DORSEY™
always ahead

The Next Department of Justice: Transition to a New Administration

January 9, 2017

The Next Department of Justice: Transition to a New Administration

Page No.

Program Materials

Dorsey Government Enforcement and Corporate Investigations Online Resources

Government Enforcement Actions Deskbook will help you focus on key common elements of an effective immediate response to a government or regulatory investigation.
https://www.dorsey.com/resource-landing-pages/government-enforcement-actions-deskbook

Domestic Internal Investigations Handbook addresses challenges that arise when conducting an investigation.
https://www.dorsey.com/resource-landing-pages/domestic-internal-investigations-handbook

Other Online Resources

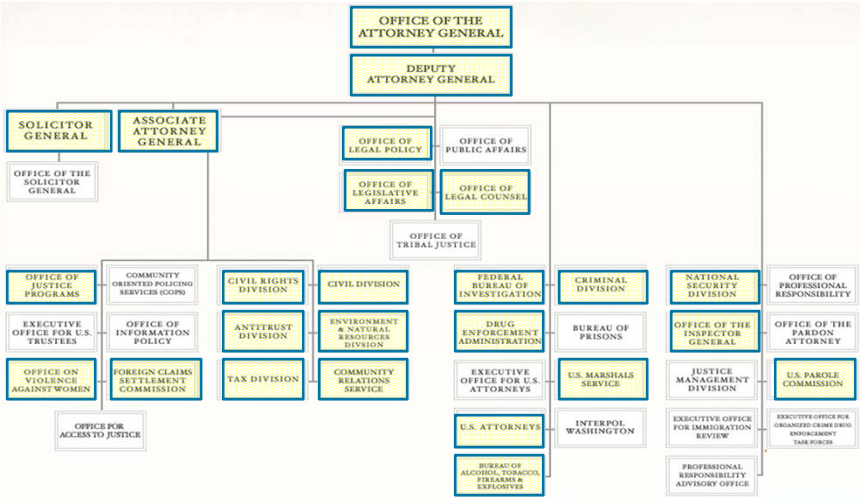
United States Government Policy and Supporting Positions (Plum Book), 2012
The Plum Book is published after the Presidential election, alternately, by the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform
https://presidentialtransition.usa.gov/2015/09/23/plum-book/

The Federalization of Criminal Law, Task Force on the Federalization of Criminal Law, American Bar Association, Criminal Justice Section (1998)
http://www.americanbar.org/content/dam/aba/publications/criminaljustice/Federalization_of_Criminal_Law.authcheckdam.pdf

The Executive Branch Transition Process

- **Pre-Election**
  - Transition Councils and Agency Transition leads
    - https://presidentialtransition.usa.gov/
  - Interim leadership identified
  - Briefs prepared for new leadership
- **Post-Election**
  - President elect deploys agency review teams
  - President elect begins selecting appointees
  - https://greatagain.gov/agency-landing-teams-54916f71f462#.gxhe2iway
- **Post-Inauguration**
  - On-board new appointees

DOJ Appointees Requiring Confirmation



*https://presidentialtransition.usa.gov/2015/09/23/**plum-book**/*

The Day After the Election

- **Who stays and who goes, how and when?**
  - **Political appointees**
    - **At will appointees**
    - **Term appointments**
  - **Civil service**
- **Before the Clock Strikes Midnight**
  - **Political to Career Conversions – "Burrowing In"**
    - **Must comply with nine merit principles and thirteen prohibited personnel practices; 5 U.S.C. §2301(b) and §2302(b)**
    - **Office of Personnel Management approval**
  - **Midnight rulemaking**
  - **Executive orders**
  - **Clemency**
  - **What does the prior appointee want to do?**

Between Administrations: The Rock and the Hard Place

- **Interim Leadership – responsibility with limited authority**
  - **Loss of the bully pulpit**
  - **Looking toward the future**
- **Is this a good time to approach law enforcement?**

The Handoff – Transition

- **The Successor – who is next, how is he/she selected, when does he/she arrive?**
  - **Minnesota Appointees**
    - **U.S. District Judges (PAS) (2)**
    - **U.S. Attorney (PAS)**
    - **U.S. Marshal (PAS)**
    - **State Director, USDA Rural Development (SC)**
    - **State Executive Direction, Farm Services Agency (SC)**
  - **Cross party nominations – Democratic senators and Republican representatives**
- **What can you learn from the selection process?**
- **The Oath of Office – when authority passes**

Taking Charge

- **New Leadership, New Strategies**
  - **The Old**
    - https://www.justice.gov/jmd/strategic2014-2018/index.html
  - **The New**
    - https://greatagain.gov/
- **Obstacles to Change**

"There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things."
— Niccolo Machiavelli
The Prince (1532)

Predictions

Never make predictions, especially about the future - Casey Stengel

- **Terrorism**
- **National Security**
- **Cybercrime**
- **White Collar/Corruption**
  - **False Claims Act**
  - **Foreign Corrupt Practices Act**
- **Civil Rights**
- **Immigration**
- **Violent Crime and Drugs**

https://www.justice.gov/jmd/strategic2014-2018/index.html
https://www.justice.gov/usao/priority-areas
https://www.fbi.gov/about/mission

Transition Overview

2016 Presidential Transition

August 2, 2016

Introduction

This document provides an overview of the 2016 Presidential transition process. It outlines the major transition activities and governance structure in order to provide a quick guide of the who, what, and when of the major milestones that occur during a Presidential transition. While this document offers a broad overview, the designated transition lead within each agency is the appropriate contact for agency-specific transition questions.

The peaceful transfer of power has been a hallmark of American democracy for more than 200 years. Presidential transitions are a time of significant change across the Federal government. President Barack Obama was grateful for the seriousness and thoroughness with which the George W. Bush Administration approached the transition process in 2008. Like his predecessor, President Obama is committed to leaving the federal government in the best possible stead for his successor.

As we prepare for the upcoming Presidential transition we know that, while many Federal employees have experienced one or more Presidential transitions, it will be the first transition for a number of Federal employees. Regardless of whether this transition is your first one or one of many, we hope this overview will help all Federal employees – both career and appointees – better understand and engage in this important process. Federal employees play a critical role in the process, and we look forward to working collaboratively across the Administration to ensure a smooth Presidential transition.

2016 Transition Activities

The 2016 Presidential transition process consists of three phases, each comprised of major activities:

The activities described below are crucial to the successful transfer of power between the incoming and outgoing Administrations. (See also Appendix 1 for a timeline of these activities)

Phase 1: Pre-Election

May 6, 2016: Transition Councils Formally Established

In May, the President issued an Executive Order that took the following steps to provide governance for the transition:

- Created the **White House Transition Coordinating Council (WHTCC)**, which is chaired by the Chief of Staff to the President and comprised largely of senior White House officials, to oversee the overall transition effort (see Appendix 2 for council membership);
- Created the **Agency Transition Directors Council (ATDC)**, which is co-chaired by the Federal Transition Coordinator at the U.S. General Services Administration (GSA) and the Deputy Director for Management at the Office of Management and Budget (OMB) and comprised of senior career officials from twenty-one agencies, to manage day-to-day agency transition activities (see Appendix 3 for council membership); and
- Directs the ATDC to consult on transition-related issues with the existing **President's Management Council (PMC)**, which is chaired by the OMB Deputy Director for Management and comprised of Deputy Secretaries from large agencies, to maintain consistent engagement by senior agency leadership.

Working in close coordination, these three councils provide guidance to agencies in gathering briefing materials and other information relating to the Presidential transition. The councils also oversee the preparation of career employees who are designated to fill non-career positions on an interim basis during a Presidential transition, and assist in the off-boarding of political appointees concluding their service and the on-boarding of political appointees joining service to work for the President-elect. In addition to these three councils, OMB and GSA are convening regular calls and meetings with other Federal agencies, boards and commissions throughout the government so that they receive guidance for their respective transition preparations.

May 6, 2016: Agency Transition Leads Designated

In May, the head of each agency also designate senior career employees from the agency to serve on the ATDC. The ATDC meets on a monthly basis to share best practices and discuss issues. In addition, agencies also designated senior career leadership for each

agency major component and subcomponent to implement activities relating to the Presidential transition. Staff within each agency meets on an as-needed basis to prepare their agencies. As mentioned above, OMB and GSA are convening regular calls and meetings with Federal agencies, boards and commissions not represented on the ATDC so that they receive guidance for their respective transition preparations.

August 1, 2016: Eligible Candidates Offered Transition Services and Facilities

Following the nominating conventions in late July, the transition teams of each eligible Presidential candidate are offered the use of facilities and related services to prepare for the coming change in government. These teams focus on the development of their candidate's policy agenda and personnel so that he or she is ready to govern if elected.

September 15, 2016: Acting Officers Identified for Vacant Non-Career Positions

In preparation for potential gaps between the exit and on-boarding of senior political appointees between Administrations, agency heads must identify qualified career employees to serve in critical non-career positions in an acting capacity if a position becomes vacant. These "Acting Officers" should be identified by September 15 in accordance with the Vacancy Reform Act (VRA).

November 1, 2016: Agency Briefing Materials Finalized

In line with guidance from the ATDC agencies prepare briefing materials and information relating to the Presidential transition for Agency Review Teams (also known as Agency Landing Teams), who will review briefing materials and meet with internal agency transition teams to better understand each agency and its current state of affairs. Briefing materials are prepared for two audiences: Agency Review Teams and incoming political appointees following the Inauguration. Agency Review Teams (see below) begin arriving at agencies after the election and are responsible for gathering information about the structure, function, and pressing issues facing federal agencies. Accordingly, these materials include, but are not limited to, an agency's mission, vision and strategic goals; organizational chart; budget; human capital overview; current Presidential appointees; and an overview of priority issues facing the organization.

Phase 2: Post-Election

November 9, 2016: President-elect and Vice-President-elect Offered Support

Following the election on November 8, the Administration (through GSA) will offer services and facilities to the President-elect and Vice-President-elect as they prepare to assume their duties. Post-election support will begin immediately following the GSA Administrator's ascertainment of the apparent successful candidates for the Office of President and Vice-President. The offices for the President-elect's transition will be located at GSA headquarters.

November 9, 2016: Agency Review Teams Begin Arriving at Agencies

Soon after the election, Agency Review Teams will be deployed by the President-elect to federal agencies. As mentioned above, the teams review briefing materials and meet with

internal agency transition teams to better understand each agency and its current state of affairs. In 2008, the Obama-Biden Transition team had approximately 500 agency review team members across more than 60 agencies and Executive Office of the President (EOP) components.

November 9, 2016: Selection of Incoming Presidential Appointees Begins

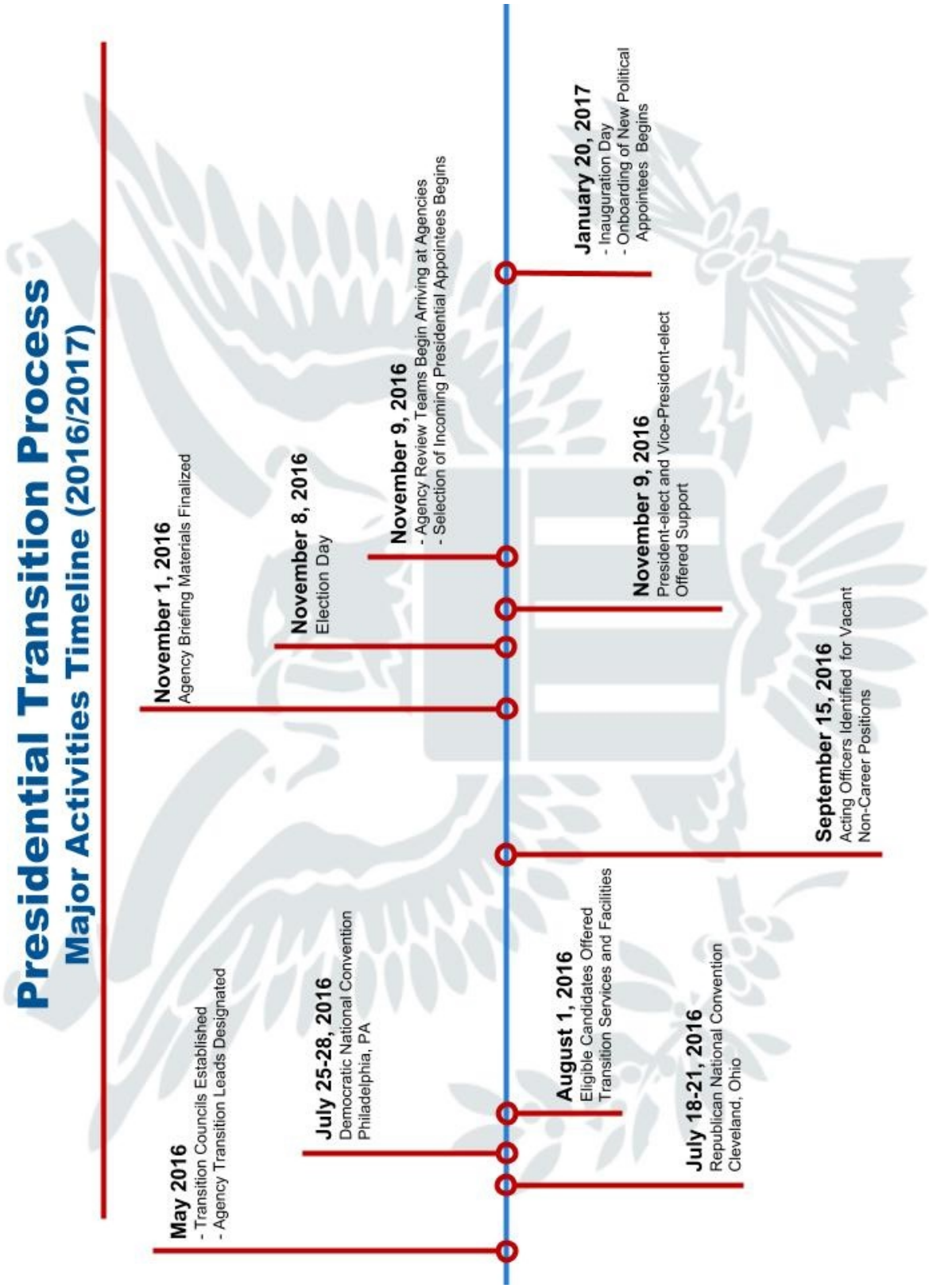
Following the election, the incoming Administration begins identifying, selecting, and vetting candidates for approximately 4,100 Presidential appointments. In some cases, an eligible candidate may begin identifying and vetting of potential appointees during the pre-election phase. Announcements of candidates for key positions often occur between the election and Inauguration. Nominations of individuals for Senate-confirmed appointments, confirmation of nominees, and appointments to positions not requiring Senate confirmation begin on Inauguration Day and continue through the post-Inauguration phase. Presidential appointments may involve background, security, and financial disclosure reviews conducted by the Office of Personnel Management (OPM), the Department of Justice (DOJ), and the Office of Government Ethics (OGE) prior to nomination. Agency Reviews and information from OPM plays a key role in understanding, from a human capital perspective, the skills, number, and types of Presidential appointments that need to be made.

Phase 3: Post-Inauguration

January 20, 2017: Inauguration & On-boarding of New Political Appointees Begins

Inauguration Day marks the official end of the current Administration. In past transitions, the President has requested all non-termed political appointees to submit in advance a letter of resignation effective upon the swearing-in of the new President. On this day, agencies will begin on-boarding new appointees and will continue to do so over the course of 2017. On-boarding includes appointee orientation activities, such as briefings and workshops, which are funded through the GSA. On January 20, 2009, the Obama Administration had seven Senate-confirmed appointees ready to begin work.

Appendix 1: Presidential Transition Process



Appendix 2: 2016 White House Transition Coordinating Council Members

Chair

Denis McDonough
Chief of Staff to the President

Vice Chair

Anita Breckenridge
Assistant to the President & Deputy Chief of Staff for Operations

Council Members

Kristie Canegallo
Assistant to the President &
Deputy Chief of Staff for Implementation

Susan Rice
Assistant to the President for
National Security Affairs

Lisa Monaco
Assistant to the President for
Homeland Security and Counterterrorism

Jeff Zients
Assistant to the President for Economic Policy &
Director of the National Economic Council

W. Neil Eggleston
Counsel to the President

Shaun Donovan
Director of the Office of Management and Budget

Rudy Mehrbani
Assistant to the President for
Presidential Personnel

Denise Turner Roth
Administrator of General Services

James Clapper
Director of National Intelligence

Timothy O. Horne
Federal Transition Coordinator

Appendix 3: 2016 Agency Transition Directors Council Members

Co-Chairpersons

Andrew Mayock
Senior Advisor
Office of Management and Budget (OMB)

Timothy O. Horne
Federal Transition Coordinator
U.S. General Services Administration (GSA)

Council Members

Beverly Ortega Babers
U.S. Department of the Treasury (DOT)

Barbara E. Carson
U.S. Small Business Administration (SBA)

Denise Carter
U.S. Department of Education (ED)

Thomas Cremins
National Aeronautics & Space Administration (NASA)

Shelley K. Finlayson
U.S. Office of Government Ethics (OGE)

John Gentile
U.S. Department of Health & Human Services (HHS)

Henry Hensley
U.S. Department of Housing & Urban Development (HUD)

Edward C. Hugler
U.S. Department of Labor (DOL)

Lana Hurdle
U.S. Department of Transportation (DOT)

Edward Keable
U.S. Department of the Interior (DOI)

Kristie A. Kenney
U.S. Department of State (DOS)

Shannon Kenny
U.S. Environmental Protection Agency (EPA)

Ingrid Kolb
U.S. Department of Energy (DOE)

Lee Lofthus
U.S. Department of Justice (DOJ)

Vincent Micone
U.S. Department of Homeland Security (DHS)

Richard Christian (Chris) Naylor
National Archives & Records Administration (NARA)

Pravina Raghavan
U.S. Department of Commerce (DOC)

Michael Rhodes
U.S. Department of Defense (DoD)

Jozetta Robinson
U.S. Office of Personnel Management (OPM)

Kevin Shea
U.S. Department of Agriculture (USDA)

Robert (Bob) D. Snyder
U.S. Department of Veterans Affairs (VA)

Council Staff

Asma Mirza
Special Assistant
OMB

Rayden Llano
White House Fellow
OMB

Jamise Harper
Chief of Staff to the FTC
GSA

Nathan Kreoger
Special Assistant
GSA

Appendix 4: Frequently Asked Questions

1. **Who should I contact with any questions pertaining to the Presidential transition?**

   You should contact your manager or your agency's designated transition point of contact with any questions regarding the transition (see Appendix 3). If you are unable to identify your point of contact, please email presidentialtransition@gsa.gov.

