methods will be most effective in helping the nation address the larger issues at stake.

The Department must work through these critical issues to determine how to best use its limited but substantial resources to help foster partnerships, support law enforcement efforts across the country, and ensure confidence in community-police relations. Effective policing at the state and local level contributes significantly to the success of law enforcement efforts at the federal level. By dedicating resources for funding, oversight, and leadership, the Department can strengthen relationships among federal, state, and local agencies and benefit from the collective knowledge obtained at all levels of law enforcement in order to combat crime and address emerging threats.

4. Safeguarding National Security Consistent with Civil Rights and Liberties

Source: DOJ OIG

Terrorism continues to pose a fundamental threat to the national security of the United States, along with jeopardizing the peace and safety of individuals throughout the world. Protecting U.S. citizens against acts of terrorism is a top priority in the Department's FY 2014-2018 Strategic Plan, and must continue to be a central focus. FBI Director Comey stated that "the threats posed by foreign fighters, including those recruited from the United States, traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists…remain the biggest priorities and challenges for the FBI, the U.S. Intelligence Community, and our foreign, state, and local partners." Recent acts perpetrated abroad by ISIL and al-Qaeda affiliates, as well as domestic acts perpetrated by homegrown violent extremists in Texas and Tennessee earlier this year, demonstrate all too well the need for the Department and its components to remain on guard to try to disrupt this persistent threat.

The Department's proposed FY 2016 budget allocates $4.4 billion to national security efforts to counter both international and domestic terrorism, improve information sharing and collaboration within the Intelligence Community, counter violent extremism and domestic radicalization, and enhance cybersecurity. Additionally, the ongoing discussions over the government's surveillance efforts and the passage of what is commonly referred to as the USA FREEDOM Act of 2015 have drawn significant additional attention to the challenge of operating critical national security programs consistent with the public's expectation of privacy. In light of the potential magnitude and serious nature of the threats posed to the public, it is particularly important for the Department to act effectively and aggressively while ensuring that the civil rights and civil liberties of American citizens are protected.

The Department continues to focus much of its efforts on fighting international terrorism. In a June 2015 hearing before the House Homeland Security Committee, the FBI stated that one of the highest priorities for the FBI and the Intelligence Community is to stop homegrown violent extremists, who may be inspired by foreign terrorist ideologies to attack the United States from within. Yet domestic terrorist attacks by individuals motivated by U.S.-based extremist ideologies also remain a serious threat. In response to the threat of domestic terrorism, in 2014 then-Attorney General Eric Holder re-established the Domestic Terrorism Executive Committee to assess and share information about ongoing domestic terror threats. In October 2015, the Department announced the appointment of a new Domestic Terrorism Counsel to serve as the main point of contact for U.S. Attorneys working on domestic terrorism matters. The Department's FY 2016 budget request also includes $15 million to implement the Countering Violent Extremism Initiative

to address both types of threats to the homeland. It is important that the Department continue to develop and work on these and other initiatives to identify and disrupt potential acts of terrorism – a priority that is particularly crucial in light of a March 2015 report by the 9/11 Commission that found limited resources and inconsistent implementation of the FBI's programs to counter violent extremism.

Another challenge for the Department is to prioritize the appropriate sharing of national security information among its components and the Intelligence Community so that responsible officials have the necessary information to act in a timely manner against terrorist threats. Department leadership has publicly agreed and, in its FY 2016 budget request, included additional resources to enhance collaboration with the intelligence community through improved information technology infrastructure and counterintelligence programs. Our ongoing joint review with the Inspectors General of the Intelligence Community and Department of Homeland Security involves oversight of some of these efforts. This joint review is designed to determine whether counterterrorism information is adequately and appropriately shared with all participating agencies, and identify any gaps or duplication of effort in this area.

As the Department continues its important work to protect Americans from national security threats at home and abroad, it must be sure not to impair the civil liberties of those it is protecting. Earlier this year, Congress passed the USA FREEDOM Act, which, among other things, altered the government's authority to conduct electronic surveillance and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes. The Department must continually strive to achieve the appropriate balance between its national security efforts and respect for the privacy interests of American citizens, a topic the OIG has focused on in some of our national security oversight work. As required by the USA FREEDOM Act, the OIG currently is reviewing the FBI's use of Section 215 orders under the Foreign Intelligence Surveillance Act (FISA) between 2012 and 2014. This review is examining, among other things, the effectiveness of Section 215 as an investigative tool and the FBI's compliance with the final standard minimization procedures adopted by the Attorney General in March 2013 for handling non-publicly available information concerning U.S. persons that is produced in response to Section 215 orders. Previous OIG reviews of the FBI's use of Section 215 orders found that the interim minimization procedures that had been adopted by the FBI in September 2006 did not provide specific enough guidance to agents for the handling of non-publicly available U.S. person information. As a result, the FBI and the Department did not meet the requirements of the statute requiring the Department adopt minimization procedures. However, we found that by 2013 the Department had adopted final minimization procedures for Section 215 materials. The OIG also is reviewing the FBI's use of information derived from the National Security Agency's (NSA) collection of telephony metadata obtained from certain telecommunications service providers under Section 215. This review will examine the FBI's procedures for retaining, analyzing, and disseminating leads the NSA develops from the metadata, and any changes that have been made to these procedures over time. The review also will examine how FBI field offices respond to leads, the scope and type of information field offices collect as a result of any investigative activity based on those leads, and the role those leads have had in FBI counterterrorism efforts.