2. **What are the roles and responsibilities of the White House Transition Coordinating Council (WHTCC)? Who sits on the council?**

   The WHTCC supports the Presidential transition by providing guidance to agencies and the Federal Transition Coordinator regarding preparations for the Presidential transition, including succession planning and preparation of briefing materials. The WHTCC also facilitates communication and information sharing between the transition representatives of eligible candidates and senior employees in agencies and the Executive Office of the President, and it prepares and hosts interagency emergency preparedness and response exercises. WHTCC members include:

   - Assistant to the President and Chief of Staff (Chair)
   - Assistant to the President and Deputy Chief of Staff for Operations (Vice Chair)
   - Assistant to the President and Deputy Chief of Staff for Implementation
   - Counsel to the President
   - Assistant to the President for Presidential Personnel
   - Assistant to the President for National Security Affairs
   - Assistant to the President for Homeland Security and Counterterrorism
   - Assistant to the President for Economic Policy and Director, National Economic Council
   - Director of National Intelligence
   - Director of the Office of Management and Budget
   - Administrator of General Services
   - Federal Transition Coordinator
   - A Transition Representative for each Eligible Candidate (Advisory Capacity)

3. **What are the roles and responsibilities of the Agency Transition Directors Council? Who sits on the council?**

   The ATDC's responsibilities include coordinating transition activities among the Executive Office of the President, agencies, and the transition team of eligible candidates and the President-elect and Vice-President-elect; providing guidance to agencies in gathering briefing materials and information relating to the Presidential transition; and ensuring agencies adequately prepare career employees who are designated to fill non-career positions during a Presidential transition. ATDC members include:

   - OMB Deputy Director for Management (Co-Chair)
   - Federal Transition Coordinator (Co-Chair)

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of the Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Department of the Treasury
- Department of Veterans Affairs
- Environmental Protection Agency
- National Aeronautics and Space Administration
- Small Business Administration
- Office of Personnel Management
- Office of Government Ethics
- National Archives and Records Administration
- A Transition Representative for each Eligible Candidate (Advisory Capacity)

4. How will responsibility for transition activities be divided between the WHTCC, the ATDC and the PMC?

The WHTCC will provide overall oversight and guidance on the Presidential transition process to agencies and the Federal Transition Coordinator. The ATDC, in concert with the PMC, will coordinate transition activities across large agencies drawing upon WHTCC guidance.

5. My agency is not represented on the ATDC. How will we be kept informed of and engage in the Presidential transition process?

To ensure a whole of government approach, OMB's Deputy Director for Management and the Federal Transition Coordinator will regularly convene the transition directors of agencies that are not covered by the ATDC to provide updates on the transition process.

6. Is there guidance to assist Federal agencies in developing transition related briefing materials for the incoming Administration?

In the spirit of approaching the Presidential transition process through a demand-driven perspective that is based on prior experience and input from the eligible

candidates' transition representatives, the current Administration will provide broad guidance to assist agencies in developing briefing materials for the incoming Administration that is useful and enables the next team to quickly and smoothly begin their new roles.

7. Where can I find additional resources related to the Presidential transition?

For additional information on the Presidential transition, please visit the Presidential Transition Directory at https://presidentialtransition.usa.gov/.

U.S. Department of Justice
Office of the Attorney General

UNITED STATES DEPARTMENT OF JUSTICE

FISCAL YEARS 2014-2018

STRATEGIC PLAN

A MESSAGE FROM THE ATTORNEY GENERAL

Shortly after beginning my first job as a line attorney at the Department of Justice nearly 37 years ago, I discovered that I had been given a once-in-a-lifetime opportunity. I had the chance to be part of a highly skilled and motivated group of extraordinary men and women who were reaffirming our Nation's founding principles of liberty, equality, and security; helping to shape America's future; and taking innovative and collaborative steps to protect our fellow citizens.

Today, as Attorney General, I have the privilege of leading this great organization. As I look toward the future, I am focusing our actions in four key areas to fulfill one core mission: protecting the American people. First and foremost, we will protect Americans from terrorism and other threats to national security, both at home and abroad. Second, we will protect Americans from the violent crimes that have ravaged too many communities, devastated too many families, and stolen too many promising futures. Third, we will protect Americans from the financial fraud that devastates consumers, siphons taxpayer dollars, weakens our markets, and impedes our ongoing economic recovery. And, finally, we will protect those most in need of our help – our children; the elderly; victims of hate crimes, human trafficking, and exploitation; and those who cannot speak out or stand up for themselves.

The Department's strategic goals reflect the above four key areas of focus. Our goals are: Strategic Goal 1, *Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law*; Strategic Goal 2, *Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law*; and Strategic Goal 3, *Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal, and International Levels*. These three goals provide the framework that supports my priorities.

This *Strategic Plan* highlights our efforts to support all of these priorities in our multiple roles as law enforcer; litigator; and partner with state, local, tribal, and international governments. It describes our strategies for protecting our people from terrorists; our citizens, institutions, and environment from harm; and all individuals involved in the judicial process – including those housed in our prisons – from danger and fear.

It is through the commitment to justice by the individuals who make up this organization that I envision future generations of Americans continuing to enjoy the freedoms and opportunities that our forefathers sought. This *Plan* describes our contribution to helping this great democracy continue to develop and flourish. But we are not finished. As we consider where we must go from here, I am reminded of the words 37 years ago of my first boss and one of my heroes, Attorney General Edward Levi, "the agenda of the Department is inevitably unfinished…[and] is also always boundless."

Eric H. Holder, Jr.

INTRODUCTION

The *Department of Justice Strategic Plan for Fiscal Years 2014-2018* (*Strategic Plan* or *Plan*) provides a guide for describing and accomplishing the Department of Justice (the Department or DOJ) priorities over the next 5 years. This new *Plan* reflects the goals, objectives, and areas of emphasis of Attorney General Eric H. Holder, Jr. While the strategic goals are similar to those in the prior version, this *Plan* places a stronger emphasis on *rule of law, international partnerships, reinvigorating the traditional missions* of the Department, *criminal justice reform,* and *restoring credibility* in this institution.

Under this Administration and Attorney General, the Department has strengthened the rule of law across our Nation and beyond our borders, has revitalized its traditional missions, and has reinvigorated its working collaboration with state and local law enforcement to make communities safer. The Department has reinforced its commitment to combating tax fraud schemes, protecting Americans' civil rights, preventing gun violence, and preserving the environment. And it has achieved unprecedented gains holding accountable those whose illegal and irresponsible conduct precipitated the recent financial crisis.

However, our work is not finished. DOJ must build on the great work being done across the country to reduce violent crime and reform our criminal justice system. We must continue to look for ways to ensure that federal laws are enforced fairly and federal resources are used efficiently, while increasing support to those who become victims of crime and promoting public safety overall.This *Plan* describes the Department's strategies to support its top priority which is, and will continue to be, combating terrorism. At the same time, the *Plan* describes the Department's work and responsibilities that extend over the broad spectrum of American life. These responsibilities include making streets safe for families, ridding communities of illegal guns and drugs, stopping those that would undermine the financial stability of communities and the Nation, protecting children and other vulnerable persons from predators, protecting the environment, and preserving civil liberties and freedoms.

The circumstances and issues DOJ employees face are some of the most challenging and complex in government. The tasks the Department must address are significant, varied, and critical to the Nation. This *Strategic Plan* responds to these challenges through three strategic goals focused on advancing the Department's priorities and reflecting the outcomes the American people deserve. These goals are:

Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law

Goal 2: Prevent Crime, Protect the Rights of the American People, and Enforce Federal Law

Goal 3: Ensure and Support the Fair, Impartial, Efficient, and Transparent Administration of Justice at the Federal, State, Local, Tribal, and International Levels

DOJ integrates these strategic goals into its management and operations to ensure a

more efficient and stronger Department. This involves setting long-term goals and objectives, translating those goals and objectives into budgets and program plans, implementing programs, monitoring program performance, and evaluating the results. The Department's *Strategic Plan* provides the overarching framework for component strategic plans as well as annual performance plans, budgets, and reports.

Further, DOJ will reevaluate and strengthen its approach as needed. The world is not static and, as challenges arise, the Department will respond. The strength of a strategic plan is, in part, its flexibility to meet evolving demands; accordingly, this *Strategic Plan* should be considered a living document that will be modified, as needed, to meet new and important challenges.

Priority Goals

In support of building a high-performing government, the Department developed four Priority Goals that reflect the Attorney General's priorities, complement and support the three DOJ Strategic Goals, and focus on results that can be accomplished within 12 to 24 months (FY 2014-FY 2015). The four draft Priority Goals are:

1) National Security: Protect Americans from terrorism and other threats to National Security, including cyber security threats. By September 30, 2015, the Department of Justice will: disrupt 125 terrorist threats and groups and disrupt and dismantle 200 cyber threat actors.

2) Violent Crime: Protect our communities by reducing gun violence using smart prevention and investigative strategies in order to prevent violent acts from occurring. By September 30, 2015, the Department will: increase the number of records submitted to the National Instant Criminal Background Check System Index by states and federal agencies by 10%; increase the number of records entered into the National Integrated Ballistic Identification Network (NIBIN) by 3%; and increase the number of NIBIN "hits," that is, the linkage of two or more separate crime scene investigations, based upon comparisons of the markings made on fired ammunition recovered from crime scenes by 3%.

3) Financial and Healthcare Fraud: Reduce financial and healthcare fraud. By September 30, 2015, the Department of Justice will: reduce by 3 percent, the number of financial and healthcare fraud investigations pending longer than 2 years to efficiently and effectively drive those investigations to resolution.

4) Vulnerable People: Protect vulnerable populations by increasing the number of investigations and litigation matters concerning child exploitation, human trafficking, and non-compliant sex offenders; and by improving programs to prevent victimization, identify victims, and provide services. By September 30, 2015, working with federal, state, local, and tribal partners, protect potential victims from abuse and exploitation through three sets of key indicators: open investigations concerning non-compliant sex offenders (4% over average of FYs 2012, 2013), sexual exploitation of children (3% over average of FYs 2011, 2012, 2013), and human trafficking (2% over FY 2013); open litigation matters concerning sexual exploitation of children and human trafficking (5% increase over baseline (TBD)); percent of children recovered within 72 hours of issuance of an AMBER alert (90%).

Per the Government Performance and Results (GPRA) Modernization Act, 31

U.S.C. 1115(b)(10), requirement to address Federal Goals in the agency Strategic Plan and Annual Performance Plan, please refer to Performance.gov for information on Federal Priority Goals and the agency's contributions to those goals, where applicable.

The Mission

... to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.

The Core Values

These core values underlie the Department's work, inform its strategic goals, and guide its employees.

Equal Justice under the Law. Upholding the laws of the United States is the solemn responsibility entrusted to DOJ by the American people. The Department enforces these laws fairly and uniformly to ensure that all Americans receive equal protection and justice.

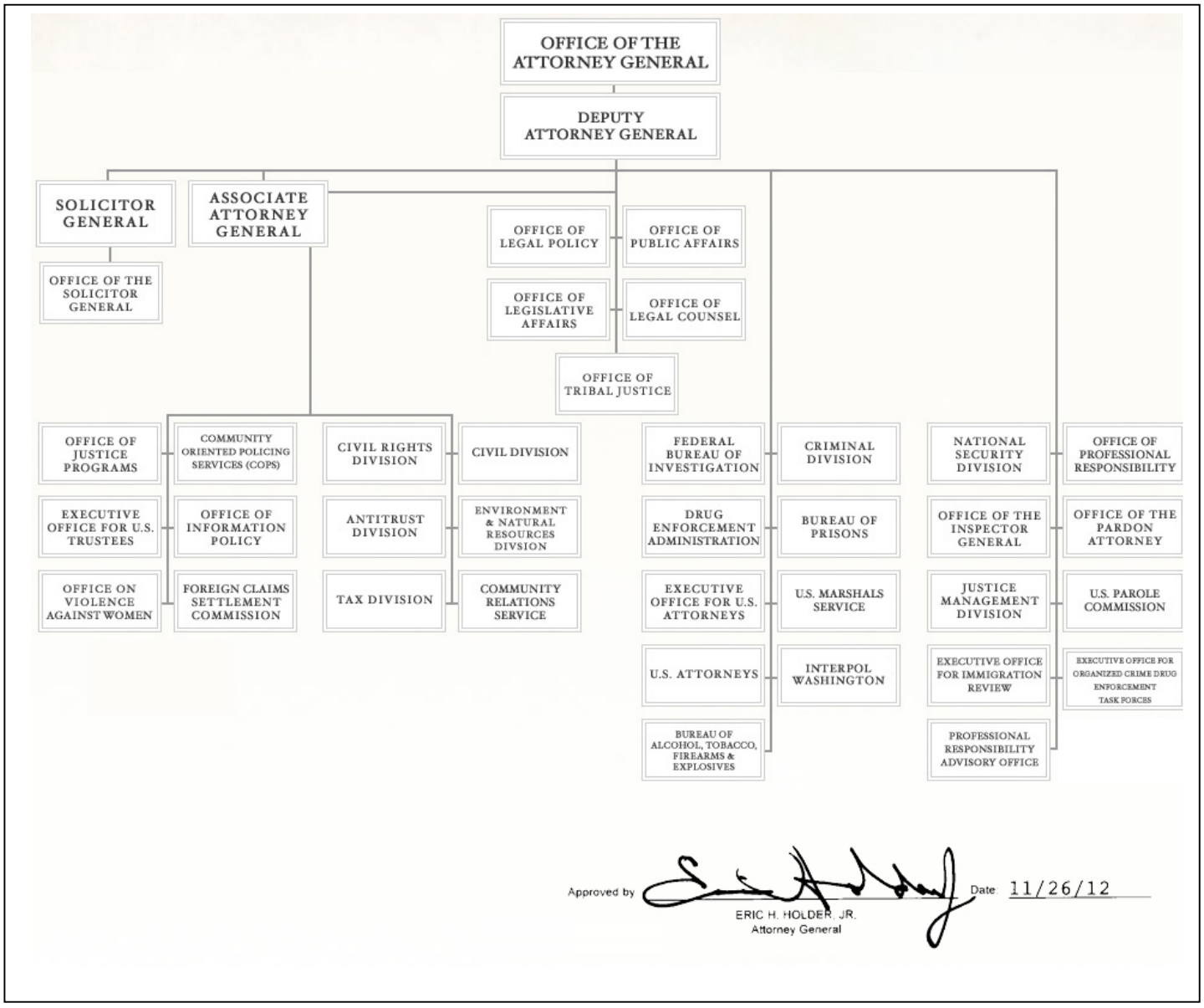
Honesty and Integrity. DOJ adheres to the highest standards of ethical behavior, cognizant that, as custodians of public safety, its motives and actions must be beyond reproach.

Commitment to Excellence. The Department seeks to provide the highest levels of service to the American people. DOJ is an effective and responsible steward of the taxpayers' dollars.

Respect for the Worth and Dignity of Each Human Being. Those who work for the Department treat each other and those they serve with fairness, dignity, and compassion. They value differences in people and ideas. They are committed to the well-being of employees and to providing opportunities for individual growth and development.

The Organization

Led by the Attorney General, the Department comprises approximately 40 separate component organizations. More than 114,000 employees ensure that the Department carries out the individual missions of its components. The Department's headquarters are in Washington, D.C., and it conducts most of its work in field locations throughout the country and overseas.


OFFICE OF THE ATTORNEY GENERAL
DEPUTY ATTORNEY GENERAL
SOLICITOR GENERAL
OFFICE OF THE SOLICITOR GENERAL
ASSOCIATE ATTORNEY GENERAL
OFFICE OF LEGAL POLICY
OFFICE OF PUBLIC AFFAIRS
OFFICE OF LEGISLATIVE AFFAIRS
OFFICE OF LEGAL COUNSEL
OFFICE OF TRIBAL JUSTICE
OFFICE OF JUSTICE PROGRAMS
COMMUNITY ORIENTED POLICING SERVICES (COPS)
CIVIL RIGHTS DIVISION
CIVIL DIVISION
EXECUTIVE OFFICE FOR U.S. TRUSTEES
OFFICE OF INFORMATION POLICY
ANTITRUST DIVISION
ENVIRONMENT & NATURAL RESOURCES DIVSION
OFFICE ON VIOLENCE AGAINST WOMEN
FOREIGN CLAIMS SETTLEMENT COMMISSION
TAX DIVISION
COMMUNITY RELATIONS SERVICE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL DIVISION
DRUG ENFORCEMENT ADMINISTRATION
BUREAU OF PRISONS
EXECUTIVE OFFICE FOR U.S. ATTORNEYS
U.S. MARSHALS SERVICE
U.S. ATTORNEYS
INTERPOL WASHINGTON
BUREAU OF ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES
NATIONAL SECURITY DIVISION
OFFICE OF PROFESSIONAL RESPONSIBILITY
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF THE PARDON ATTORNEY
JUSTICE MANAGEMENT DIVISION
U.S. PAROLE COMMISSION
EXECUTIVE OFFICE FOR IMMIGRATION REVIEW
EXECUTIVE OFFICE FOR ORGANIZED CRIME DRUG ENFORCEMENT TASK FORCES
PROFESSIONAL RESPONSIBILITY ADVISORY OFFICE
Approved by
Date: 11/26/12
ERIC H. HOLDER, JR.
Attorney General

The Structure of the *Plan*

The *Plan* is divided into five sections. The first introduces the *Plan* and provides background information. The second presents an overview of the major issues and trends that are driving DOJ's strategic goals and objectives. The third describes the goals and objectives that the Department will pursue over the next 5 years, along with the strategies to attain them. The fourth discusses the management principles that support the Department's mission and the President's goals. The fifth consists of Appendices, including the Department's performance measures, program evaluations, acronyms, and component websites.

The scope and complexity of the Department's mission make it impossible to describe in a single document the full range and content of the Department's programs and activities. Where appropriate, there are references to other plans and reports that provide more detailed information in specific areas. Also, some DOJ components have developed strategic plans that further describe their individual efforts to support the mission of the Department.

This *Plan* and links to components' websites and other plans are available at **www.justice.gov/**.

Statutory Compliance

The *Department of Justice Strategic Plan for Fiscal Years 2014-2018* is prepared pursuant to the requirements of the Government Performance and Results Modernization Act of 2010 (GPRMA). It updates and supersedes the *Strategic Plan* published by the Department of Justice in February 2012, covering fiscal years 2012-2016.