Source: DOJ OIG

The Department's use of other investigative tools to enhance its national security efforts, particularly those involving broad data collection, also requires close monitoring due to the risk of gathering data that is outside that allowed by federal law. In January 2015, a partially declassified version of our September 2012 report on the FBI's use of Section 702 of the FISA Amendments Act was publicly released in response to

Freedom of Information Act (FOIA) litigation. Section 702 authorizes the targeting of non-U.S. persons reasonably believed to be located outside the United States for the purpose of acquiring foreign intelligence information. In this report, the OIG reviewed (a) the number of disseminated FBI intelligence reports containing a reference to a U.S. person, (b) the number of U.S. person identities subsequently disseminated, (c) the number of targets later determined to be located in the United States, (d) whether communications of such targets were reviewed, and (e) whether the FBI complied with the targeting and minimization procedures required under the Act. Our report highlighted the challenges inherent in balancing national security interests with civil rights and liberties. In our ongoing work, we continue to evaluate whether the Department is meeting this challenge.

As it employs a variety of strategies to protect the American people from terrorist threats, the Department has the responsibility to ensure that it uses its national security powers both effectively and appropriately, and protects the American people from improper infringements on their civil liberties. The recent public debate over the government's collection of telephony metadata in bulk, as well as the passage of the USA FREEDOM Act to curtail such collection activities, underscores the challenge the Department faces in this area. It must resolve the tension that can exist between national security and civil liberties, striking a balance that will allow the Department to act both forcefully and lawfully in an area where the stakes could not be higher.

5. Ensuring Effective Oversight of Law Enforcement Programs

Source: OJP website

Careful and responsible management of federal law enforcement programs presents a unique challenge to the Department, both domestically and internationally. Many of these programs are not subject to significant public scrutiny, which only heightens the need for effective internal oversight.

One of the Department's constant challenges is balancing the potential risks inherent in its investigative strategies with its law enforcement mission to protect public safety. Perhaps the best recent example of where these two goals can collide was highlighted in our 2012 Fast and Furious report. In it, we found that ATF failed to exercise sufficient oversight of sensitive activities involving firearms trafficking that posed a danger to the public and presented other risks. In response to our review, ATF established a Monitored Case Program to provide greater oversight and coordination of sensitive investigations. We are currently conducting a follow-up review to evaluate the measures the Department and ATF have taken since our 2012 report, including the Monitored Case Program. We are also evaluating the effectiveness of that program in a separate review of several ATF storefront undercover operations that continued or began after the inception of the Monitored Case Program.

Another example where the Department must balance its law enforcement efforts with public safety is in its administration of the Federal Witness Security (WITSEC) Program. The program must ensure the security of witnesses who may be critical to federal prosecutions without unduly increasing threats to the public. Our March 2015 audit on the handling of sex offenders in the WITSEC Program found that the Department had not used adequate safeguards to protect and notify appropriate law enforcement agencies about the risks posed by these participants. The audit also identified a loophole in the program that left law enforcement

agencies uninformed about certain participants who subsequently left the program. In a May 2013 report, we found that Department components responsible for administering the WITSEC program did not inform the Terrorist Screening Center of new identities provided to known or suspected terrorists in the program, and thus their new, government-provided names were not included on the terrorist watchlist. We currently are conducting a follow-up audit to assess whether this problem continues and determine if the Department has appropriate procedures in place to mitigate the risk to the public.

Monitoring the use of confidential informants poses a similar challenge for the Department's law enforcement components. While agents rely on their sources to provide valuable information, they also need to make sure the sources do not take advantage of their status and break the law. The level of secrecy necessary for confidential source programs to be successful adds to the difficulty of closely monitoring their use. As a result, the need for components to follow uniform guidelines is essential if Department leaders are to be assured the programs are working as designed. But in our July 2015 audit of the DEA's Confidential Source Program, we found that the DEA's policies did not align with Attorney General Guidelines for reviewing, approving, and revoking a confidential source's authorization to conduct "otherwise illegal activity" as part of their cooperation with the government. Moreover, we found instances where sources actually were provided Federal Employees' Compensation Act benefits without appropriate processes in place for reviewing the claims and determining eligibility. We are continuing our examination of the DEA's Confidential Source Program, and are also conducting a review of ATF's management of its policies and practices for the identification and approval of confidential informants and its overall oversight of its confidential source program, in order to determine whether these sensitive law enforcement programs are operated appropriately.

Recent tragic events further emphasize the crucial need for effective oversight of law enforcement programs, particularly those that can help curb violent crimes. FBI Director Comey stated after the June 17, 2015, fatal shootings of nine parishioners in a Charleston church that the alleged killer "should not have been able to legally buy that gun that day." This event brought attention to potential shortcomings in the processes in place for the National Instant Criminal Background Check System (NICS) – which is administered in part by the FBI and provides criminal background checks in support of the Brady Handgun Violence Prevention Act of 1993. The Department must do everything it can to ensure that the background check process works effectively and protects the public's interests. We are currently auditing NICS to evaluate its effectiveness – among other issues, this audit will focus on how the FBI refers NICS purchase denials to ATF, ATF's review of those referrals, and whether prosecutions result from this process.