OIG Top Management and Performance Challenges Facing the Department of Justice – 2016

November 10, 2016

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 2016 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 nine challenges that we believe represent the most pressing concerns for the Department:

- Safeguarding National Security and Ensuring Privacy and Civil Liberties Protections
- Enhancing Cybersecurity in an Era of Increasing Threats
- Managing an Overcrowded Federal Prison System in an Era of Limited Budgets and Continuing Security Concerns
- Strengthening the Relationships Between Law Enforcement and Local Communities Through Partnership and Oversight
- Helping to Address Violent Crime Through Effective Management of Department Anti-Violence Programs
- Ensuring Effective Management and Oversight of Law Enforcement Programs and Promoting Public Trust
- Monitoring Department Contracts and Grants
- Managing Human Capital and Promoting Diversity With a Workforce Increasingly Eligible to Retire
- Using Performance-Based Management To Improve DOJ Programs

We believe safeguarding national security and enhancing cybersecurity in the wake of recent threats are particular challenges that will be at the forefront of the Department's attention and require vigilance in the foreseeable future. In addition, we have identified two of the challenges, helping to address violent crime and managing human capital while promoting diversity, as emerging issues that merit the Department's continued attention. Meeting all of these challenges will require the Department to develop innovative solutions and conduct careful monitoring of its efforts to achieve success.

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

Attachment.

This page intentionally left blank.

Safeguarding National Security and Ensuring Privacy and Civil Liberties Protections

Countering the Terrorist Threat

As reflected in the recent attacks in New York and New Jersey, San Bernardino, and Orlando, terrorism remains a serious threat to the national security of the United States. The Federal Bureau of Investigation (FBI) has described this threat as "persistent and acute," and it continues to be listed by the Department of Justice (Department) as its top priority. The challenge for the Department is to protect the homeland from this threat, while also safeguarding privacy and civil liberties. In its proposed Fiscal Year (FY) 2017 budget, the Department allocates $6.5 billion to prevent terrorism and promote national security, including counterterrorism and counterintelligence efforts.

Source: FBI website

According to the Department, the Islamic State of Iraq and the Levant (ISIL) is creating "an unprecedented threat environment." ISIL uses Internet and social media campaigns to promote its ideology and recruit like-minded extremists to become foreign fighters in Iraq and Syria or to attack the West from within. Attacks in the United States by so-called homegrown violent extremists (HVE) on civilian targets increased in 2016, many of them reportedly motivated by ISIL propaganda. According to a Joint Intelligence Bulletin issued by the FBI, the Department of Homeland Security (DHS), and the National Counterterrorism Center, 10 of the 13 attacks and disruptions by HVEs between August 2015 and August 2016 were focused on civilian targets, as compared to 2 of the 18 attacks and disruptions that took place in the first 7 months of 2015.

Countering terrorist radicalization and recruitment and identifying HVEs before they engage in terrorist acts remains an exceptional challenge. FBI Director Comey recently acknowledged the magnitude of the task when he observed, "We are looking for needles in a nationwide haystack, but we are also called upon to figure out which pieces of hay might someday become needles." He also noted that "untangling the motivation" of the assailants is a very real challenge. Indeed, the tragic incidents highlighted above illustrate that the FBI continues to face the same challenges in locating and stopping attacks by HVEs that it did prior to the Boston Marathon Bombings in April 2013. One of the Boston attackers, Tamerlan Tsarnaev, was the subject of an earlier FBI assessment that was closed with no nexus to terrorism and was not reopened following his travel to Dagestan in 2012. A coordinated review in 2014 by four OIGs of information sharing prior to the Boston Marathon Bombings concluded that the U.S. government had information regarding Tsarnaev's travel, and that the travel was significant and warranted further investigation. As with the Boston attacks, the more recent attacks by HVEs highlight the difficulty the FBI faces as it receives information

about people who may pose a threat and then must determine which information is credible and worthy of additional investigation, an inquiry FBI agents must perform in each of the thousands of assessments conducted each year.

The Department has noted that social media is a critical tool that terror groups can exploit in recruitment efforts for both homegrown and internationally directed terrorism. Engagement with the private sector is crucial to ensuring that the Department understands the latest social media and online communication tools and maintains the ability to lawfully access information transmitted through them. In January 2016, President Obama announced the creation of a counterterrorism task force to thwart terrorists' use of social media. As part of this effort, Attorney General Lynch, Director Comey, and senior intelligence officials met with representatives of various U.S. technology companies to discuss ways to identify and remove extremist online content. According to news reports, Twitter, Microsoft, and Google have since implemented or are experimenting with ways to prevent terrorists from using their systems to communicate with others. In August 2016, Twitter reported that since the middle of 2015, it had suspended 360,000 accounts for violating the prohibition on making violent threats and promoting terrorism.

Balancing Security and Transparency Amid Global Threats

The Department faces a growing challenge as it seeks to engage and share information with private sector technology companies because of concerns raised by these companies about the privacy implications of the Department's requests for assistance. In some instances, these concerns have led to legal challenges. For example, as described in additional detail in the section on Cybersecurity, the recent dispute between the Department and Apple over obtaining access to information from the iPhone used by one of the San Bernardino attackers, highlights the challenge of obtaining investigative information from terrorists who communicate using encryption while protecting the privacy interests of law-abiding individuals. In another instance, Twitter recently sought to publish the number of secret orders it received from the government that required the company to turn over its customers' information, claiming that government-imposed restrictions on disclosing this information violated the company's First Amendment rights.

The disputes with Apple and Twitter, as well as the public debate about the appropriate scope of government surveillance, have highlighted the tension between security and transparency. The former Director of the National Security Agency, General Michael Hayden, explained the need to balance these considerations in this way: the federal government must provide the American people enough transparency to ensure that they understand what the government does to keep them safe without divulging so much information that it would hinder the government's ability to keep them safe.

The Office of the Inspector General's (OIG) oversight of the Department's counterterrorism efforts is intended to provide both transparency and accountability so that the public and policymakers can assess whether the Department is appropriately balancing privacy and security interests, and whether it is collecting and handling information in a manner that complies with federal law. For example, on June 2, 2016, the OIG submitted to Congress a classified version of a report on the FBI's use of Section 215 orders under the *Foreign Intelligence Surveillance Act* between 2012 and 2014, and its handling of non-publicly available information concerning U.S. persons received in response to these orders. An unclassified version of the report was released in September 2016. The report concluded that the process used by the FBI to obtain business records orders contained safeguards that protected U.S. persons from unauthorized collection, retention, and dissemination of information about them.

The Department's sharing of terrorist threat information and coordination of its operations with other entities involved in counterterrorism activities across the federal government also continue to be a focus of the OIG's oversight work. For example, as noted above, our office participated in a joint review with three other OIGs

of information sharing prior to the Boston Marathon Bombings. We currently are conducting a joint review with the Inspectors General of the Intelligence Community (IC) and DHS that focuses on the domestic sharing of counterterrorism information. This review will identify and examine the federally supported field-based intelligence entities engaged in counterterrorism information sharing to determine their overall missions, specific functions, capabilities, funding, and personnel and facility costs. The review also will determine whether counterterrorism information is being adequately and appropriately shared with all participating agencies and will identify any gaps and/or duplication of effort among the entities.


Source: OIG

Additionally, the OIG is conducting a review of the handling of known or suspected terrorists (KST) admitted into the federal Witness Security (WITSEC) Program. The review will examine practices for watchlisting and processing encounters with KSTs participating in the WITSEC program, and procedures for mitigating risks to the public through restrictions placed on this high-risk group of program participants. This is a follow-up review to our 2013 report, which found that the Department did not authorize the disclosure to the Terrorist Screening Center of new identities provided to KSTs and their dependents who were admitted into the WITSEC Program. This potentially allowed KSTs to use their new government-issued identities to fly on commercial airplanes and evade one of the government's primary means of identifying and tracking terrorists' movements and actions. Separately, the OIG has initiated a review of the FBI's efforts to protect seaports and maritime activity. That review is examining the FBI's roles and responsibilities for assessing maritime terrorism threats, preventing and responding to maritime terrorist incidents, and coordinating with DHS components to ensure seaport security.

The Department also faces a continuing challenge in countering the threat to the United States from foreign governments. For example, in August 2016, an FBI employee pled guilty to acting as an agent of China for providing restricted and sensitive FBI information to the Chinese government. Moreover, as we note in the Cybersecurity section of this report, recently DHS and the Office of the Director of National Intelligence identified Russia as directing a campaign of attacks intended to interfere with the U.S. election process. These examples highlight the importance of the Department remaining vigilant in its counterintelligence efforts against foreign adversaries to protect the nation's security.

Leveraging Emerging Technologies While Safeguarding Privacy

Concerns about the appropriate balance between security and privacy also will arise as the Department determines how to leverage emerging technologies that provide law enforcement with valuable information, such as geolocation or facial recognition technologies, while ensuring that the technology is used responsibly and lawfully. In 2013, the OIG released an interim report on the Department's use of Unmanned Aircraft Systems (UAS), or drones, in law enforcement operations and issued a final report in March 2015. The interim report found that in light of the technological capabilities of UAS, especially those raising unique privacy and evidentiary concerns, the Department should develop UAS-specific policies to guide the law enforcement components' use of this technology. In May 2015, the Department established policy guidance on the use of UAS, including privacy and civil liberties protections. Separately, in September 2015, the Department issued a new policy for the use of cell-site simulators that requires, among other things, that law enforcement agents obtain a search warrant before deploying the devices.

The effects of technology on Department operations were highlighted earlier this year when a senior Department official testified about the legal standards used by the Department to obtain various types of geolocation information. This official pledged that the Department is dedicated to ensuring that its policies and practices comply with applicable laws and uphold the Department's long-standing commitment to individuals' privacy and civil liberties. Continued oversight is required to ensure that the Department adheres to this commitment. For example, a report issued in May 2016 by the Government Accountability Office (GAO) found that although the Department has an oversight structure in place to help ensure the privacy of facial recognition data, the FBI did not update privacy guidelines for the system until 3 years after it began conducting facial recognition searches, and did not conduct sufficient testing to ensure the accuracy of search results. Given the sensitivity of biometric and geolocation data, and the proliferation of devices capable of capturing this type of information, the Department will need to ensure that its policies continue to evolve appropriately with technology.

Safeguarding national security must continue to be a top priority for the Department, and balancing this mandate with ensuring appropriate protection of privacy and civil liberties will continue to be a challenge. The Department has acknowledged that the challenges raised by modern technology are complex and that the agency will need to remain agile to address them. As both threats and technology evolve, the Department must continually reevaluate its national security efforts in order to appropriately safeguard the interests of the homeland and U.S. citizens.

Enhancing Cybersecurity in an Era of Increasing Threats

The cyber threat to the nation is growing and cyber intrusions are becoming increasingly commonplace, dangerous, and sophisticated. The FBI has stated that it continues to see an increase in the scale and scope of malicious cyber activity as measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, and remediation costs incurred by victims. In order to protect the homeland in the digital age, the Department must continue to prioritize addressing these evolving cyber threats. Recent high profile cyber breaches, including those that reportedly may even have the potential to impact voting systems, demonstrate the importance of the Department remaining vigilant in combating cyber threats. Key to the Department's efforts will be its success in developing and maintaining a capability to identify the individuals or organizations responsible for intrusions. Challenges in this regard include the expanded use of encryption that can limit law enforcement from gaining access to critical investigative information and the recruitment and retention of technically-trained, highly-skilled cyber professionals to support the Department's cybersecurity mission. The Department must also take steps to guard against loss of data on its own computer systems. To this end, the Department's FY 2017 budget request provides $900 million to defend and protect Department networks, mitigate insider threats, investigate and prosecute criminal and terrorist cyber activity, and guard against identity and intellectual property theft and financial fraud, including a $175 million increase for FBI cyber investigation investments.

Strengthening the Nation Against Cyber Intrusions

Source: FBI website

Cyber intrusions that threaten the nation's security are among the highest priority matters investigated by the Department. One of the challenges for the Department in this area is detecting and deterring cyber intrusions before they occur rather than reacting to them after they have succeeded. Among the most dangerous cyberattacks are intrusions directed toward our national security, intellectual property, and democratic system by nation-states, nation-state sponsored hackers, global cyber syndicates, and so-called "botnets." According to FBI Director Comey, China, Russia, Iran, and North Korea present the most prominent nation-state cyber threats. As recently as October 2016, DHS and the Office of the Director of National Intelligence identified Russia as directing a campaign of attacks intended to interfere with the U.S. election process, with the goal of stealing and disclosing information intended to interfere with that process. This highlights the very serious potential consequences of a successful cyberattack. The stakes are high and, in an environment where actors are rapidly changing their tactics and techniques, the Department must ensure it remains agile in responding to cyber threats.

Given that the cyber threat is multi-faceted, the Department must continue to develop relationships with the private sector, state and local law enforcement, and global partners to effectively combat cyber threats. The frequency and impact of cyberattacks on the nation's private sector networks have increased dramatically in the past decade and are expected to continue to grow, making such partnerships between the public and

private sectors critically important. The *Cybersecurity Information Sharing Act of 2015* is intended to encourage companies to voluntarily share information about cyber threat indicators with federal, state, and local governments, as well as other private entities. However, as Director Comey observed in August 2016, it can be difficult to get the private sector to report system breaches to law enforcement. Sharing cyber incidents with the government (or other organizations) can expose a private company's network vulnerabilities and bring negative publicity, as well as create negative repercussions for multinational organizations that seek to do business in the very countries that may be sponsoring the cyberattacks.

Source: FBI website

The Department also faces challenges protecting its own systems. In response to the Office of Personnel Management (OPM) data breach in June 2015, the Department implemented various solutions to strengthen network security. This did not, however, prevent the February 2016 breach of Department data that exposed the contact information of 20,000 FBI employees. This "social engineering attack" was reportedly accomplished by a hacker posing as an employee to break into networks used by the Department's Civil Division by tricking staffers at an IT help desk into disclosing critical information. Department employees—the end users on the government's computer systems—are the first line of defense against cyberattacks of this type and the Department must continue to increase its security awareness in order to help thwart such threats.

Insider threats pose yet another cyber challenge to the Department. For example, as devices and technology become increasingly portable and outsourced, the Department's ability to detect and deter improper or unlawful activity by its employees will continue to be tested. President Obama signed an executive order in October 2011 requiring federal agencies to establish an insider threat detection and prevention program for their classified information. In accordance with this directive, the Department established such a program designed to detect patterns and indicators of insider threats. The OIG is currently examining the FBI's Insider Threat program to evaluate its ability to deter, detect, and mitigate insider threats. While the Department must be vigilant to detect insider threats, it must be careful not to allow such efforts to chill whistleblowers, who perform an important service to the Department and the public when they come forward with information regarding what they reasonably believe to be wrongdoing or mismanagement.

Unlocking Encrypted Messages to Fight Crime and Terrorism

Director Comey has stated that the growing use of encryption, which shields communications from all but those sending and receiving the messages, is one of the most pressing problems for law enforcement. As technology continues to evolve, the Department has sought to have the tools and methods it says it needs to gather evidence on terrorists and criminals who are increasingly using technology to hide their actions from law enforcement. For example, the FBI and others in law enforcement have said that investigations have stalled because of unlockable electronic devices. The FBI stated that in the first 10 months of FY 2016, it was unable to unlock 650 of 5,000 electronic devices investigators attempted to search. To address this challenge, the Department has requested $38 million for anti-encryption technology and research as part of its FY 2017 budget request. This issue recently attracted substantial public attention during the Department's legal battle to compel Apple to create special software to unlock the phone of one of the alleged terrorists

involved in the San Bernardino shooting. Department attorneys argued before a federal judge that law enforcement should be permitted to obtain an order requiring Apple to assist them with their investigation; attorneys for the company argued in response that, among other things, developing such a "back door" would have the effect of violating the privacy expectations of its customers and leave consumers vulnerable to hackers if the decryption tool fell into the wrong hands. The FBI successfully unlocked the San Bernardino phone with the assistance of a third party before the court rendered a decision in the dispute with Apple, but the broader issue and challenge remain.

The darknet presents another challenge for the Department in identifying criminals acting in an anonymous environment of increasing sophistication. The darknet is a part of the Internet that uses techniques, including special network configurations and encryption, allowing users to communicate anonymously. The darknet offers those attempting to evade law enforcement a means in which to commit a wide range of cybercrimes. These crimes can include hacking into non-authorized systems, disabling websites, or disseminating ransomware, which is malicious software used to lock the computer of an unsuspecting website visitor and require them to pay ransom to have their computer unlocked. The darknet can also shield individuals engaging in other criminal activities, such as child pornography and narcotics trafficking. It is difficult for law enforcement to identify individuals committing crimes using the darknet because they often use crypto-currencies such as Bitcoins, which allow users to remain anonymous. Although the FBI had success shutting down the Silk Road, a well-known darknet market for contraband, a successor darknet market reportedly soon replaced it, illustrating how important it will be for the Department to adjust to rapidly changing cyber environments.

Hiring Highly-Skilled Cyber Professionals

Attracting highly-skilled, technically-trained cyber professionals is a persistent challenge for the Department. Cyber professionals are in high demand in the private sector, potentially putting the government at a competitive disadvantage when it comes to recruiting these individuals. The FBI has noted that the significant salary gap between public and private sector positions can deter individuals from applying for jobs in the federal government and that many applicants are unable to pass the rigorous background investigation the FBI conducts on all potential employees. The pay gap and background screening issue have left the FBI often understaffed in this critical area. As we noted in a March 2016 report about an FBI computer forensic laboratory in New Jersey, the lack of qualified examiners with advanced training was a primary cause of the backlog of cases. It is imperative that the Department continue to develop new and creative hiring and retention strategies to attract highly skilled cyber professionals.

As the frequency and impact of cyber intrusions continue to increase and the nature of the attacks continues to change, the Department will be challenged to shift more of its efforts from reacting to attacks to preventing them. The Department must continue to prioritize resources to anticipate and prevent cyber intrusions, identify and investigate cyber actors before they strike, and engage with private sector partners and others in state and local law enforcement and abroad to accomplish this. And, while looking outward to protect from the cyber threat, the Department must also continue to focus on ensuring the security of its own computer systems and data. The Department must also marshal resources to address the impact of encryption, while at the same time recognizing and protecting civil rights and civil liberties. Finally, the Department faces the daunting challenge of creatively recruiting highly skilled cyber professionals to address these concerns.