With agents and attorneys stationed in more than 140 countries, the Department also must have effective mechanisms in place to carefully oversee law enforcement personnel working abroad. Our work has shown the problems that result when Department employees do a poor job of representing their agency and their nation overseas. In January 2015, the OIG completed a review of policies and training governing the off-duty conduct of Department employees working in foreign countries. We found that the Department had not revisited off-duty policies or training in any comprehensive manner since 1996, even though the need for revision had been recognized. We also found that policies and training did not clearly communicate what employees could and could not do while off duty. In response to our report, in October 2015, the Department issued new policies and guidelines governing off-duty conduct and ethics to address the issues we identified as needing attention.

Source: DOJ OIG

Carrying out dangerous law enforcement missions overseas also presents complex challenges for both agents on the ground and their managers back in the United States, particularly if events do not unfold as planned. We are currently conducting a joint review, along with the Department of State OIG, examining the post-incident responses by DEA and Department of State personnel to three drug interdiction missions in Honduras in 2012 that all involved the use of deadly force. This joint review will address many aspects of such international operations, including pertinent pre-incident planning, rules of engagement governing the use of deadly force, and post-incident investigative and review efforts. It will also evaluate the accuracy of information provided to Congress and the public regarding these incidents. Effective management of such dangerous operations is critical to their success, and to the Department's international law enforcement efforts.

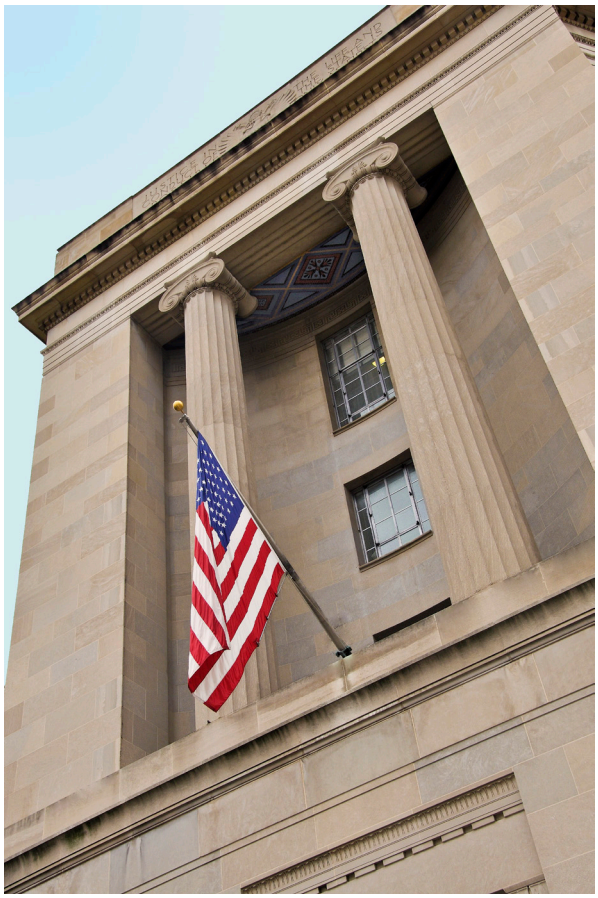
Another challenge throughout the Department's law enforcement components is to adequately address and respond to allegations of employee sexual harassment or misconduct. In March 2015, we issued a report that determined this was an area where the Department needed to focus more attention. This review was conducted in response to congressional inquiries after allegations arose regarding the conduct of U.S. government personnel, including DEA agents, during the President's 2012 trip to Colombia. We found that component supervisors did not always comply with their component policies, and did not report allegations of sexual harassment and misconduct to their respective internal affairs offices, as required. We also found that while the FBI had adequate offense tables to address these violations, ATF, DEA, and USMS did not. Additionally, we concluded that none of the four law enforcement components properly used their offense tables for charging employees with sexual harassment and sexual misconduct offenses. We further found that all four components had inadequate policies and procedures regarding employees sending sexually explicit text messages and images. These failures may hamper the components' ability to conduct misconduct investigations, fulfill their discovery obligations, and deter misconduct. The Department must put in place policies and procedures to ensure that such misconduct by its employees is handled appropriately.

The Department's ability to monitor asset seizure activities, which are often carried out in conjunction with state and local law enforcement, has also gained renewed public attention this past year. These sensitive seizure actions require effective management to ensure that the Department's authorities are used appropriately. For instance, the DEA conducts significant interdiction operations at mass transportation facilities, but our January 2015 review of the DEA's use of cold consent encounters found that the DEA does not centrally manage or coordinate training, policy, and operational requirements, which contributed to confusion regarding appropriate procedures for these encounters and searches. Our current work includes a review of the Department's oversight of its asset seizure activities, particularly seizures that may be forfeited administratively. This review is also examining the Department's implementation of an Attorney General order, issued in January 2015, that limited the ability of federal agencies to adopt seizures made by state and local law enforcement. Given the risks to civil liberties and public confidence in law enforcement attendant with such activities, the Department must ensure that they are carried out appropriately.

Adding to the Department's oversight challenges is the need to integrate rapidly evolving technologies into rules and policies designed for a pre-digital era. In March 2015, the OIG issued its second audit report regarding the Department's use of Unmanned Aircraft Systems (UAS), or drones, in law enforcement operations. We identified discrete program management challenges in the FBI's use of drones, and found that the FBI and Federal Aviation Administration (FAA) had drafted rules that expand the locations and times that the FBI could operate its drones without first requesting written FAA permission. In May 2015, the Department issued agency-wide guidance restricting the use of drones to only properly authorized investigations and activities. While the Department has taken steps to formalize its oversight of this particular technology, it must remain vigilant in adapting its management efforts as advanced technological tools, and their use by law enforcement, evolve. In that regard, the Department also recently issued policy guidance governing the use of cell site simulators, sometimes known as "Stingrays." Cell-site simulators

function as cell towers and are used by law enforcement to transmit cell signals – including those from non-target devices – to locate or identify cellular devices in a particular area. The new policy requires Department components to obtain a search warrant supported by probable cause before using cell-site simulators, with exceptions for certain exigent or exceptional circumstances. Use of other technologies to collect and store vast amounts of data, such as that collected by license plate readers, may reveal an individual's movements or travel patterns. Use of these technologies will require the Department to balance public safety and privacy interests, to ensure these tools are used effectively and responsibly.

6. Promoting Public Confidence by Ensuring Ethical Conduct throughout the Department



Source: DOJ OIG

In order to carry out the crucial mission of enforcing the law, defending the interests of the United States, and protecting the public, the Department's employees must ensure that their behavior and motives are ethical and beyond reproach. Failure to meet these core expectations undermines the Department's credibility, presents security risks, and diminishes the Department's effectiveness.

The Department continues to face challenges in holding all of its senior officials to the highest standards of ethical conduct and must ensure the consequences of wrongdoing are clearly understood. To assist the Department in doing this, in June 2015 the OIG began posting on our public website summaries of certain high level employee misconduct findings that did not result in a criminal prosecution. This should help ensure public confidence that government employees who commit wrongdoing are held accountable.

Eradicating nepotism and favoritism in hiring throughout the Department remains a challenge for management. In February 2015, the OIG reported that senior level managers at the International Criminal Police Organization (INTERPOL) in Washington violated the Standards of Ethical Conduct in 2011 and 2012 when they used their positions to benefit friends and acquaintances by placing them in unpaid intern positions that provided significant advantage when they subsequently competed for paid contractor and full-time positions. The OIG also found that INTERPOL's Executive Officer exploited his position by working to obtain positions for his son and three others. Separately, an OIG investigation revealed that in 2014 an Assistant Director at the USMS improperly influenced the hiring of a contract employee with whom the official had a prior romantic and ongoing personal relationship. As we reported in last year's challenges, in September 2014 the Deputy Attorney General directed all DOJ components to adopt uniform hiring procedures and disclosure forms following two previous OIG investigations that revealed multiple violations of the prohibition against nepotism and other personnel rules. We believe these steps will help reduce nepotism and favoritism in Department hiring going forward, but that the problem persists and the Department must continue to work to address it so that employees and the public understand and believe that hiring is based on merit and not personal connections or other improper considerations.

Strong controls and oversight of law enforcement remain an important issue for the Department as it seeks to maintain its reputation as an organization that prizes integrity. Yet, several OIG investigations in the past year highlight that the Department still struggles to meet different aspects of that challenge. In particular, the Department must remain vigilant in ensuring its employees safeguard sensitive information they encounter in their daily work. The consequences of failures in this area are illustrated by former FBI Special Agent Robert Lustyik, who pleaded guilty to selling confidential law enforcement information regarding a foreign politician for use by his political rival. In March and September 2015, Lustyik was convicted of corruption in two different federal cases and sentenced to consecutive 10- and 5-year prison sentences respectively following separate OIG investigations in Utah and New York. Another ongoing challenge for the Department is maintaining adequate evidence controls to prevent tampering or other agent misconduct, which can undo successful criminal prosecutions. In July 2015, former FBI Special Agent Matthew Lowry was sentenced to 3 years in prison after an OIG investigation revealed that he stole drug evidence while working as an agent between 2013 and 2014. Lowry's misconduct tainted several investigations, requiring prosecutors in the District of Columbia to dismiss cases against more than two dozen convicted drug dealers, and to forego the prosecution of 26 others. Similarly, the Department must also implement controls to prevent employees from inappropriately enriching themselves with Department funds. A former DEA employee was sentenced to 2 years in prison and ordered to pay restitution in the amount of $113,841 after an OIG investigation revealed she had applied for and used credit cards issued to fictitious DEA employees. And the Department must also closely monitor undercover operations, particularly those in emerging areas. This challenge is exemplified by former DEA Special Agent Carl Force, who pleaded guilty to extortion, money laundering, and obstruction of justice in connection with his theft of $700,000 in bitcoins, a form of electronic currency. Force stole the bitcoins while working undercover, as part of the multi-agency Electronic Crimes Task Force, to investigate the Silk Road, an online marketplace selling illegal drugs and other contraband.