Managing an Overcrowded Federal Prison System in an Era of Limited Budgets and Continuing Security Concerns

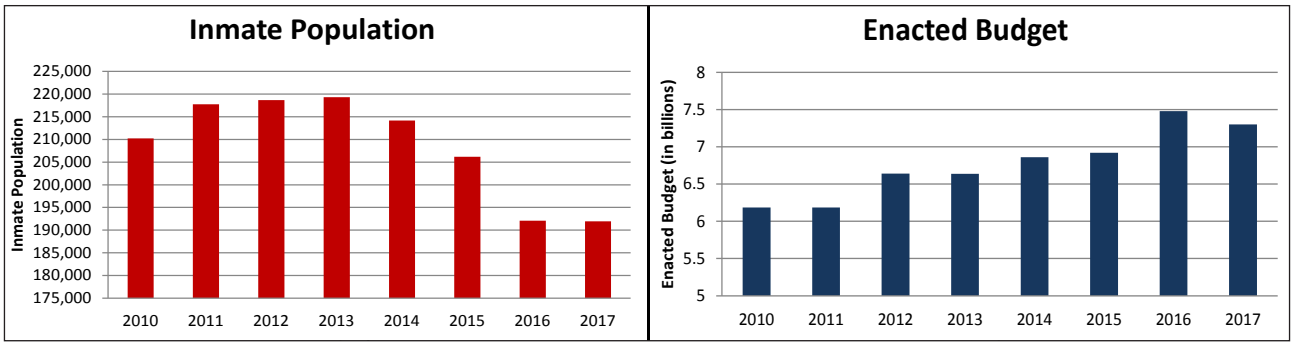
Confining offenders in prisons and community-based facilities that are safe and humane, while controlling costs and the size of the inmate population, is the constant challenge faced by the Federal Bureau of Prisons (BOP). While the inmate population has dropped 3 years in a row, falling to 192,170 at the end of FY 2016, overcrowding remains a challenge. As of September 30, 2016, BOP's institutions remained 16 percent over rated capacity, and high security institutions were 31 percent over rated capacity. This is a significant concern because more than 90 percent of high security inmates have a history of violence. The BOP's strategic plan says its goal is to achieve an overall overcrowding level "in the range of 15 percent." Thus, the Department continues to face a multi-faceted crisis in the federal prison system—addressing overcrowding while controlling spending and meeting the increasing resource needs of a changing inmate population.

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 continue to look for ways to contain costs. For the first time in recent years, the BOP has requested fewer funds for the FY 2017 budget—$7.3 billion—than the current funding level of $7.48 billion. Despite this, the BOP currently has the largest budget of any Department component other than the FBI, accounting for more than 25 percent of the Department's discretionary budget in FY 2016. Moreover, the cost of the prison system remains well above the $6.2 billion level of spending in FY 2010. Department spending on the federal prison system impacts its ability to fund other important Department operations, such as its critical law enforcement and national security missions. As such, it is imperative that the Department manage the prison system in the most cost-efficient manner possible.

Source: DOJ

To accomplish this, the Department must consider innovative solutions to contain costs. For example, inmate medical care continues to be a major part of BOP's overall spending, and is an area that needs to be monitored closely. From FY 2010 to FY 2014, BOP spending for outside medical services increased 24 percent, from $263 million to $327 million. A June 2016 OIG report found these rising costs were due, in part, to BOP being the only federal agency that pays for medical care without being able to rely on a federal statute or regulation that could limit BOP's reimbursement rates to those set by Medicare. In addition to rising medical costs, the BOP also is facing medical staffing shortages, as described in a March 2016 OIG report, which found that recruitment of medical professionals was one of the BOP's greatest challenges and that staffing shortages (a) limit inmate access to medical care, (b) result in an increased need to send inmates outside the institution for medical care, (c) contribute to increases in medical costs, and (d) can also impact prison safety and security.



Source: OIG

The Department must also take additional steps to ensure that it releases inmates when their sentences are complete. In a May 2016 OIG report, we found that of the 461,966 inmates released between 2009 and 2014, the BOP released 152 inmates from prison too late and 5 prisoners too early as a result to staff error. Being released late from prison is unjust and raises serious civil liberties concerns. Moreover, in addition to the enormous personal costs to inmates, these errors can result in additional litigation, settlement, and imprisonment costs, all borne by taxpayers.

Ensuring the Security of Inmates, Staff, and the General Public

The Department must continue its efforts to ensure the safety and security of staff, inmates, and the general public in federal prisons. In this regard, the smuggling of contraband into federal prisons remains a serious and significant problem, and addressing it must remain a high priority for the BOP. Preventing the physical and sexual abuse of inmates is also a critical safety responsibility for the Department, the role of which was expanded by the *Prison Rape Elimination Act of 2003*. Our Investigations Division continues to investigate allegations of contraband smuggling, bribery, and physical and sexual abuse of inmates by BOP employees. In FY 2016, these types of allegations resulted in 79 BOP employees receiving administrative sanctions or resigning while under investigation, and 50 BOP employees being convicted criminally.

In June 2016, the OIG evaluated BOP's contraband interdiction efforts and highlighted several areas the BOP must address in order to better tackle this problem. For example, our review found that the BOP's staff search policy lacks comprehensiveness to effectively deter staff from introducing contraband, which continues to pose a security concern to inmates, staff, and the public. From FYs 2012 to 2014, the BOP reported recovering over 21,000 contraband items in its institutions, including cell phones (the most common), narcotics, weapons, and tobacco. Another area of concern is BOP's operation of its armories, where prisons store emergency equipment such as firearms, ammunition, and other defensive gear. In a March 2016 report, we found weaknesses in BOP's armory controls that increased the risk that critical equipment could be lost, misplaced, or stolen. BOP needs to tighten these controls to reduce the risk of munitions and equipment falling into the wrong hands.

The Department faces similar challenges ensuring safety and security at its private or contract prisons. An August 2016 OIG report found that these prisons, which house mostly low security foreign national inmates, incurred more safety and security incidents per capita in a majority of the key categories we examined than comparable BOP institutions housing low security inmates. For example, in addition to a contraband seizure rate 8 times higher than that of BOP-run institutions, contract prisons also experienced higher rates of assaults both by inmates on staff and vice versa. The week after our report was issued, the Department announced it intends to phase out the use of contract prisons by either declining to renew current prison contracts or working to "substantially reduce" the scope of existing contracts. As efforts to phase out the use of contract prisons move forward, the Department will need to carefully manage the inmate population to ensure that it does not exacerbate overcrowding in BOP-run institutions.

Managing Department Programs That Also Can Impact Inmate Population Numbers

Further compounding BOP's challenge to ensuring inmate safety and security is the continued overcrowding of the federal prison system. This problem cannot be addressed by the BOP alone, given that it has little control over the number of inmates it is charged with safely housing. Rather, multiple Department-level efforts may impact the overcrowding and cost concerns facing the federal prison system. In August 2013, the Department launched its Smart on Crime initiative with the goal of reforming the federal criminal justice system by, among other things, curbing reliance on incarceration for less dangerous offenders. Proposed reforms include requiring U.S. Attorneys' Offices (USAO) to modify their guidelines for when federal prosecutions should be brought, limiting the use of mandatory minimums and enhancements for repeat low-level, non-violent drug defendants, and enhancing prevention and reentry efforts at each USAO. In December 2015, the OIG initiated a review of the Department's implementation of certain principles regarding prosecution and sentencing reform it announced in its Smart on Crime initiative.

Source: DOJ

As part of Smart on Crime, federal prosecutors are encouraged to consider alternatives to incarceration, such as pretrial diversion and diversion-based court programs, in appropriate cases involving non-violent offenders. In July 2016, the OIG released an audit that found the Department cannot fully measure the success of its diversion programs because neither the Executive Office for United States Attorneys (EOUSA) nor the USAOs are adequately tracking this information. Furthermore, we found a wide disparity between how often these programs are used by different USAOs. For example, while one district diverted as many as 326 defendants, other districts diverted none. In line with the OIG's findings, the GAO echoed the same concerns in its own June 2016 report on the Department's use of alternatives to incarceration. Mirroring our findings, the GAO report also suggested that the Department would benefit if it could better measure the success of its different pretrial diversion programs.

Another area where the Department can make strides is by improving how the BOP prepares inmates for release into the community. During the past 3 years, the BOP has released nearly 125,000 federal inmates into residential reentry centers, home confinement, or directly into communities. Although the BOP invests a considerable amount of money each year into its reentry programs and requires that most sentenced inmates participate in its Release Preparation Program (RPP), the OIG found in an August 2016 review that it has no performance metrics to determine whether its RPPs are successful. In fact, the last BOP study on the overall recidivism rate for federal inmates occurred more than 20 years ago. The BOP must begin measuring both the overall recidivism rate for federal inmates, as well as how successful each prison has been in preparing inmates for release, so the Department can better determine which facilities and programs deserve to be funded and expanded, and which programs should be ended. The good news is the BOP told us it is currently working on a study to fill this knowledge gap and that, for the first time since 1994, it aims to release recidivism rates in FY 2017.

Although the Department makes clear that its Clemency Initiative, announced in April 2014, is not intended as a means to reduce the number of inmates, grants of clemency have an effect on the inmate population. As conceived, the Department said it would prioritize clemency applications for non-violent, low-level offenders. In February 2016, the OIG initiated a review of the Department's handling of the executive clemency process, with an emphasis on assessing the procedures followed by the Department and the impact

of the Department's new criteria for prioritizing commutation petitions. While our review is ongoing, the number of inmates granted clemency by the President has increased significantly this past fiscal year, with 95 inmates granted clemency in March, 58 inmates in May, 42 inmates in June, and another 325 in August. As FY 2016 came to a close, the President had commuted 583 sentences, compared to 79 the year before.

Another program that has the potential to impact the prison population is the Department's Compassionate Release Program. In August 2013, the BOP announced, as part of the Smart on Crime initiative, that it was expanding its criteria for inmates seeking compassionate release to include elderly inmates. This change allowed inmates age 65 and older, of which there were 4,384 in BOP custody at the time, to request a reduction in sentence if they meet certain criteria. However, our subsequent report on the BOP's aging inmate population, released in May 2015, found that during the first year the new BOP policy was implemented only 2 of the 348 inmates who applied were released under the new provisions. While the number of inmates released under these provisions in FY 2015 increased, in FY 2016 the BOP released only 5 inmates, despite a 65-percent increase in applications. In February 2016, the Inspector General appeared before the U.S. Sentencing Commission and highlighted the concerns we expressed in our report about the age and time served requirements. The Commission adopted significant changes to the U.S. Sentencing Guidelines addressing these issues in April 2016. We will continue monitoring the program to determine whether these changes lead to more use of compassionate release for appropriate inmates.

Another Congressionally-authorized program that could impact the federal inmate population if managed successfully is the International Prisoner Transfer Program, which allows the Department to transfer foreign inmates to their host nations to serve their prison sentence. In an August 2015 status report, the OIG found that the number of inmates transferred under the program had actually decreased since our prior report in 2011, despite a substantial increase in the number of inmates applying for such transfers. Using FY 2013 BOP annual cost data, we found that BOP could potentially save $4.5 million by transferring just 1 percent of inmates who applied and were ultimately transferred. The OIG's status report recommended that Department leadership boost the effectiveness of this program by actively engaging with treaty transfer partners, and the Department has since taken some steps to encourage treaty nations to accept more inmates. Yet, despite its efforts, over the past 3 years the number of foreign nationals transferred to treaty nations has sharply declined. In fact, since FY 2014, the Department has transferred just 436 inmates (averaging 145 inmates per year), its lowest total in more than a decade, down from the 227 per year average between FY 2011 and FY 2013.

The operation of the federal prison system presents a host of continuing challenges for the Department. While it has taken positive steps in some areas, such as its plan to determine and release recidivism rates that will help it evaluate the efficacy of its programs, there is still substantial progress to be made. Indeed, BOP will need to make progress on a number of fronts if it is to achieve its mission of confining offenders in "prisons and community-based facilities that are safe, humane, cost-efficient, and appropriately secure, and that provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens."

Strengthening the Relationships Between Law Enforcement and Local Communities Through Partnership and Oversight

Recent shootings by, and of, local law enforcement officers have raised serious questions about the relationship between law enforcement and the communities they serve. As Attorney General Lynch recently observed, the loss of life among civilians and law enforcement, "brings pain not just to individual communities, but to our entire nation." The Department's burden continues to be to determine how best to assist in solving a problem that manifests itself locally, yet has an indisputable effect on the Department, federal law enforcement, and the country as a whole. There are at least five ways where the Department plays a critical role in this area: (a) creating an effective data collection system to accurately understand police use of deadly force; (b) partnering with state and local governments, and local law enforcement agencies, through grants programs; (c) monitoring and assisting with the reform of police departments that are found to have engaged in a pattern or practice of unlawful or unconstitutional misconduct; (d) investigating and prosecuting law enforcement officers, whether local, state, or federal, who violate federal civil rights laws; and (e) assisting in the response to civic unrest as needed when an incident of police-community violence does occur. The challenge for the Department is how to address these areas when it has limited resources to use, limited jurisdiction upon which to act, and limited impact over local crime fighting.

Compiling Accurate and Complete Data on Law Enforcement Shootings

Source: OJP website

For government decision-makers and the public to better understand the issues raised by law enforcement shootings, there needs to be data that adequately measures the nature and scope of the issue. The *Violent Crime Control and Law Enforcement Act of 1994* requires the Department to collect "data about the use of excessive force by law enforcement officers" and issue an annual report regarding such data. In addition, pursuant to the Death in Custody Reporting Act, state and local law enforcement agencies face grant funding reductions if they do not report to the Department information regarding the death of any person while in law enforcement custody, including while under arrest. Nonetheless, the Department has historically struggled to collect adequate data regarding officer-involved shootings and excessive use of force by law enforcement officers, because state and local law enforcement agencies are not legally required to provide such data to the federal government. Thus, FBI Director Comey has emphasized that the Department needs "more and better information," including better data "related to officer-involved shootings...and attacks against law enforcement officers," which he said would help inform the "passionate, important conversations" we are having "in this country about police use of force."

In October 2016 Attorney General Lynch announced that the Department has taken several steps toward improving its collection of this critical data. These include: (a) the FBI's partnership with local, state, tribal, and federal law enforcement to create a National Use-of-Force Data Collection Program, which is expected to be piloted in early 2017 and include data regarding instances where a law enforcement officer discharges a firearm at a person as well as instances where the use of force results in death or serious bodily

injury; (b) the Bureau of Justice Statistics issuance of a draft proposal outlining its plan for collecting death-in-custody data from state and local law enforcement agencies; (c) the Attorney General's issuance of a memorandum to federal law enforcement agencies notifying them of their obligation to comply with the *Death in Custody Reporting Act*, beginning with FY 2016 data; and (4) the creation of a new Office of Community Oriented Policing Services (COPS)-administered Police Data Initiative that will collect and publicly release data from law enforcement agencies regarding stops and searches, uses of force, and officer-involved shootings.

The Department's challenge will be to collect and organize the data collected through each of these efforts to improve the nation's understanding of this problem, and to help local, state and federal law enforcement search for creative solutions based on this information. In that regard, complete, timely, and reliable data is essential so that the nation may have informed policy discussions about this subject.

Using Grants To Assist Local Law Enforcement With Hiring, Equipment and Training

One of the Department's greatest challenges is to figure out what state and local efforts to support and how to best do so with its limited resources. The primary method it has relied on to date is to partner with state and local law enforcement by offering grants for hiring, equipment, training, research, and other efforts to assist them and improve police-community relations. By offering grants to local communities from COPS, Office of Justice Programs (OJP), and Office on Violence Against Women (OVW), the Department has the potential to provide important assistance to local law enforcement. For example, the COPS Hiring Program recently announced $119 million for hiring community policing officers. This year's grants mark over $14 billion to advance community policing since 1995, with approximately 129,000 police positions funded. The challenge for the Department is to ensure that its grant funds are wisely spent and promote sustainable and effective initiatives so as to maximize the impact in assisting communities in preventing violence between police and communities.

Source: COPS website

Body cameras used by state and local law enforcement have the potential to assist in furthering transparency and accountability in encounters between citizens and the police. Last year OJP awarded nearly $20 million to law enforcement agencies in 32 states through the *2016 Body-Worn Camera Policy and Implementation Program*. Through such programs, we believe the Department should continue working to ensure that its limited grant funding is being used to support positive reforms in local policing.

Another challenge for the Department is to look for ways to help local law enforcement standardize its training and practices to aid with the safe and effective fulfillment of their responsibilities, strengthen professionalism, and thereby enhance the ability to reduce community tensions. Both OJP and COPS have developed technical assistance programs that target improving police department practices and community relations. Specifically, OJP's Diagnostic Center provides systems analysis and recommendations related to improving or deploying data to drive justice reform, such as assessing early intervention systems to improve officer accountability. Under the Collaborative Reform Initiative, COPS provides a more comprehensive assessment of requesting police departments' operations to identify issues that may affect public trust, including use of force practices, and issues public recommendations consistent with best practices in policing. A similar but separate COPS effort, the Critical Response Technical Assistance program, offers

a more focused assessment of how police departments handle procedures related to particular high-profile events and incidents or sensitive issues. And lastly, the Department has announced its intention, as part of some training grants, as well as through internal training for the four federal law enforcement components and Department attorneys, to address the issue of implicit bias at all levels in the justice system. To multiply the effect of its prevention dollars, the Department might consider providing grants for law enforcement agencies to obtain accreditation through recognized providers to supplement efforts to increase professionalism and improve community relations. Such an initiative may fit with the recent efforts at direct outreach by Attorney General Lynch during her nationwide community policing tour.

Providing Oversight through Pattern or Practice Investigations

While it seeks ways to assist local police departments through its grants, the Department also plays a critical oversight role through its Civil Rights Division (CRT) in ensuring that police departments act in accordance with the Constitution and federal statutes. CRT investigates law enforcement agencies across the nation to address allegations of excessive force; unlawful stops, searches, or arrests; and discriminatory policing. Under the *Violent Crime Control and Law Enforcement Act of 1994*, it is unlawful for law enforcement officers to engage in a pattern or practice of conduct that deprives individuals of rights protected by the Constitution or federal statutes, and the Department may initiate a civil action when it has reasonable cause to believe that such conduct has taken place. Thus, under 42 U.S.C. § 14141, CRT conducts "pattern or practice" investigations through which it endeavors to address local issues and create models for effective and constitutional policing nationwide. With approximately 18,000 state and local law enforcement agencies throughout the country, however, the challenge for CRT is to identify where and how it can best target Departmental attention and resources to maximize its impact. In the past 7 years CRT has opened "pattern or practice" investigations on 23 police departments across the country, and is currently enforcing 17 agreements with law enforcement agencies, including 14 consent decrees and one post-judgment order. The OIG is currently conducting an audit of CRT's efforts to address patterns or practices of police misconduct, including how CRT identifies and selects matters for investigation, the role of the Department's grant programs in addressing or preventing such conduct, and how these efforts are coordinated.