A valuable resource for the Department in combating these challenges are whistleblowers, who perform a critical public service in bringing to light information that safeguards the Department against fraud, waste, and misconduct. The OIG remains committed to supporting the efforts of whistleblowers and ensuring that they are fully aware of their rights and protections from reprisal. For FBI employees, there is a separate regulatory scheme through which whistleblowers pursue allegations of reprisal within DOJ. However, a January 2015 report by GAO found that there was significant room for improvement in the Department's process, particularly with regard to the scope of the persons to whom disclosures can be made and be considered protected, and the timeliness of the Department's handling of these important matters. At the OIG, the number of FBI whistleblower retaliation complaints has risen dramatically in recent years. This increase will likely accelerate in the future due to the OIG's expanded training and education efforts, including partnering with the FBI to create a new mandatory training program for all FBI employees, as well as a recent DOJ proposal, supported by the OIG, to increase the list of officials to whom protected disclosures may be made under the FBI whistleblower regulation. The Department will face a growing challenge in handling an expanding docket of these matters in a timely fashion so that any appropriate remedies are not rendered moot by the passage of time or otherwise.

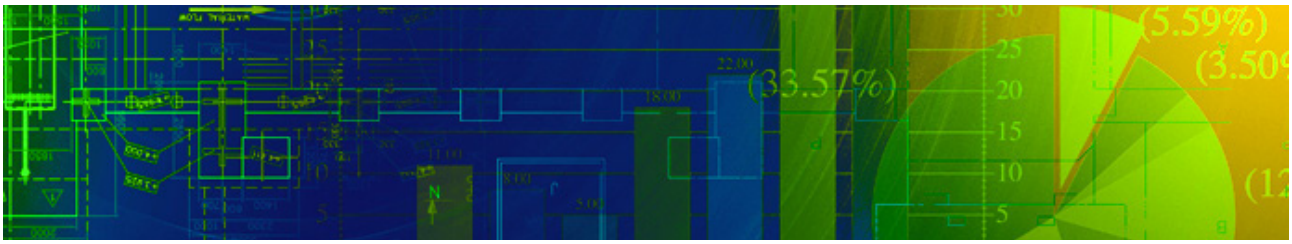
Source: DOJ OIG

For the Department's leaders to be effective in managing agency programs, they must be able to rely on accurate, real-time information regarding which programs are working and which need improvement. But as recent experience has shown, those goals can be thwarted if the Department denies or delays the OIG's access to all of its records, as required by the Inspector General Act. In recent years, several OIG reviews were delayed by Department components that withheld certain information requested by the OIG, including (a) an evaluation of how the Department's law enforcement components handled sexual harassment

allegations, (b) an audit of the DEA's policies and oversight over its higher risk confidential sources, and (c) a multi-agency review of the government's sharing of information leading up to the Boston Marathon bombing. For Department leadership to be able to benefit from the OIG's work in improving the integrity and efficiency of the Department's operations, our office must be able to engage in independent oversight. This also fosters public trust in government. In July, the DOJ Office of Legal Counsel (OLC) issued an opinion concluding that the Inspector General Act did not authorize the DOJ OIG to have independent access to grand jury, wiretap, and certain credit information. Immediately following the issuance of OLC's opinion, the OIG requested that Congress promptly pass legislation, supported by the entire IG community, to ensure that Inspectors General have independent access to the information they need to perform their critical duties. Both the Attorney General and the Deputy Attorney General have expressed their support for this effort and the Department should make every effort to ensure this important principle remains at the core of the law that ensures IGs can perform their critical duties.

Another issue that continues to draw widespread scrutiny is the process for how the Department handles complaints regarding the conduct of Department attorneys when they are acting as such. A December 2014 GAO report found the Department does not do enough to ensure that attorneys who have engaged in professional misconduct serve the discipline imposed. The GAO report acknowledged that the Executive Office for U.S. Attorneys (EOUSA) revised its procedures for documenting attorney discipline after a February 2014 OIG review of that component's flawed disciplinary system. But the GAO report also found that poor recordkeeping still hampered EOUSA's ability to ensure that discipline decisions were consistent and that discipline was actually imposed. More fundamentally, the GAO report also noted that Congress and others, including the American Bar Association, continue to voice concerns that the Department's underlying process for disciplining attorneys lacks transparency. The GAO report noted that some members of Congress have called for the OIG to have jurisdiction over professional misconduct investigations against DOJ attorneys on the grounds that the OIG's statutory and operational independence from the Department would better ensure that sufficient and timely information on attorney misconduct is provided to the public. Similarly, the independent, non-partisan Project on Government Oversight called in a March 2014 report for jurisdiction over attorney misconduct within the Department to be transferred to the OIG, just as it exists at other agencies throughout the federal government, based on our statutory independence and transparency. As mentioned above, the OIG regularly posts summaries of employee misconduct findings on its website, including those involving Assistant U.S. Attorneys. By contrast, the Department's Office of Professional Responsibility (OPR), which has exclusive jurisdiction to investigate Department attorneys for alleged misconduct arising from litigation-related activities, discloses only summary data and examples in its Annual Reports, and the most recent annual report available on its public website describes misconduct that occurred more than 2 years ago. The Department faces a significant challenge in ensuring the public credibility and transparency of investigations of its attorneys who are themselves at the forefront of carrying out the laws.

Source: DOJ OIG



Source: COPS website

7. Effectively Implementing Performance-Based Management

Performance-based management continues to be a challenge for not only the Department, but also the entire federal government. The Government Performance and Results Modernization Act of 2010 (GPRA) and corresponding guidance in the Office of Management and Budget's Circular No. A-11 emphasize priority-setting, cross-organizational collaboration to achieve shared goals, as well as the use and analysis of goals and measurements to improve outcomes. GPRA also requires federal agencies to establish priorities, conduct quarterly data-driven reviews to measure performance, and use Performance.gov as a vehicle to report this information to the public. As the Department implements these GPRA requirements, it must work to develop, collect, and analyze meaningful and outcome-oriented performance metrics.

The Department has over 40 components that administer programs with a wide range of important goals, including prevention of terrorism, promotion of national security, reduction of violent crime, and enforcement of federal laws. Measuring programmatic outcomes is frequently not easy with these types of programs, but the Department must continue to develop the means to identify and collect data related to performance measures. In short, collecting the right data, and then using it to evaluate performance and improve management of programs, will aid the Department in accomplishing its strategic goals.

The Department has begun implementing the tenets of performance-based management with the development of four priority goals and a focus on results that can be accomplished within 12 to 24 months. The Department reported to the public, via Performance.gov, that as of March 2015 it exceeded all priority goals in the areas of national security, violent crime, and financial and healthcare fraud, while noting it still needed to do more to protect vulnerable victims. However, our work has found that the Department must improve the reliability of the data it collects and must better analyze this data to improve its tracking and assessment of operational performance.

Many of the Department's current performance goals and indicators focus on inputs, workload, or processes, rather than focusing on outcomes and results. For example, several of the Department's performance measures, such as the reduction of the number of financial and healthcare fraud investigations pending longer than 2 years, focus on workload as opposed to outcomes. While they may provide information about the number and duration of financial and healthcare fraud investigations, these measures fail to convey the significance and impact of the Department's efforts to reduce these types of crime. Results-oriented measures are critically important if the Department is to effectively monitor whether its programs, initiatives, and operations are accomplishing their intended goals. The Department must capture information that meaningfully links its inputs to outcomes in order to properly direct its efforts and show the value of its programs to taxpayers.

As an example, a June 2015 GAO report found that while the Department has created "key indicators" intended to measure the success of its Smart on Crime initiative, these indicators generally do not show whether the Department is making progress toward the initiative's goals. Specifically, the GAO found that 7 of the 16 indicators are confusing or do not represent the information the indicator name implies, and that

13 of the 16 indicators lack contextual information needed to appropriately interpret their results. In the same report, the GAO reviewed the performance measures for the Department's Clemency Initiative and reported that, even though the goal is to expeditiously process clemency petitions, the Department is not tracking how long, on average, each step in the review process takes. In addition, the GAO concluded that the BOP does not have a comprehensive plan in place to gauge the success of the nearly 20 reentry programs designed to reduce recidivism. Research indicates that improved data collection and clearly defined goals and progress measures can assist agencies such as the Department in more effectively measuring their efforts.

Our work has also identified repeated instances where the Department does not collect the right information needed to inform program decisions and therefore struggles to make meaningful program improvements. For example, our January 2015 review of the DEA's cold consent encounters at mass transit facilities found that task force agents do not collect demographic information about each encounter they conduct or encounters that do not result in drug or money seizures. As a result, the DEA cannot assess whether it is conducting these encounters in an unbiased or effective manner. We identified another example of inadequate data collection and analysis during our November 2014 audit of the Department's international fugitive removal efforts. In this audit, we found that the Department should adopt a fully-informed decision-making process that considers several factors including the cost of bringing an international fugitive to the United States to face justice. However, we found that the USMS did not maintain complete and accurate cost data associated with its international fugitive removal efforts and, therefore, could not do this. Findings such as these indicate a continued need for the Department to embrace performance-based management by asking the right questions that generate data directly relevant to the requirements and goals of its programs.

Reliable data is an essential building block to effective performance-based management and has proven to be elusive at times for the Department. In its 2014 Annual Performance Report, the Department said it views data reliability and validity as critically important in the planning and assessment of its performance and that every effort is made to ensure the completeness and reliability of its data. Yet, the OIG continues to find examples where the Department has failed to collect accurate and reliable data. As the Inspector General noted in recent testimony before Congress about the BOP, the absence of reliable data impinges on the OIG's mission as well as the Department's ability to evaluate the effectiveness of its programs and to make necessary improvements. For example, during several of our reviews, the OIG was unable to obtain recidivism data from the BOP for federal inmates. If it had better data, the Department could better focus its limited resources and make strategic investments in programs that show progress in reducing incarceration costs, deterring crime, and improving public safety.

Source: DOJ

Further, the OIG has found that on many occasions when the Department does try to collect data, the data is inaccurate, unreliable, or simply goes unused, thereby impacting its ability to effectively manage and assess its operations. For example, our June 2015 review of the U.S. Attorneys' Offices' (USAOs) debt collection program found insufficient data entry controls for the Department's debt collection tracking system. As a result, the system did not contain sufficiently reliable information to enable the USAOs and the Executive Office for U.S. Attorneys (EOUSA) to accurately assess the performance of their Financial Litigation Units and the debt collection program as a whole. This deficiency was coupled with the failure of the debt collection tracking system to capture all the information needed to sufficiently evaluate debt collection performance across the USAOs. As a result, the USAOs and the EOUSA could not rely on the data they collected to inform management decisions for the USAOs' debt collection program. This report also identified staffing issues that limited the ability of Assistant U.S. Attorneys to track debt collection matters. Given that the U.S. Treasury is owed more than $1 billion, it is important that the Department prioritize its data collection in this area so it can better track down the money the federal government is owed.