The challenge for CRT is to be able to select and conduct investigations and enforce resulting consent decrees in ways that effectively address unconstitutional practices, ensure accountability, and increase community confidence in both local law enforcement departments with high-profile problems and those with less well known issues. Further, transparency in the CRT process can assist other local law enforcement entities in assessing and improving their own operations.

Investigating and Prosecuting Violations of Federal Civil Rights Laws

In addition to helping reform troubled police agencies through grants and oversight, the Department, through CRT's Criminal Section and USAOs around the country, also prosecutes law enforcement officers for violating individuals' civil rights. During the last 8 years, the Department has charged more than 480 defendants, most of whom were local, state, and federal law enforcement officers, with committing willful violations of constitutional rights under color of law and related offenses. Here, too, the Department must determine how to best use its limited resources in what are resource-intensive cases. In doing so, the Department must carefully consider where federal investigation and prosecution is appropriate, taking into account local conditions and interests and the state or local jurisdiction's ability and willingness to prosecute effectively, as laid out in United States Attorneys' Manual Title 9-27.240. The challenge for the Department then is to determine when federal intervention is warranted in these difficult and often high-profile cases.

Providing Support To Communities in Emergency Situations

Source: CRS website

Finally, if prevention fails and civic unrest directed at local law enforcement threatens or begins to unfold, the Department faces the challenge of effectively using its limited resources to provide conciliation services and to ensure they are effective in addressing difficult local situations. The Department's Community Relations Service (CRS), created by the *Civil Rights Act of 1964*, is authorized to provide emergency response support through the deployment of conciliators to affected communities. As CRS's Strategic Plan notes, "timing is essential in preventing community tensions from erupting into violence." However, CRS is a relatively small Department component, with a staff allocation of 74 employees, 28 positions currently unfilled, and a budget of $14.5 million in FY 16. Ensuring appropriate and effective deployment of these limited resources, at a time when numerous communities are facing these issues, is an important challenge for the Department.

Ultimately, the Department must work through all these critical issues to determine how to optimally use its limited but substantial resources and personnel to help improve the relationship between law enforcement and the public they serve. Through effective data collection tools, efficient and effective use of grant programs, oversight through pattern or practice investigations and criminal prosecutions where warranted, and response support when needed, the Department can act in multiple ways to strengthen relationships among law enforcement and the communities they serve. These efforts, if successful, can maximize the safety of citizens while protecting the Constitutional rights guaranteed to all Americans.

Helping to Address Violent Crime Through Effective Management of Department Anti-Violence Programs

While state and local law enforcement has primary responsibility for addressing street crime, including in responding to the increases in violent crime that certain communities in our nation are facing, the Department plays an important role in those efforts. Indeed, the Department's strategic plan identifies combating violent crime as one of four "priority goals" and the Department has a number of initiatives underway to accomplish this. These include law enforcement efforts by the Department's law enforcement components and USAOs; technical assistance to state, local, and tribal governments by law enforcement and grant-making components; and grant funding for a wide array of violence-related issues and programs through OJP, OVW, and COPS. For example, the FBI operates more than 160 Safe Streets Task Forces that partner with state and local law enforcement to investigate gang and drug-related violent crime, and the Bureau of Justice Assistance has created the Violence Reduction Network, which is designed to provide enhanced technical assistance and other services to select cities that are addressing serious problems with violent crime. In addition, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) has made addressing violent crime a leading priority and has established task forces focused on gang and firearms-related violence. The Department also has placed increased emphasis on violence prevention and reentry programs through its "Smart on Crime" initiative.

Source: OJP website

The United States as a whole currently is enjoying some of the lowest reported rates of crime and violent crime in decades, with the overall crime rate reported by the FBI for 2015 roughly half of what it was in 1990. Unfortunately, despite such reductions in nationwide reported crime rates, many neighborhoods remain plagued by violence. Areas within localities such as Baltimore, Chicago, Detroit, East St. Louis, and Flint continue to face the problem of entrenched violence, each with reported rates of crime that are many multiples of the national average. Overall, the reported murder rate rose nearly 11 percent nationally in 2015. But in some cities the increases were far more dramatic, such as Baltimore which experienced nearly a 63 percent increase to approximately 55 murders per 100,000 inhabitants. Gangs—national and neighborhood-based—contribute significantly to the violence problem. According to the 2015 National Gang Report from the FBI-sponsored National Gang Intelligence Center, gangs continue to grow, and they are expanding their criminal activities, thus posing "a significant threat to law enforcement and to the communities in which they operate."

In addition to the incalculable loss of human life, in some neighborhoods residents live in fear of being caught in the crossfire of gang fighting, exacting a significant social and economic cost. According to researchers at the University of Chicago, the total annual social and economic cost to the City of Chicago and its residents related to violence of this sort totals in the billions of dollars. Similarly, researchers at Temple University have evaluated the harms that gangs inflict on communities and identified 16 characteristics other than violence; these include economic factors, fear from intimidation, and interference with schooling.[1]

[1] Ratcliffe, Jerry H., Harms of Violent Street Gangs - How Do Gangs Harm Their Communities (October 10, 2015) at 1.

Americans are highly cognizant of the harm caused by violent criminals. A Gallop poll taken in April 2016 showed that concern over crime had reached a 15-year high, with 53 percent of poll respondents stating that they worried "a great deal" about crime and violence. As Attorney General Lynch noted in September 2016, "nothing threatens the vibrancy of our communities and the well-being of our people as severely as violence. Violent crime endangers lives, destroys families and paralyzes neighborhoods. It stifles opportunity and spreads fear. It deters investment and discourages education."

The OIG in the past has evaluated aspects of the Department's management of its anti-violence programs. For example, we have evaluated the level of coordination between the Department's violent crime task forces; ATF's implementation of its Violent Crime Impact Team initiative, which was designed to reduce homicides and other firearms-related violent crimes; and the intelligence and coordination activities of the National Gang Intelligence Center and the National Gang Targeting, Enforcement, and Coordination Center. In each of these reviews we identified important areas for improvement.

In an environment of limited government resources, we believe that it is essential for the Department to pay especially close attention to its stewardship of its anti-violence resources in light of the stakes involved. In order to better understand the Department's approach to management of its current violent crime initiatives, the OIG has initiated a review that is examining the Department's strategic planning and accountability measures for combating violent crime. Strategic planning is a basic management discipline used by businesses and the military, as well as law enforcement agencies, to help ensure that limited resources are directed to the most pressing problems and effectively disbursed. There are numerous examples of these efforts in the violent crime area, such as the strategic plan and implementation measures developed by the Memphis Shelby Crime Commission in Memphis, Tennessee, and the planning process employed by UnifiedErie, a community effort to reduce crime and violence in Erie, Pennsylvania. These and other examples show the many benefits of planning, including improved decision making and performance and, as a leading academic in the field of strategic planning has described, the creation of "significant and enduring public value."[2]

Source: UnifiedErie website

Our pending violent crime review is examining planning activities throughout the Department, to include the law enforcement and grant-making components, Main Justice, and USAOs, and attempting to better understand how the Department is evaluating risk and allocating its violent crime resources. Among the issues we are examining more closely are whether the FBI's own advances in planning techniques might offer some important lessons for the Department as a whole, how the Department has conceived the role of U.S. Attorneys in the fight against violent crime, and whether the tens of millions of dollars that the Department distributes in grants each year are being effectively coordinated within the Department. While local law enforcement clearly has the lead role in efforts to address violent crimes on the streets of our communities, the unique role the Department plays in assisting those efforts through its law enforcement and grant-making components makes it essential that the Department's programs be carried out effectively and efficiently. We expect our review to assist the Department in those efforts.

[2] See John M. Bryson, Strategic Planning for Public and Nonprofit Organizations 4th Ed. (San Francisco, CA: Jossey-Bass), 8.

Ensuring Effective Management and Oversight of Law Enforcement Programs and Promoting Public Trust

The Department is tasked with the Attorney General's highest priorities; among these are enforcing the law, defending the interests of the Unites States, and seeking just punishment for those guilty of unlawful behavior. It relies on the services of over 110,000 employees to manage federal law enforcement programs and meet its mission of ensuring public safety. The same leaders and supervisors responsible for carrying out the crucial mission of the Department are also tasked with responsibility for effective management and oversight of these law enforcement programs and ensuring ethical conduct. The issue of oversight continues to challenge Department supervisors, and how they undertake this responsibility affects whether the Department will be seen by the public as one abiding by high ethical standards; run effectively and within the rules.

Ensuring Effective Management and Oversight of Law Enforcement Programs

Federal law enforcement programs require effective planning, management, and oversight. The inherent risks associated with many of these programs must be balanced with the public's safety, as well the privacy and civil rights of individual citizens. Strong leadership, adept supervision, and effective management are essential elements of this balance. The examples described below illustrate the importance of these efforts.

Source: DOJ

Confidential Source (CS) and Confidential Informant programs are the backbone of federal law enforcement agencies, yet managing these programs has been and continues to be a significant challenge facing the Department. The Attorney General's Guidelines Regarding the Use of Confidential Informants (AG Guidelines) provide guidance to all Department law enforcement components on establishing, approving, utilizing, and evaluating sources. Yet, in the past 4 years, our reviews have found that two of the Department's law enforcement components, the Drug Enforcement Administration (DEA) and ATF, were not in full compliance with the AG Guidelines.

For example, the OIG's July 2015 audit of the DEA's CS Policies and Oversight of Higher-Risk CSs found that the Criminal Division's 2004 approval of the DEA's confidential source policies allowed the DEA to differ in several significant respects from the AG Guidelines' requirements. The DEA's differing policies for reviewing, approving, and revoking CSs' authorization to conduct "otherwise illegal activity" have resulted in DEA personnel being able to use CSs to conduct high-risk activities without the level of review that the AG Guidelines would otherwise require. More recently, our September 2016 audit of the DEA's oversight and management of its confidential source program found that between FYs 2011 and 2015 the DEA did not adequately oversee payments to its sources, which exposed the DEA to an unacceptably increased risk for fraud, waste, and abuse. This is particularly true given the frequency with which DEA offices utilize and pay confidential sources. We found that the DEA had over 18,000 active confidential sources assigned to its domestic offices, with over 9,000 of those sources receiving approximately $237 million in payments for information or services they provided to the DEA. We also estimated the DEA may have paid about $9.4 million to more than 800 previously deactivated sources during that same 5-year period. In addition, we found problems related to the DEA's use of "Limited Use" sources, who are deemed by the DEA to be low-

risk and thereby needing less supervision than other sources. Our review showed that the DEA signed up employees of Amtrak and the Transportation Security Administration (TSA) as Limited Use sources, despite the fact that the DEA could have obtained the information provided by these sources at no cost to the DEA. In January 2016, our Investigations Division reported that a single Amtrak employee was paid $854,460 over a 20-year period ending in January 2014 thereby wasting substantial government funds. Our audit, meanwhile, found that between FYs 2011 and 2015, the DEA paid at least 33 Amtrak employees a total of $1.5 million and 8 TSA employees a total of more than $94,000.

The DEA is not alone in struggling in this critical area. In our 2012 review of ATF's Operation Fast and Furious, we determined that the Department had never amended the AG Guidelines to include ATF in its coverage, even though ATF became a part of the Department in 2003. Our report recommended that the Department examine ATF's policies to ensure that they were in compliance with the AG Guidelines and other Department policies. In a follow-up review that the OIG released in February 2016, we noted that the Department believed that ATF's law enforcement policies complied with DOJ policies with three exceptions, each of which were addressed with revisions to ATF policy. The OIG is currently performing an audit of the ATF's management and oversight of its confidential informants.

To effectively protect Americans at home, the Department's law enforcement components often must partner with foreign nations and conduct operations overseas. The relationships that these agencies forge with international law enforcement are essential to the Department's mission but provide unique challenges for the components. In order to conduct successful and often complex investigations of sophisticated criminal targets, agencies within the Department often use extensive undercover or other long-term investigative operations or the expenditure of substantial funds in operation specific areas. However, in recent years, questions have been raised regarding some of these operations. The OIG, in collaboration with the Department of State (State) OIG, is conducting a review of the post incident responses by State and the DEA to three drug interdiction missions in Honduras in 2012, all involving the use of deadly force. The review, among other things, addresses pertinent pre-incident planning, the rules governing the use of deadly force, the cooperation by State and DEA personnel with post shooting reviews, and the information provided to Department leadership, Congress, and the public regarding the incidents.

The Department's law enforcement components also must be reasonable stewards of Department resources with regard to overseas operations. As discussed in more detail in the section on Contracts and Grants Oversight, in March 2016 the OIG found that the DEA expended nearly $8.6 million to purchase a large aircraft to support its counternarcotics efforts in Afghanistan, and that 7 years after purchase, it was inoperable and had never flown to Afghanistan. The DEA's inefficient use of its aviation assets coupled with the number of mission requests declined by the DEA raised serious questions as to whether the DEA was able to meet the operational needs for which its presence was requested in Afghanistan.


Source: DOJ

The Department has a zero tolerance policy for sexual harassment, and it is imperative that the Department's law enforcement components, in rule and practice, comply with this policy. Essential to ensuring that this policy is made a reality is the handling of sexual harassment complaints. In March 2015, the OIG issued a report on the handling of sexual harassment and misconduct allegations by the Department's four law enforcement components. The OIG identified systemic issues in the processes for handling such allegations at the DEA, FBI, U.S. Marshals Service (USMS), and ATF. Specifically, the OIG found that although ATF and the USMS had clear policies requiring supervisors to report misconduct allegations, supervisors sometimes failed to report such allegations, even when the allegation was similar to past misconduct. Further, the DEA's reporting policies did not clearly delineate what should be reported to

headquarters officials. As a result, DEA supervisors exercised discretion in deciding what to report. Another ongoing OIG review of the handling of sexual harassment and misconduct allegations in the Department's Civil Division will assess how that division responds when allegations of this kind are made against its employees. Separately, the OIG has begun a review of the related issue of gender equity in the operations of the four law enforcement components. In this review, we intend to assess component demographics, gender discrimination complaints, and the complaint process, as well as staff perceptions related to gender equity and the reasons for those perceptions.

Promoting Public Trust by Ensuring Ethical Conduct

As the federal agency charged with protecting the safety, civil rights, and freedom of American citizens, the Department and its employees must uphold the highest ethical traditions. Over the past year, the OIG has investigated law enforcement agents and attorneys for a wide range of criminal and administrative misconduct, ranging from misuse of power, acceptance of bribes, improper gifts and favors, and harassment. As detailed below, such misconduct erodes public confidence in the integrity of law enforcement and may have a significant negative impact on the Department's prosecutions.

Source: DOJ

With their power to make arrests and carry firearms, law enforcement agents are expected to not only enforce the law, but also follow it themselves. When they fail to meet the high expectations of the citizenry, it not only harms the Department's reputation, but also can impede programs and result in greater distrust of all law enforcement. The challenge for the Department is to provide effective supervision to try to prevent these incidents from occurring and, when they do, to locate and stop the behavior as quickly as possible and minimize its impact on the Department's law enforcement efforts and the public at large.

As reflected in a number of recent OIG investigations, Department employees are engaging in increasingly complex types of wrongdoing, thereby increasing the Department's challenge in deterring such misconduct. Several OIG criminal investigations illustrate the point, including an embezzlement of Bitcoins by a DEA agent and U.S. Secret Service agent, the theft of heroin by an FBI agent, and a conflict of interest by a former senior FBI official.

When Department attorneys commit misconduct unrelated to their legal work, the OIG has jurisdiction; and, in the past year, we have investigated a wide range of allegations of such wrongdoing by the Department's attorneys. For example, OIG investigations found that a U.S. Attorney violated Department regulations on political activities and fundraising and lacked candor in interviews with the OIG about those activities; and that a U.S. Attorney violated Department rules on the use of government travel cards. In addition, the OIG found that a U.S. Attorney had an inappropriate relationship with a subordinate, including sending multiple harassing e-mails and communications to the employee and then encouraging the employee not to cooperate with the OIG investigation and lying to Department officials about the underlying conduct. In another OIG investigation, we determined that an Assistant U.S. Attorney made unwanted sexual advances towards three female USAO employees while attending training.

To ensure transparency regarding our investigations, the OIG regularly posts summaries of employee misconduct findings on its website, including those involving federal prosecutors and employees from throughout the Department, including all four law enforcement components, who are members of the Senior Executive Service or level GS-15 and above.