Having accurate metrics, good data, and strong analysis is valuable, but if the Department does not have enough talented personnel to carry out its goals, its program performance inevitably will suffer. To improve its performance, the Department needs to do a better job investing wisely in human capital. Since January 2011, the Department has had to operate with fewer staff for many reasons, including budget constraints and difficulties in the hiring process. A January 2014 GAO report found that 28 percent of employees working for the Department in 2012 will be eligible to retire by September 2017. In light of the Department's request to Congress for funding to add 580 positions during FY 2015 and another 1,598 positions in FY 2016, it needs to find strategies to ensure that it is wisely planning for new hires and investing in human capital so that programs have the personnel they need to be successful.

Performance-based management remains an ongoing challenge for the Department. Improving the Department's collection and analysis of program performance measures is critical, as is collecting more reliable data. Enhancing these areas will assist the Department in more effectively measuring its programs and allocating its resources, and as a result, achieve more of its strategic management goals. The OIG is taking steps to apply data analytics models to Department data with the goal of better assessing the effectiveness and efficiency of the Department's programs and operations, along with improving the OIG's ability to identify waste, fraud, and abuse. However, the success of the OIG's efforts will depend, at least in part, on the quality and relevance of the data the Department collects.

8. Protecting Taxpayer Funds from Mismanagement and Misuse

Source: Office for Victims of Crime website

With an FY 2015 budget of $26.2 billion, the Department must act as a responsible steward of not only the funds it uses internally but also funds it distributes to outside parties through contracts and grants. To ensure that it earns the public's trust, it is imperative that the Department diligently protect taxpayer funds, manage its own resources wisely, and seek ways to improve the economy and efficiency of agency programs.

The Department faces significant challenges in using and monitoring funds within its control. In FY 2015, the OIG's audit-related efforts resulted in 79 reports that contained approximately $53 million in questioned costs, reported over $4 million in funds that should be put to better use, and made more than 300 recommendations for management improvements. Our work has highlighted shortcomings in the Department's management and oversight of tax dollars – particularly funds distributed through contracts and grants. Our reports show this remains a continuing challenge for the Department.

Funds Spent within the Department

The Department expends millions of taxpayer dollars on its internal operations and programs and must handle these funds efficiently and responsibly. Yet, recent OIG work has shown that there is room for improvement in the Department's management of its spending in a wide variety of areas. For example, in the OIG's audit of the Department's use of extended Temporary Duty (TDY) travel, we found that the FBI, Criminal Division, National Security Division, and the Executive Office for United States Attorneys and U.S. Attorneys' Offices, made extensive use of extended TDY. Based on the limited data available, we estimated that these components combined spent more than $54 million on 4,788 extended TDY events between FY 2012 and the first quarter of FY 2014. However, we found that the components are not adequately tracking extended TDY, and that they may be inappropriately relying on it to respond to staffing or other issues, using it when it is not warranted and not using it when it is. Similarly, the OIG's March 2015 audit of the Department's Unmanned Aircraft Systems (UAS) provided another example of poor fiscal management.

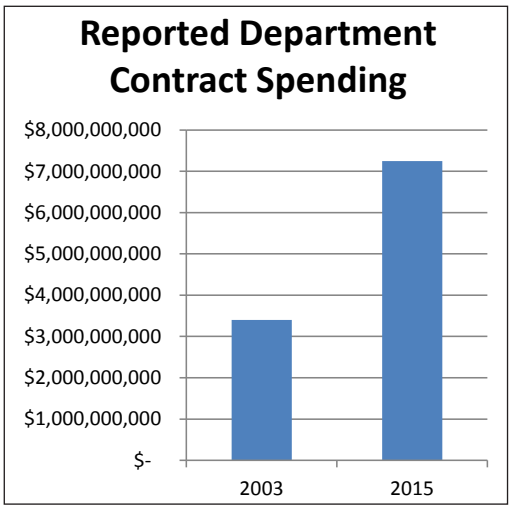
We found that ATF spent approximately $600,000 on UAS vehicles (commonly referred to as "drones"), but never flew them operationally. We also found that less than a week after ATF suspended its UAS program in June 2014 and disposed of its drones, a separate unit within ATF purchased five small commercial drones for approximately $15,000 without coordinating with ATF's UAS program office.

More broadly, the Department faces a significant challenge ensuring that it puts in place policies and procedures sufficient to make its stated commitment to collecting federal criminal and civil debts – the principal balance and interest on which totaled some $114.6 billion in FY 2014 – into a reality. In a report reviewing the debt collection program of the U.S. Attorneys' Offices, the OIG found that, despite acknowledging the importance of this effort, the USAOs failed to prioritize debt collection activity, which resulted in insufficient attorney and support staffing and ineffective collaboration within the USAO, thereby hindering collection efforts. If the Department is to effectively manage its budget in times of limited funding, it cannot afford to fail in this important area.