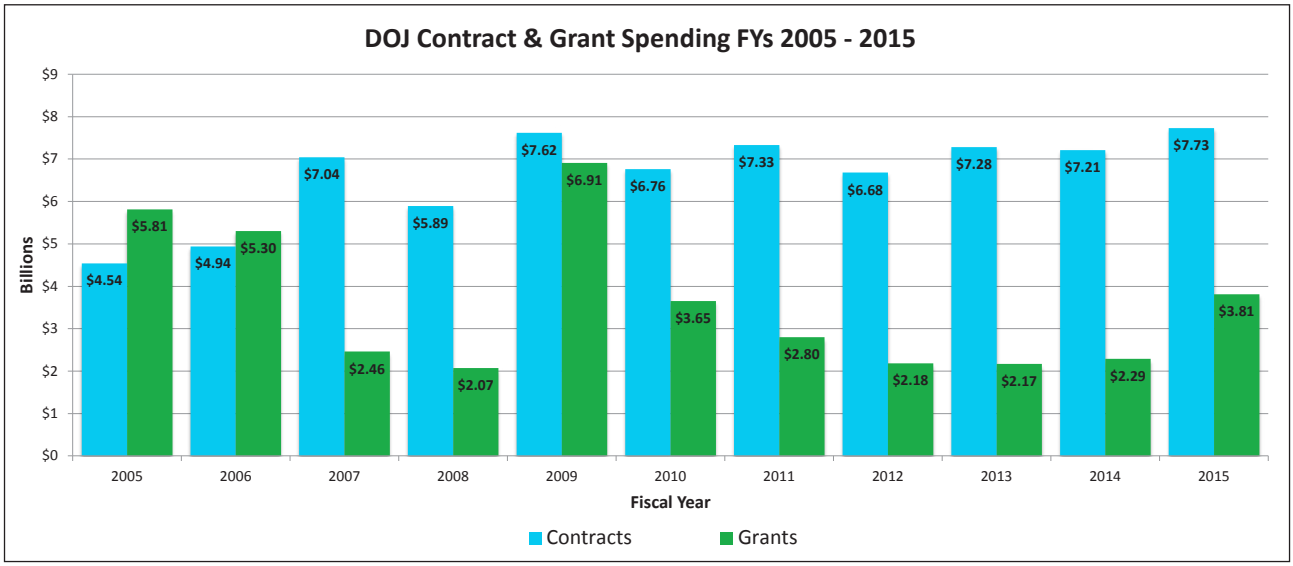
The OIG, however, does not have authority to investigate allegations of misconduct against Department attorneys when the allegations are related to their work as lawyers. Those allegations fall under the exclusive jurisdiction of the Department's Office of Professional Responsibility. The OIG has long believed that there is no principled basis for this continued limitation on our jurisdiction, and no reason to treat the investigation of misconduct by prosecutors differently than misconduct by agents. Under the current system, misconduct allegations against agents are handled by a statutorily independent OIG, while misconduct allegations against prosecutors are handled by a Department component that lacks statutory independence and whose leadership is both appointed by and removable by the Department's leadership. Bipartisan bills pending in both the U.S. House of Representatives and the U.S. Senate would remove this limitation on the OIG's jurisdiction. The legislation, as now proposed, would allow the OIG to investigate these important matters, where appropriate, with the independence and transparency that is the touchstone of all of the OIG's work, thereby providing the public with confidence regarding the handling of these matters. The Department's attorneys should be held to the same standards of oversight as other Department components, and the OIG should have oversight over all Department employees, just like every other OIG.

In response to a draft of this report, the Department questioned our position that the OIG should have the same authority as every other federal Inspector General to review allegations of misconduct by Department attorneys in connection with their work as lawyers. Among other things, the Department took issue with our description of OPR's relative lack of independence as compared to the OIG by asserting that (1) OPR's Counsel "remains unchanged with successive Attorneys General and presidential administrations," (2) the OIG has not "criticized OPR's work, the thoroughness of its investigations, or the soundness of its findings," and (3) the OIG has not "identified a single OPR investigation that failed to appropriately hold accountable . . . Department attorneys." On the first point, the same could be said of supervisory attorneys throughout the Department and, in fact, contrary to the Department's claim with regard to OPR, in April 2009, less than 4 months after the last change in presidential administrations, the new Attorney General replaced the OPR Counsel without any public explanation. On the second and third points, neither the OIG nor the public are in a position to fully assess the thoroughness and soundness of OPR's work precisely because OPR does not disclose sufficient information to allow for such an assessment. However, federal judges, the American Bar Association, and the Project on Government Oversight (POGO) have all questioned the level of independence, transparency, and accountability of OPR. *See, e.g.*, Order by Hon. Emmet G. Sullivan Appointing Henry F. Schuelke Special Counsel in United States v. Stevens, No. 08-cr-231 (Apr. 7, 2009), p. 46. ("*the events and allegations in this case are too serious and too numerous to be left to an internal investigation that has no outside accountability*") ; "Criminal Law 2.0," by Hon. Alex Kozinski, 44 Geo. L.J. Ann. Rev. Crim. Proc. iii (2015); ABA Recommendation urging the Department of Justice to release "as much information regarding individual investigations as possible," Aug. 9-10, 2010, available here; "Hundreds of Justice Department Attorneys Violated Professional Rules, Laws, or Ethical Standards: Administration Won't Name Offending Prosecutors," Report by POGO, March 13, 2014, available here.

Moreover, whatever the soundness of OPR's work, the Department's efforts to equate OPR's independence and transparency with that of the OIG flies directly in the face of the *Inspector General Act*, which fundamentally exists to create entities with an enhanced degree of independence and transparency so that they can credibly conduct investigations and reviews where there would be an expectation that more independent and transparent oversight is required. That is the very reason why Attorney General Ashcroft expanded the OIG's jurisdiction in 2001 to include the FBI and the DEA, and there simply is no reason why Department attorneys continue to be protected from the possibility that their conduct may warrant independent review by the OIG in appropriate cases.

Monitoring Department Contracts and Grants

As the Department strives to address some of the nation's most serious domestic and international threats, it must also do so in a fiscally responsible way. From FY 2005 to FY 2015, Department annual spending on contracts increased from $4.5 billion to $7.8 billion, while grants decreased from $5.8 billion to $3.8 billion during the same period. Recently, however, Department spending on grants has increased significantly. For example, between FY 2014 and FY 2015, Department grant spending grew by over $1.5 billion, due in large part to an increase in grant awards under the Crime Victims Fund (CVF), discussed below. Grant and contract funds are spent to help accomplish goals as varied as reducing crime, housing prisoners, and providing services to victims and at-risk populations. As stewards of taxpayer funds, the Department must act responsibly and wisely in managing these resources.



Source: Federal Procurement Data System and USASpending.gov

The Department faces significant challenges in ensuring effective oversight of its contracts and grants. In FY 2016, OIG's audits revealed nearly $25 million in questioned costs and reported over $2 million in funds that should have been put to better use, with 353 recommendations for management improvement. Additionally, the OIG's work has recently resulted in the recovery of nearly $5 million in money paid to contractor employees or credited back to the Department to address audit findings. While the Department's grant-making components have improved their oversight of grantees over the past several years, as referenced below, this remains a continuing challenge, especially since contract and grant spending represents a large a slice of the Department's $37.9 billion FY 2016 discretionary and mandatory budget.

Spending on Contracts

The Department awards contracts to procure a range of goods and services, from basic office supplies to aircraft operations. Given the increase in the amount of Department funds awarded to contractors over the past decade, the OIG has become increasingly involved in auditing contracts. In that role, we have observed significant challenges in both the Department's awarding and its monitoring of contract funds.

To effectively use the contracting process, the Department must comply with federal regulations by determining its needs prior to solicitation and then fully evaluating all bids prior to award. Our recent audit work has identified instances in which the Department failed to follow procedures designed to ensure fiscal responsibility and basic fairness in these processes. For example, in an audit of two FBI fuel procurement contracts, we found that the FBI did not award a bulk fuel procurement through the FAR-identified mandatory source and did not establish a requirement for the specific fuel type for the Miami Field Office. Similarly, our audit of DEA's Aviation Operations with the Department of Defense in Afghanistan found that the DEA did not fully comply with the Federal Acquisition Regulations (FAR) and its own solicitation in purchasing an aircraft for over $8 million.

Source: OIG

The Department also faces challenges monitoring contracts after monies have been awarded. Monitoring a contract post-award helps ensure the contractor abides by its terms, including those that govern the proper use of funds, compliance with laws and regulations, and contractor performance to achieve anticipated outcomes. Again, our audit of the DEA's Aviation Operations in Afghanistan showed major deficiencies in these areas. We found that the program had missed every intended delivery date from the first delivery date in December 2012. Those missed deadlines contributed to the program cost spiraling to $86 million, almost four times the original anticipated amount of $22 million, and the aircraft was still not operational as of June 2016.

The OIG recently identified similar challenges in how the BOP monitors contract prisons. In an August 2016 report, we found that the BOP still had monitoring improvements to make since our 2015 audit of the Reeves County contract prison, discussed in last year's report. We found that a checklist in the BOP's Quality Assurance Plan did not address certain important BOP policy and contract requirements in the areas of health and correctional services. As a result, the BOP has not been able to effectively ensure that contract prisons comply with these requirements. The week after our audit was released, the Department announced that it would begin the process of reducing and ultimately ending its use of privately operated prisons.

Spending on Grants

Grant funding also presents challenges, as the Department must not only guard against fraud and mismanagement but also seek to enhance taxpayer value by finding ways to better measure and ensure positive outcomes. As with contracts, our recent OIG work has identified challenges in both allocation and oversight of these expenditures.

In last year's Top Management and Performance Challenges report, we highlighted the enhanced responsibility the Department would face in its management of the CVF due to the over three-fold increase in the amount of CVF funds Congress authorized the Department to spend in FY 2015. In FY 2016, Congress increased the cap on CVF spending by over $600 million to more than $3 billion, most of which OJP's Office for Victims of Crime distributes via grants to programs intended to assist victims of crime. Rather than tax dollars, the CVF is financed by fines and penalties paid by convicted federal offenders. Nonetheless, an increase in available funds brings with it an increased risk of misuse and mismanagement. To monitor increased CVF spending, the OIG was allocated $10 million from the CVF in both FY 2015 and FY 2016 for enhanced oversight and auditing activities related to the fund. We are currently conducting a risk assessment of OJP's management of the CVF.

Simultaneously, the OIG continues to conduct audits of state CVF formula grantees and their allocation and management of funds to sub-grantees to ensure adherence to the terms of the grants. In these audits, we have identified various areas in need of improvement, including instances in which grantees failed to properly monitor sub-grantees. For example, in a recent audit of ten CVF formula grants, the OIG found that the California Governor's Office of Emergency Services was funding several sub-grantees with histories of fraudulent and even criminal conduct, while also failing to issue sub-recipient monitoring reports in a timely manner.

In addition to challenges in grant allocation, the Department must also ensure proper post-award oversight. OIG work has identified instances in which the Department was unable to ensure adequate performance by grantees and sub-grantees. Some examples include the failure by grantees to comply with essential grant conditions; maintain adequate records and accounting systems; and submit accurate, complete, and timely financial and performance reports.

Such challenges were highlighted in a November 2015 audit of an OVW grant to the Dawson County Domestic Violence Program in Glendive, Montana. In that audit, we questioned the entire amount—nearly $4 million—the grantee had used because the grantee was unable to provide a complete and accurate set of accounting records. In addition, limitations in the grantee's tracking system inhibited the OIG from adequately assessing program performance and, thus, taxpayer value. For example, the grantee could not even confirm the total number of victims served.

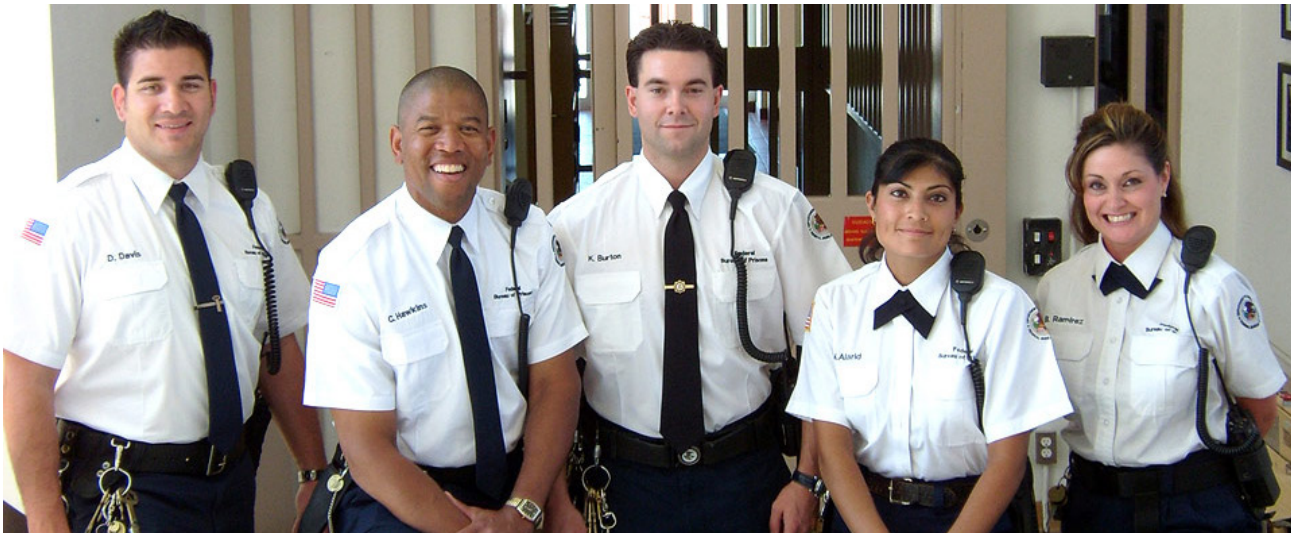
The OIG continues to work with the Department's grant-making components to ensure that grant dollars are used to achieve positive outcomes. For example, in 2015, we conducted an audit of grants awarded to the Navajo Division of Public Safety through OJP's former Correctional Systems and Correctional Alternatives on Tribal Lands Program. We found that the grantee constructed two correctional facilities with capacities that were at least 250 percent larger than needed. Since the completion of our audit, one facility has not yet opened due to construction issues, and the other facility is 82-percent vacant. The OIG is continuing to monitor open recommendations from the audit and is also conducting a comprehensive audit of OJP's management and oversight of the Tribal Justice Systems Infrastructure Program (formerly the Correctional Systems and Correctional Alternatives on Tribal Lands Program).

At recent Congressional hearings, top officials within OJP spelled out steps they are taking to improve OJP's processes. These steps include (a) collaborating with other components to prevent duplication of efforts, (b) establishing procedures to identify and monitor high-risk grantees, (c) providing enhanced technical assistance to grantees, and (d) verifying grantee claims of program success by collecting and examining source documentation.

The OIG's work illustrates that the Department must improve its oversight of its contract and grant award and monitoring efforts to guard against waste, fraud, abuse, and mismanagement, and to ensure the most efficient and effective use of taxpayer funds.

Managing Human Capital and Promoting Diversity With a Workforce Increasingly Eligible to Retire

Agencies across the federal government face the challenge of hiring and retaining talented employees with the skillsets needed to accomplish agency missions, while their aging workforces increasingly become eligible to retire. This challenge represents a serious problem for the Department—and the public that it serves and protects—if it is unable to hire and retain experienced agents and attorneys with the specialized skills needed to investigate and prosecute complex cases related to, for example, terrorism, cybersecurity, financial crime, civil rights, and public corruption. As of September 2014, approximately 31 percent of the Department's permanent career employees were eligible to retire by 2019. In the next 10 years, 85 percent of the federal government's Senior Executive Service will be eligible to retire. As the number of retirement-eligible employees grows, the Department needs to develop long-term strategies to recruit and retain a skilled and diverse workforce.



Source: BOP website

Managing Human Capital To Prepare For Increasing Numbers of Retirements

Succession planning in the government offers unique challenges for agency leaders. From FYs 2005 to 2014, retirement in the Executive Branch increased by 10.9 percent. During this time, mandatory retirements also increased by 83.8 percent. As the rate of federal retirements continues to increase, the Department has an opportunity to institute proactive policies and guidance that guard against the loss of institutional knowledge and to maintain continuity of operations. In facing this transition in its workforce, the Department must strive to mitigate the loss of institutional knowledge created by the retirements of senior employees and managers, ensure that mid-career employees are prepared to take over senior positions, and train new employees to step into important leadership roles.

A unique challenge for the Department's law enforcement components is the difficulty retaining experienced Special Agents in management positions because agents are eligible for full retirement at age 50 with 20 years of service, and know they must retire at age 57. As a result, experienced agents often retire or take private sector positions well before those in most other federal occupations. Law enforcement leaders in the Department have told us this has a negative impact on the level of experience and knowledge of upper-

management in their ranks. One option that law enforcement components can use in special cases is to grant extensions allowing agents to work past their mandatory retirement age; however, given its limits, this choice is not a solution to the larger problem.

Hiring Quality Candidates to Ensure Department Mission and Agency Goals are Met

As the Department recognizes, its employees are its greatest assets. The Department's challenge is to recruit skilled and diverse talent to help meet mission goals. Advances in technology will continue to affect every aspect of Department operations such as data management, communications, cyber investigations, and cybersecurity. It is therefore imperative that the Department be innovative in its efforts to fill vacant positions that require specialized skills, in areas such as Science, Technology, Engineering, and Mathematics (STEM). As we note in the section on Cybersecurity, the FBI faces significant challenges in hiring qualified IT experts to address its responsibilities in this area given competition from the private sector. These challenges have grown even more acute as some segments of the economy have experienced economic growth and IT job vacancies outnumber those who can fill them.

Another example of the challenge in hiring experts with a STEM background is the Department's difficulty hiring medical professionals for its federal correctional institutions. In March 2016, the OIG conducted a review of the BOP's medical staffing challenges and found that multiple factors, including pay, the location of the institutions, and the correctional setting itself, negatively impact the BOP's ability to recruit and retain medical professionals. The OIG also found that the salaries and incentives the BOP offers are not competitive with those of the private sector, particularly given the need to compensate BOP employees for working in a correctional setting.

Source: DOJ

Another hiring challenge for the Department in recent years has been adjusting to the generational shift in the workforce. For example, in 2006, nearly 47 percent of the Department's workforce was under the age of 40, while only 9 percent of Department employees were 55 and older. Ten years later, Justice Management Division (JMD) data shows that approximately 24 percent of the Department's workforce is age 35 and under (often referred to as "Millennials"), 52 percent are ages 36 to 51 (often referred to as "Generation X"), and 24 percent are age 52 and older (often referred to as "Baby Boomers"). While the Department's workforce is aging, it must address the additional challenge of generational changes as it seeks to bring on board younger employees. The President has recognized that students and recent graduates "infuse the workplace with their enthusiasm, talents, and unique perspectives." OPM has found that one of the best ways to ensure the federal workforce better reflects the people it serves is to actively recruit the next generation of federal employees. However, while the workforce is trending younger, the traditional federal hiring process still favors applicants possessing prior work experience. To meet this challenge, the Pathways program, which recruits students and recent graduates with less work experience, has evidence of being effective. Using Pathways, the Department hired 170 employees in FY 2015 and 113 employees FY 2016. Moreover, OPM statistics show that 93 percent of those hired through Pathways want to stay in government. This program has the potential to help mitigate the impact of increasing retirements by bringing on board a new generation of talented employees who can begin developing institutional knowledge at the outset of their careers, and potentially develop into future leaders.

OPM has also found that offering telework to employees is an important recruitment and retention tool, and it helps to improve employee attitude and job satisfaction across the federal workforce. However, the Department's current telework participation rate is 11 percent, far below the government-wide participation rate of 31 percent. While we recognize that telework opportunities for those with law enforcement responsibilities are more limited, we nevertheless believe that a participation rate of only 11 percent suggests there is opportunity for improvement in this area.