Despite these challenges, the Department has made important progress controlling costs in other areas, as shown by the OIG's most recent report on Conference Planning and Reporting Requirements. Between FY 2010 and 2014, DOJ conference costs fell by about $72 million, as the number of conferences attended fell from 1,740 to 445. This is one example of how, across all components, the Department should continue to identify ways to run its programs more effectively and efficiently.

Funds Spent via Contracts and Grants

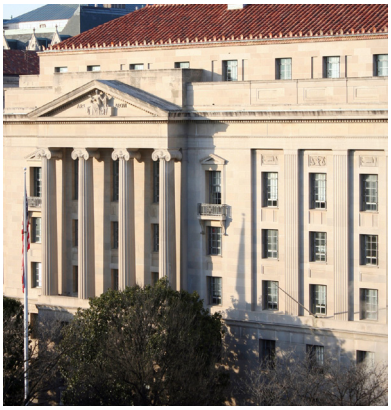
Given the scope of its procurements and awards, the Department also faces a vast oversight challenge as it seeks to ensure that it awards contracts and grants wisely and judiciously, and that the recipients use these funds to achieve their intended purpose. According to data from the government's USAspending.gov website, Department spending on contracts with outside companies increased dramatically over the past decade, more than doubling between FY 2003 and FY 2013. The exposure of such widespread government contracting remains real given the Department reportedly spent over $7 billion on contracts during FY 2015. This requires vigilant and continuous risk-based management and oversight of the Department's contracts. The primary responsibility for performing this function inevitably rests with the Department, though to help ensure that this occurs, the OIG continues to hire personnel with specialized knowledge about government contracts to help it monitor the Department's efforts in light of the significant tax dollars spent in this area.



Source: USAspending.gov

One area of significant exposure where the OIG has recently focused attention is the Department's use of high-dollar contracts to run privately-managed prisons, which housed approximately 24,000 inmates, or 12 percent of the BOP's inmate population, as of September 2015. In April 2015, the OIG issued a report on the Reeves County Detention Center in Pecos, Texas, one of BOP's largest private prison contracts, questioning its use of $2 million and its plans for unnecessarily spending another $1 million. Currently, we are also conducting two audits of contracts for prisons operated by the Corrections Corporation of America (CCA) – the BOP contract award to CCA to operate the Adams County Correctional Center in Natchez, Mississippi, and the USMS contract awarded to CCA to operate the Leavenworth Detention Center in Leavenworth, Kansas. We are also conducting a broader review of the Department's efforts to monitor its extensive use of contract prisons. The Department must ensure that these funds are spent wisely and result in institutions that are safe and secure.

Grant funding also continues to present a significant risk for mismanagement and misuse due to the sheer volume of recipients and money involved, along with program objectives that are often hard to quantify and results that are not adequately measured. According to USAspending.gov, from FY 2010 through FY 2014, the Department awarded approximately $13 billion in grants to thousands of recipients. Our recent OIG work has identified several instances when Department components exercised limited monitoring of grants and conducted few site visits. Additionally, we have found further breakdowns in monitoring at the subgrantee level, when grant recipients distribute the funds to third parties and do not adequately ensure they fulfill grant conditions. The Department must undertake robust efforts in this area to ensure that the billions it gives out in grants are appropriately spent and that the public receives the expected and desired return on its investment.



Source: DOJ OIG

One particular area where the Department will face increased responsibility is in its management of the Crime Victims Fund (CVF). In December 2014, Congress authorized the Department to use up to $2.36 billion of the current CVF balance. This more than triples the amount of CVF funds the Department was authorized to expend compared to FY 2014. This increase will allow the Department to distribute significantly more CVF grant funds through victim compensation and assistance grant programs. The OIG currently is auditing the Department's risks in managing the increase in CVF grant funds and we anticipate being active in auditing those receiving the CVF grants in the future. But the challenge remains for the Department to effectively and efficiently manage such vast expenditures in order to ensure that the goals Congress set for these grants are met in a timely fashion.

The Department's failure to effectively oversee grant awards was exemplified in an audit of grants awarded to the Navajo Division of Public Safety by the Office of Justice Programs, Bureau of Justice Assistance. In that audit, we found $35 million in questioned costs focused on the construction of correctional facilities in two Arizona locations with capacities that were at least 250 percent larger than needed. Similarly, the OIG's audit of $77.5 million in grants to the Puerto Rico Department of Justice (PRDOJ) questioned over $5 million, including millions in funds that were drawn down and not expended and others that were never used, despite the difficult economic and criminal justice challenges on the island. We also found that the PRDOJ failed to accomplish a significant portion of the grant-funded projects, something the Department failed to identify or address.

These are just examples, but the lesson is clear: both contracts and grants continue to present significant management and oversight challenges for the Department, and it must find new and better ways to interact with funding recipients to ensure that funds are expended for their stated purposes. At the most extreme end of the spectrum the OIG's Fraud Detection Office has uncovered issues including improper consultant payments, conflicts of interest, and embezzlement, affirming the need for vigilance in these areas. The OIG conducts integrity briefings for thousands of participants every year to help bring these issues to the fore, but it is ultimately up to the Department to ensure that its funding is spent responsibly.