Once a new employee has been selected, it is critical for the Department to make the hiring process as swift as possible, particularly for positions deemed mission critical. OPM has set 80 days as the goal for federal agencies to complete the hiring process. While this is a useful target, we recognize it might not be practical for agencies such as the Department that have unique hiring needs. Still, JMD statistics suggest there is room for improvement, as they show that on average it took more than 5 months to hire attorneys (225 days), criminal investigators (162 days), IT specialists (190 days) and legal assistants (248 days)—all deemed mission critical positions. The Department's FY 2014-2018 Strategic Plan sets a goal to evaluate a new system that would enable human resources staff to hire people faster by automating manual and paper-based processes. Another significant factor delaying employee start dates can be the time required to complete background checks, which need to be performed in a timely manner. In 2012, the OIG released a report finding that clearances for mission critical positions in the Department such as agents, intelligence analysts, and linguists, consistently took longer than 60 days, a benchmark that agencies are expected to achieve 90 percent of the time under the *Intelligence Reform and Terrorism Prevention Act of 2004*.

Retaining Diverse Talent to Minimize the High Cost of Employee Turnover

The Department must also focus on retaining the talent it hires in order to hold down high turnover costs. OPM estimates turnover costs can range from 90 percent to 200 percent of an employee's annual salary. The Department should consider how programs that encourage diversity, mentorship, employee engagement, and accountability between managers and those they supervise, can improve workplace environments and foster retention.

Source: DEA website

Establishing a diverse work force is a challenge for the Department across the organization, but particularly at the management level. Data shows only 35 percent of employees at the GS-14 level and above are women, and only 23 percent are from racial and ethnic minority groups. While announcing a new report promoting diversity in law enforcement, in October 2016 Deputy Attorney General Yates noted the benefits of having police "reflect the communities they serve." A growing body of evidence suggests diversity can make policing more effective, safe, and just, according to the report by the Civil Rights Division and the Equal Employment Opportunity Commission. Although the report was focused on local law enforcement, it offered advice on recruitment, hiring, and retention that could be of value to the Department's own law enforcement components. Statistics show that as of FY 2014, 69 percent of the Department's criminal investigators were white men, 12 percent were white women, 15 percent were minority men, and 3 percent were minority women.

Engaging employees is one way to improve retention. The Department can accomplish this by providing ways for employees to enhance their skillsets. Another method encouraged by OPM is that employees have multiple mentors in different areas, such as a career guide, an information source within the office to help an employee understand how the office works, a friend to confide in, and an intellectual guide. Employee

engagement can also be improved by creating developmental assignments for employees to grow their abilities, and ensuring that employees are cross-trained in order to preserve institutional knowledge that might be lost with an employee's retirement or extended absence. Interestingly, the 2015 Federal Employee Viewpoint Survey (FEVS) found that although 68 percent of Department respondents were satisfied with employee engagement, only 58 percent were satisfied with how agency leaders communicate with and motivate their employees.

Another challenge for the Department is to ensure that managers and employees are held accountable for their performance. According to OPM, a bad hire can cost an agency as much as three times an employee's salary. To illustrate, if an agency hires a GS-14 or GS-15 employee who is not fully successful during the probationary period, it could cost the agency more than $300,000. According to the 2015 FEVS Survey, 44 percent of respondents did not think Department managers were taking sufficient steps to deal with poor performers who either cannot or will not improve. However, managers point out that often co-workers are unaware that actions are being taken to address poor performance because the *Privacy Act* places limits on what managers can disclose about disciplinary actions they take.

The Department will continue to face challenges as an increasing number of employees retire and take with them a vast amount of institutional knowledge. The Department must ensure that it responds to this generational shift by recruiting and retaining a diverse workforce with varied skillsets. To do so, the Department will need to look for innovative strategies and improve on-boarding time, among other things, to remain competitive with other markets and attract the most qualified candidates for critical Department operations.

Using Performance-Based Management To Improve DOJ Programs

A Challenge Facing Every Component and Program

In an era when government agencies at the local, state, and federal level are moving toward a more widespread recognition of the importance of a data-driven approach to planning and management, our reviews have repeatedly found that this remains a significant challenge for the Department. From the Department's failure to evaluate "big data" on important criminal justice issues, such as whether its detention and rehabilitation programs impact recidivism, or knowing how many officer-involved shootings there have been across the nation, more needs to be done. While this challenge appears at the end of this report, it does so precisely because it impacts every one of the challenges previously discussed, illustrating how the deficit in performance-based management is a challenge across many of the Department's programs.

For example, the Department's primary method of measuring crime in the United States remains the FBI's 1930s-era annual compilation of Uniform Crime Reporting (UCR) statistics. Yet, as the FBI has acknowledged, these crime statistics do not sufficiently characterize crime today (they do not, for example, explicitly address cybercrime), and are far less useful in directing enforcement efforts than they otherwise could be if they were available much sooner, instead of nine months after the previous reporting year ended. Meanwhile, only a third of the nation's law enforcement agencies are reporting crime data using the National Incident-Based Reporting System (NIBRS), a much more comprehensive system the FBI developed in 1989 to replace the UCR's summary reporting. Although the FBI, working with the Bureau of Justice Statistics, is committed over the next four years to try and recruit a statistically-representative sample of law enforcement agencies to use NIBRS, and has transferred $45 million to BJS so far to support this work, a more comprehensive crime data solution appears years away.

Source: FBI website

At a time when some big city police departments can tell you where and when every gunshot was fired in the city with audio recordings of the shots e-mailed instantly to precinct captains' cell phones with precise geo-location information, the Department has much it can learn from its local law enforcement partners. Because police departments in some cases have detailed crime data available in near real-time, federal prosecutors are working with them to gather the information they need to figure out where to focus limited federal resources to fight gang and gun violence. Although these partnerships hold much promise for future federal, state, and local law enforcement collaboration, they illustrate that when it comes to crime data, the Department is often playing catch up with its local counterparts. Not having a national database of accurate information on shootings, including police shootings, is just one symptom of the lack of timely and comprehensive crime data. Without such information Department officials are stuck trying to tackle a problem they cannot accurately measure or analyze.

At the other end of the criminal justice process, the BOP has not released statistics on the recidivism rate of federal prisoners in more than 20 years. So although the BOP spent $7.8 billion in FY 2016 to cover inmate needs such as housing for nearly 200,000 federal prisoners, the Department cannot determine with much accuracy whether its prison system is achieving the twin goals of deterrence and rehabilitation. As discussed in the Prisons challenge, our August 2016 review of the BOP's RPP found that, "the BOP does not collect

comprehensive re-arrest data on its former inmates, has no performance metrics to gauge the RPP's impact on recidivism, and does not make any attempt to link its RPP efforts to recidivism." Similarly, the BOP spent roughly $360 million a year in FYs 2014 and 2015 on approximately 200 Residential Reentry Centers, but it does not currently track the success of its RRC programs, a subject of one of our ongoing BOP reviews. On a positive note, the BOP has announced its intention, as part of its strategic plan, to use data to begin monitoring the success of various RRCs beginning this summer. It needs to do so to tap into the potentially vast laboratory of innovation available to make its programs as efficient and effective as possible.

Multiple mandates affirm the importance of performance-based management. For example, OMB Circular A-11 requires agencies to conduct at least quarterly, data-driven performance reviews on their organization's priorities to drive progress toward achieving their goals. OMB Circular A-11 describes this approach as a "management practice proven to produce better results." Similarly, the *Government Performance and Results Modernization Act of 2010* (GPRAMA) requires agencies to engage in performance management tasks such as setting strategic plans or completing annual performance plans. Additionally, the *Digital Accountability and Transparency Act of 2014* (DATA Act) directs the federal government to transform all spending information into standardized, easy-to-read data formats for better transparency. Implementation of the DATA Act will not only expand the information available to the public, but will also give the Department access to that information in a standard data format for use in management and decision making. A September 2015 GAO report found that, "if fully and effectively implemented" the DATA Act and GPRAMA could allow executive branch agencies and Congress to accurately measure the costs and magnitude of federal investments.

Collecting The Right Data

The challenge for the Department with all of its programs is to ask, "Are we collecting the right information?" However, simply collecting data, using metrics, and labeling a process "performance-based management," does not satisfactorily comply with GPRAMA and OMB guidance or the important policies underlying them. The Department must ensure it identifies performance metrics to adequately measure program outputs and must identify and collect the right data to measure its programs' impacts. As mentioned in the Prisons section, a July 2016 OIG audit found that neither the EOUSA nor the USAOs track the total number of participants placed into pretrial diversion programs. The result is an inability to calculate whether the use of such programs is meeting the goals of the Department's Strategic Plan and its Smart on Crime initiative.

Source: DOJ

Ensuring the Department effectively collects data and that the data collected reveals the true story is a challenge that impacts every facet of the Department's operations. For example, the OIG discovered that the BOP uses two systems to track recovered contraband cell phones and that over a 3-year period there was a difference of more than 41 percent in the cell phone contraband data reported between the two methods. The BOP's data collection methods, coupled with the lack of established guidance and policy on accurately and consistently documenting recovered contraband, impede its ability to effectively track contraband recoveries and analyze contraband trends. Without a reliable method to ascertain the true amount of contraband and the efficacy of its interdiction efforts, the BOP cannot fully address questions regarding prison safety.

Additionally, the Department needs to be vigilant to ensure that its data collection and metrics are accurately being used to measure program performance. For example, the OIG's audit of the FBI's Regional Computer Forensic Laboratory (RCFL) discovered that, as a result of the FBI changing its "definition" of what constituted a backlog, what appeared to be a decline in the backlog at the RCFL in fact reflected a continuing backlog. This is similar to the double counting of total cases opened by immigration courts that we noted in our 2012 review of the Management of Immigration Cases and Appeals by the Executive Office for Immigration Review (EOIR). We also found in that review that EOIR's performance reporting data underreported actual processing time, which undermined EOIR's ability to identify appeal processing problems and take corrective action. Only by choosing appropriate measures and accurately reporting on them can the Department ensure that its use of metrics will help improve Department programs. This is the essence of performance-based management and it remains a challenge for the Department.

Verifying The Data Collected Is Accurate and Reliable

Another challenge in performance-based management is verifying that the data collected is valid, accurate, and reliable. As we have included in past TMPC reports, our work has found numerous instances where data was inaccurate, unreliable, or unsupported. There are more instances of such findings from this year as well. As mentioned in the Contracts section, the OIG questioned nearly $4 million in a November 2015 audit of an OVW grant where the grantee could not confirm the total number of victims served or provide information that would allow the OIG to assess the program's performance. Our April 2016 audit of the OVW grants awarded to the Native Women's Society of the Great Plains, in Eagle Butte, South Dakota, found that the grantee could not provide adequate documentation to support the activities recorded in its progress reports.

Source: OIG

However, data reliability is not just an issue with grantees, but is an area in which the Department can improve as well. For example, our March 2016 audit of BOP's Armory Munitions and Equipment found weaknesses in BOP's controls over tracking, issuing, and reporting on both active and expired armory munitions and equipment. This inaccurate data increases the risk that armory munitions and equipment could be lost, misplaced, or stolen without being detected. Further, our March 2016 audit of the National Institute of Justice's Management and Oversight of DNA Backlog Reduction Grantees' Reporting and Use of Program Income emphasized the need for the Department to provide clear direction to grantees so the data it receives is reliable. In that audit, we found that important calculations of program income were often incorrect because the grantees had not received proper training on the calculation tool provided by the NIJ. As a result, the grantees submitted inaccurate program income calculations and reporting. In order to fully implement performance-based management, the Department must ensure that it provides guidance to those submitting data to ensure that the data provided is valid, accurate, and reliable prior to its analysis and use by the Department in program management decisions.

Analyzing The Data Collected

Another challenge for the Department is to collect and analyze data showing program results, and more significantly, *program impact*. Analyzing Department program data in meaningful ways to determine impact is essential to managing the effectiveness of these programs going forward. For example, we found in our review of the BOP's Medical Staffing Challenges that the BOP tracks the use of incentives only to ensure that spending remains within budgetary limits and not to identify the hardest to fill vacancies in the BOP system. Analyzing data to determine the hardest to fill vacancies could assist the BOP in more effectively managing its workforce, which in turn is essential to fulfilling its mission.

Such performance analysis is critically important, both when it shows program success and when it indicates that a program is falling short of its goals. In our February 2016 audit of the DEA's Controls Over Seized and Collected Drugs, for example, we found that DEA personnel still sometimes failed to meet inventory management requirements despite the increased time allowed for its personnel to complete tasks. The delayed entry of drug exhibits increases the risk of evidence tampering, misplacement, or loss, which in turn impacts the effectiveness of the DEA's program. Program management in such instances should analyze performance metrics to inform necessary program changes to eliminate problem areas and thereby increase the effectiveness of the Department's programs.

Furthermore, Department components should review what has and has not worked for other components to effectively leverage knowledge from past efforts. For example, in our February 2016 review of Department and ATF's implementation of recommendations contained in an earlier Fast and Furious report, we found several areas where the Department and ATF improved their ability to assess risk metrics in law enforcement operations but also discovered that performance-based lessons learned from one Department component's performance issues are not adequately evaluated and integrated by other components. Such disparities reflect the need for Department leaders to be engaged in making sure reforms made in one component are considered by their fellow components, so each can learn from the others.

The performance-based management challenge is more than a standalone challenge—it permeates all of the other Department challenges. From creating a comprehensive crime data solution to the analysis of BOP data to determine the recidivism rate of federal prisoners released to the public, the collection and analysis of performance measures is essential to effectively and efficiently managing Department resources to ensure that its programs consistently achieve the greatest possible impact on the many difficult challenges it faces.

Congressional Research Service
Informing the legislative debate since 1914

Temporarily Filling Presidentially Appointed, Senate-Confirmed Positions

Henry B. Hogue
Analyst in American National Government

April 1, 2016

Congressional Research Service
7-5700
www.crs.gov
RS21412

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

A vacant presidentially appointed, Senate-confirmed position (herein, "advice and consent position") can be filled temporarily under one of several authorities that do not require going through the Senate confirmation process. Under specific circumstances, many executive branch vacancies can be filled temporarily under the Federal Vacancies Reform Act of 1998 or by recess appointment. In some cases, temporary filling of vacancies in a particular position is specifically provided for in statute. Generally, designation or appointment under one of these methods confers upon the official the legal authority to carry out the duties of the office. Alternatively, an individual may be hired by the agency as a consultant. A consultant does not carry the legal authority of the office, and may act only in an advisory capacity.

In many instances, the functions of a vacant advice and consent office may be carried out indefinitely by another official, usually the first assistant, under the terms of an administrative delegation order of the agency head. In such instances, the official carries out these functions without assuming the vacant office.

Contents

Contacts

According to the 2012 edition of the *Plum Book*,[1] more than 1,000 executive branch positions are filled through appointment by the President with the advice and consent of the Senate (herein, advice and consent positions).[2] The Constitution and federal statutes provide several authorities for temporarily filling vacancies in these positions: the Federal Vacancies Reform Act of 1998[3] (Vacancies Act); the President's constitutional recess appointment power; and position-specific temporary appointment provisions. Each of these authorities is discussed below.

Designations Under the Vacancies Act

When an executive branch advice and consent position covered by the Vacancies Act becomes vacant, it may be filled temporarily in one of three ways under the act: (1) the first assistant to such a position may automatically assume the functions and duties of the office; (2) the President may direct an officer who is occupying a different advice and consent position to perform these tasks; or (3) the President may select an officer or employee who is occupying a position, in the same agency, for which the rate of pay is equal to or greater than the minimum rate of pay at the GS-15 level, and who has been with the agency for at least 90 of the preceding 365 days.

In general, a temporary appointment under the Vacancies Act continues until no later than 210 days after the date the vacancy occurred or, if the vacancy occurred during a Senate recess, 210 days after the date the Senate reconvenes. The time restriction is suspended, and the acting officer can continue to serve, if a first or second nomination for the position has been submitted to the Senate for confirmation and is pending. The acting officer can continue to serve for an additional 210 days after the rejection, withdrawal, or return of such a nomination.

Notably, the U.S. Court of Appeals for the D.C. Circuit has held that a provision of the Vacancies Act limits the conditions under which an individual may serve in both an acting capacity and as the nominee to the same position. The court's opinion appears to allow an individual to serve on this basis only if the individual has served as the first assistant to the vacant position for more than 90 of the preceding 365 days.[4]

Temporary appointments to vacancies that exist during the 60-day period following the inauguration of a new President are treated differently, which gives the new President additional flexibility during the transition. The ordinary 210-day restriction period does not commence until

[1] U.S. Congress, House Committee on Oversight and Government Reform, *United States Government Policy and Supporting Positions*, 112th Cong., 2nd sess., committee print, December 1, 2012 (Washington: GPO, 2012), pp. 197-200. The next edition of this quadrennial print, commonly known as the *Plum Book*, is expected in late 2016. The precise number of advice and consent positions is difficult to ascertain; other sources provide different estimates. CRS usually uses the *Plum Book* for such information, although some errors have been identified in its data. The *Plum Book*-based estimate includes full-time and part-time positions in the executive branch. It does not include positions that are typically considered to be routine nominations, including members of the officer corps in the military services and some positions in the Foreign Service. Advice and consent positions are also known as "PAS positions," after the abbreviation used in the *Plum Book*.

[2] Prior to October 2012, approximately 1,200-1,400 executive branch positions were filled through the advice and consent process. The Presidential Appointment Efficiency and Streamlining Act (P.L. 112-166, 126 Stat. 1283) reduced this number by 163 positions. The act changed the appointment provisions for each of these positions such that, once vacant, they are no longer to be filled as advice and consent positions. See CRS Report R41872, *Presidential Appointments, the Senate's Confirmation Process, and Changes Made in the 112th Congress*, by Maeve P. Carey.

[3] P.L. 105-277, Div. C, Title I, §151; 5 U.S.C. §§3345-3349d.

[4] SW General, Inc. v. NLRB, 796 F.3d 67 (D.C. Cir. 2015).

the later of the following two dates: 90 days after the incoming President assumes office, or 90 days after the vacancy occurs.

In general, once the time limitations of the Vacancies Act have been exhausted, only the head of the agency may perform any non-delegable function or duty of that office.[5]

Appointees under the Vacancies Act are authorized to "perform the functions and duties of the office temporarily in an acting capacity subject to [these] time limitations."[6] The act does not apply to positions on multi-headed regulatory boards and commissions, or to new positions that have never been filled.[7]

Recess Appointments[8]

The President's authority to make recess appointments is conferred by the Constitution, which states that "[t]he President shall have Power to fill up all Vacancies that may happen during the Recess of the Senate, by granting Commissions which shall expire at the End of their next Session."[9] Presidents have made such appointments during within-session recesses (*intrasession* recess appointments) and between sessions (*intersession* recess appointments). Recess appointments expire at the end of the next session of the Senate. As a result, a recess appointment may last for less than a year, or nearly two years, depending on when the appointment is made.

Presidents have occasionally used the recess appointment power in ways that have had the effect of circumventing the confirmation process.[10] In response, Congress has placed restrictions on the President's authority to make recess appointments. Under 5 U.S.C. §5503(a), if the position to which the President makes a recess appointment falls vacant while the Senate is in session, the recess appointee may not be paid from the Treasury until he or she is confirmed by the Senate. The salary prohibition does not apply (1) if the vacancy arose within 30 days before the end of the session; (2) if a nomination for the office was pending when the Senate recessed, provided that the nominee was not previously recess appointed to the position; or (3) if a nomination was rejected within 30 days before the end of the session and another individual was given the recess appointment. A recess appointment falling under any one of these three exceptions must be followed by a nomination to the position not later than 40 days after the beginning of the next

[5] 5 U.S.C. §3348.

[6] 5 U.S.C. §3345(a)(1). However, when the time limitations of the Vacancies Act have been exhausted, it may still be possible for the functions of a vacant office, except those that are non-delegable, to be carried out indefinitely by another individual pursuant to a delegation of authority. See "Delegation of Duties to another Official," below.

[7] This law superseded previous, similar statutory provisions. For more on the Vacancies Act, see CRS Report 98-892, *The New Vacancies Act: Congress Acts to Protect the Senate's Confirmation Prerogative*, by Morton Rosenberg.

[8] For a further discussion of recess appointments, see CRS Report RS21308, *Recess Appointments: Frequently Asked Questions*, by Henry B. Hogue; and CRS Report RL33009, *Recess Appointments: A Legal Overview*, by Vivian S. Chu. See also CRS Report RL33310, *Recess Appointments Made by President George W. Bush*, by Henry B. Hogue and Maureen O. Bearden; and CRS Report R42329, *Recess Appointments Made by President Barack Obama*, by Henry B. Hogue.

[9] Article 2, §2, cl. 3 of the Constitution.

[10] For example, when President George W. Bush recess appointed Charles W. Pickering to a judgeship on the United States Court of Appeals for the Fifth Circuit, he noted that 2½ years had passed since Pickering's nomination had been submitted to the Senate and stated that "a minority of Democratic Senators has been using unprecedented obstructionist tactics to prevent him and other qualified individuals from receiving up-or-down votes." The President's statement at the time of the recess appointment may be found at http://georgewbush-whitehouse.archives.gov/news/releases/2004/01/20040116-19.html.

session of the Senate.[11] For this reason, when a recess appointment is made, the President generally submits a new nomination for the nominee even when an old nomination is pending.

In some instances, a recess appointee whose nomination to the position is not successful might not be paid. These instances are discussed below. (See "Unsuccessful Nominations and Payment Limitations.")

From the 110th Congress onward, it has become common for the Senate and House to use certain scheduling practices as a means of precluding the President from making recess appointments.[12] The practices do this by preventing the occurrence of a Senate recess of sufficient length for the President to be able to use his recess appointment authority.

These congressional scheduling practices might have prevented President George W. Bush from making recess appointments at the end of his presidency; he made no recess appointments during the times this approach was in use.[13] It also might have limited use of the recess appointment power by President Obama.[14]

In January 2012, President Obama appeared to challenge the ability of this practice to prevent the exercise of his authority. He made four recess appointments during a three-day recess between pro forma sessions of the Senate on January 3 and January 6, 2012, a period that was generally considered too short to permit recess appointments. The recess during which the President made the appointments was part of a period of Senate absence that, but for the pro forma sessions, would have constituted an intrasession adjournment of 10 days or longer.

In an opinion regarding the lawfulness of these appointments, the Office of Legal Counsel in the Department of Justice argued that "the President may determine that pro forma sessions at which no business is to be conducted do not interrupt a Senate recess for the purposes of the Recess Appointments Clause."[15] The U.S. Supreme Court later concluded otherwise in a case regarding three of the four appointments. It held that, for purposes of the Clause, "the Senate is in session when it says it is, provided that, under its own rules, it retains the capacity to transact Senate business."[16] The Court also held that the President may use the recess appointment power essentially only during a Senate recess of 10 days or longer. A Senate recess of 3 days "is not long enough to trigger the President's recess appointment power," and a recess of more than 3 days but less than 10 is "presumptively too short to fall within the Clause" but "leaves open the possibility that a very unusual circumstance could demand the exercise of the recess-appointment power during a shorter break."[17]

---

[11] Congress placed limits on payments to recess appointees as far back as 1863. The current provisions date from 1940 (ch. 580, 54 Stat. 751; 5 U.S.C. §56, revised, and recodified at 5 U.S.C. §5503, by P.L. 89-554, 80 Stat. 475).

[12] The evolution of this use of scheduling practices is discussed in greater detail in CRS Report R42329, *Recess Appointments Made by President Barack Obama*, by Henry B. Hogue.

[13] See CRS Report RL33310, *Recess Appointments Made by President George W. Bush*, by Henry B. Hogue and Maureen O. Bearden

[14] See CRS Report R42329, *Recess Appointments Made by President Barack Obama*, by Henry B. Hogue.

[15] "Lawfulness of Recess Appointments during a Recess of the Senate notwithstanding Periodic Pro Forma Sessions," Memorandum Opinion for the Counsel to the President, January 6, 2012, available at http://www.justice.gov/sites/default/files/olc/opinions/2012/01/31/pro-forma-sessions-opinion_0.pdf.

[16] Nat'l Labor Relations Bd. v. Noel Canning, 134 S. Ct. 2550, 2574 (2014). The three recess appointments at issue were found to be constitutionally invalid.

[17] *Noel Canning*, 134 S. Ct. 2550, 2566-2567 (2014). The opinion gave as an example of an unusual circumstance an instance such as "a national catastrophe … that renders the Senate unavailable but calls for an urgent response." The Court noted that "political opposition in the Senate would not qualify as an unusual circumstance."

Position-Specific Temporary Appointment Provisions

In some cases, Congress has expressly provided for the temporary filling of vacancies in a particular advice and consent position. Generally, such provisions employ one or more of several methods: (1) a specified official is automatically designated as acting; (2) a specified official is automatically designated as acting, unless the President provides otherwise; (3) the President designates an official to serve in an acting capacity; or (4) the head of the agency in which the vacancy exists designates an acting official.

Method 1

The top positions at the Office of Management and Budget (OMB), the Federal Aviation Administration (FAA), and the Small Business Administration (SBA), among others, are temporarily filled through the first method.[18] For example, the *U.S. Code* provides that "[t]he Deputy Director [of OMB] acts as the Director when the Director is absent or unable to serve or when the office of Director is vacant."[19] The relevant statute states that, at the FAA, the "Deputy Administrator acts for the Administrator when the Administrator is absent or unable to serve, or when the office of the Administrator is vacant."[20] With regard to the SBA, federal law provides that the "Deputy Administrator shall be acting Administrator of the Administration during the absence or disability of the Administrator or in the event of a vacancy in the office of the Administrator."[21]

Method 2

The top positions at the General Services Administration (GSA) and Social Security Administration (SSA) are temporarily filled through the second method above, in which a specified official is automatically designated as acting, unless the President provides otherwise. With regard to GSA, the "Deputy Administrator is Acting Administrator ... during the absence or disability of the Administrator and, unless the President designates another officer of the Federal Government, when the office of Administrator is vacant."[22] Similarly, the "Deputy Commissioner [of SSA] shall be Acting Commissioner of the Administration during the absence or disability of the Commissioner and, unless the President designates another officer of the Government as Acting Commissioner, in the event of a vacancy in the office of the Commissioner."[23]

Method 3

Positions for which the President is authorized to designate an acting official—the third method above—include the General Counsel at the National Labor Relations Board and the Special Counsel for Immigration-Related Unfair Employment Practices at the Department of Justice. In

[18] 31 U.S.C. §502(b), 49 U.S.C. §106(i), and 15 U.S.C. §633(b)(1).

[19] 31 U.S.C. §502(b). If both the Director and Deputy Director are absent or unable to serve, or both positions are vacant, "the President may designate an officer of the Office to act as Director" (31 U.S.C. §502(f)).

[20] 49 U.S.C. §106(i).

[21] 15 U.S.C. §633(b)(1).

[22] 40 U.S.C. §302(b).

[23] 42 U.S.C. §902(b)(4).

the case of the General Counsel, the service of the President's designee is limited to a period that would allow the Senate to act on a nomination:

> In case of vacancy in the office of the General Counsel the President is authorized to designate the officer or employee who shall act as General Counsel during such vacancy, but no person or persons so designated shall so act (1) for more than forty days when the Congress is in session unless a nomination to fill such vacancy shall have been submitted to the Senate, or (2) after the adjournment sine die of the session of the Senate in which such nomination was submitted.[24]

The provision regarding the Special Counsel includes no such limitations: "In the case of a vacancy in the office of the Special Counsel the President may designate the officer or employee who shall act as Special Counsel during such vacancy."[25]

Method 4

In one manifestation of the fourth method, designation by agency head, in some departments and agencies, the agency head is empowered to establish a line of temporary succession in the event of a vacancy in a particular position. For the Department of Education, for example, the Deputy Secretary automatically takes over in the event of the Secretary's absence or disability, or when the position is vacant. In anticipation of potential vacancies in both positions, however, the Secretary is to establish a line of succession:

> The Secretary shall designate the order in which other officials of the Department shall act for and perform the functions of the Secretary during the absence or disability of both the Secretary and Deputy Secretary or in the event of vacancies in both of those offices.[26]

Other provisions allow agency heads to designate individuals to fill vacancies in lower level positions temporarily. For example, the Attorney General "may designate a person to perform the functions of and act as marshal," as long as that individual has not been rejected by the Senate for appointment to the position.[27] An individual appointed in this manner "may serve until the earliest of the following events: (1) [t]he entry into office of a United States marshal appointed [through the advice and consent process;] (2) [t]he expiration of the thirtieth day following the end of the next session of the Senate[;]" or (3) if the designee is nominated by the President and rejected by the Senate, "the expiration of the thirtieth day following such" rejection.[28] This provision also illustrates the kinds of limitations that are sometimes included in temporary appointment provisions.

Combinations of Tools

For at least three positions—U.S. Attorney, Solicitor of Labor, and Assistant Secretary of Labor for Mine Safety and Health—combinations of the tools identified here have been used to fill vacancies temporarily. By using more than one authority, the Administration has been able to place unconfirmed individuals in these positions for longer periods of time than would have been possible if only one authority had been used. With regard to U.S. Attorneys, the Office of Legal

[24] 29 U.S.C. §153(d).

[25] 8 U.S.C. §1324b(c)(1).

[26] 20 U.S.C. §3412(a)(1).

[27] 28 U.S.C. §562.

[28] Ibid.

Counsel at the Department of Justice determined, in 2003, that U.S. Attorney vacancies could be filled temporarily under specific provisions that allow for appointment by the Attorney General,[29] under the provisions of the Vacancies Act, or under a combination of these authorities in sequence.[30] The President temporarily filled vacancies in the two Labor Department positions by using, in succession, his recess appointment and Vacancies Act authorities. He recess appointed Eugene Scalia to be Solicitor of Labor on January 11, 2001. Several days before the appointment would have expired, at the close of the 107th Congress, Scalia stepped down from the Solicitor position and was appointed to a non-career Senior Executive Service position. With the position of Solicitor technically vacant, the President then gave Scalia a temporary appointment to the position, on November 22, 2002, under the Vacancies Act. It appears that Scalia could have served at least 210 days in this capacity, but he resigned from the post on January 6, 2003. A similar sequence of authorities was used to place Richard E. Stickler in the position of Assistant Secretary of Labor for Mine Safety and Health, first by recess appointment, on October 19, 2006, and later, under the Vacancies Act, on January 4, 2008.[31]

Unsuccessful Nominations and Payment Limitations

In some cases, individuals who are serving temporarily in advice and consent positions are also nominated to those positions. In the event that such a nomination is not successful, two provisions of law might subsequently prevent the individual from being paid as an acting official. Unlike the provisions of 5 U.S.C. §5503, which pertain to recess appointments alone and are discussed above, the following provisions appear to apply to any situation in which an individual is filling an advice and consent position on a temporary basis.

One provision from the FY2008 Financial Services and General Government Appropriations Act may prevent the official from being paid if the nomination is rejected. The provision reads, "Hereafter, no part of any appropriation contained in this or any other Act shall be paid to any person for the filling of any position for which he or she has been nominated after the Senate has voted not to approve the nomination of said person."[32] Similar provisions had been included in annual funding measures for most of, if not all of, the prior 50 years. As a practical matter, nominations are rarely rejected by a vote of the full Senate.

A second provision, addressing a different set of circumstances, prevents an individual serving in an acting or temporary capacity in an advice and consent position from being paid for his or her services if he or she has been nominated to the position twice and the second nomination has been withdrawn or returned. This second provision, which was included in the FY2009 Financial Services and General Government Appropriations Act, states:

> Effective January 20, 2009, and for each fiscal year thereafter, no part of any appropriation contained in this or any other Act may be used for the payment of services

[29] 28 U.S.C. §546.

[30] A September 5, 2003, opinion by the Office of Legal Counsel at the Department of Justice stated that the Vacancies Act could be used singly or in combination with 28 U.S.C. §546 to temporarily fill U.S. Attorney positions. (This opinion may be found at http://www.justice.gov/sites/default/files/olc/opinions/2003/09/31/op-olc-v027-p0149_0.pdf.)

[31] The White House press release announcing Stickler's recess appointment may be found at http://georgewbush-whitehouse.archives.gov/news/releases/2006/10/20061019-8.html, and the news release on his subsequent appointment may be found at http://georgewbush-whitehouse.archives.gov/news/releases/2008/01/20080104-5.html.

[32] P.L. 110-161, Div. D, Title VII, §709; 121 Stat. 2021; 5 U.S.C. prec. §5501.

> to any individual carrying out the responsibilities of any position requiring Senate advice and consent in an acting or temporary capacity after the second submission of a nomination for that individual to that position has been withdrawn or returned to the President.[33]

Consultants

At times, a nominee could be hired as a consultant while awaiting confirmation, but he or she may serve only in an advisory capacity and may not be installed in the office to which he or she has been nominated. A nominee to a Senate-confirmed position has no legal authority to assume the responsibilities of that position based on his or her status as a nominee; the authority comes with one of the limited-term appointments discussed above, with Senate confirmation and subsequent presidential appointment, or through occupying another position to which the authority of the vacant position has been delegated, as discussed below.[34]

Delegation of Duties to Another Official

As discussed in this report, the temporary filling of an advice and consent position is governed by the Vacancies Reform Act of 1998, the Recess Appointments Clause of the Constitution, and position-specific statutes. However, when the time limitations of the Vacancies Act have been exhausted, it may be possible for the functions of a vacant office to be carried out indefinitely by another individual, usually the first assistant, pursuant to a delegation of authority by the agency head.[35] In such instances, the official carries out these functions without assuming the vacant office. Generally, these functions may include any *except* those few that are statutorily vested specifically, and only, in the vacant office ("non-delegable duties").

In one such instance, described in a 2008 Government Accountability Office (GAO) opinion, the Office of Legal Counsel (OLC) at the Department of Justice was led by the Principal Deputy Assistant Attorney General for that office, Steven G. Bradbury, during a prolonged vacancy in the usual lead position, the Assistant Attorney General for OLC, after the time limitations of the Vacancies Act had been exhausted. The opinion states

> The issue remaining is whether Mr. Bradbury, as Principal Deputy Assistant Attorney General during the timeframe in which the office [of Assistant Attorney General for OLC] has been vacant, performed any functions or duties which under the Vacancies Act may be performed only by the Attorney General as head of the Department. According to the Department, Mr. Bradbury's service during the relevant time period has been in

[33] P.L. 111-8, Div. D, Title VII, §749; 123 Stat. 693; 5 U.S.C. prec. §5501.

[34] In *Buckley* v. *Valeo*, the Supreme Court held that "any appointee exercising significant authority pursuant to the laws of the United States is an 'Officer of the United States,' and must, therefore, be appointed in the manner prescribed" in Article II, Section 2, clause 2 of the Constitution (424 U.S. 1, 126 (1976)). This would appear to preclude consultants and nominees, who have not been so appointed, from exercising such authority. The exclusivity provision of the Vacancies Reform Act (5 U.S.C. §3347) is consistent with this interpretation. It establishes the act as the "exclusive means for temporarily authorizing an acting official to perform the functions and duties of" most advice and consent positions, unless otherwise expressly provided in law, or unless the President uses his recess appointment authority.

[35] Arguably, constitutional issues might arise if the functions of a *principal officer* of the United States, such as a Secretary, were carried out indefinitely by an official who had not been appointed to the position. Most advice and consent positions, however, are *inferior officers*. For a discussion of the distinction, see "Appointments Clause and Presidential Advisors" in CRS Report R40856, *The Debate Over Selected Presidential Assistants and Advisors: Appointment, Accountability, and Congressional Oversight*, by Barbara L. Schwemle et al.

> accordance with the Vacancies Act, since the position of Assistant Attorney General for OLC does not have any duties or functions which are exclusive to the position.[36]

In contrast to limitations imposed by the Vacancies Act, the first assistant or other official carrying out these delegated functions during the vacancy need not have served in the agency for a specified period prior to carrying out these duties. He or she might or might not occupy another advice and consent position. He or she may be a career or non-career appointee.

Author Contact Information

Henry B. Hogue
Analyst in American National Government
hhogue@crs.loc.gov, 7-0642

[36] U.S. Government Accountability Office, *Federal Vacancies Reform Act of 1998 - Assistant Attorney General for the Office of Legal Counsel, U.S. Department of Justice*, B-310780, June 13, 2008, pp. 3-4, available at http://www.gao.gov/products/A82394.

April 6, 2016

DOJ Announces One-Year FCPA Enforcement Pilot Program

Beth Forsythe

The U.S. Department of Justice ("DOJ") Criminal Division yesterday announced that its Fraud Section's Foreign Corrupt Practices Act ("FCPA") Unit is conducting a one-year FCPA enforcement pilot program ("Program"). A company that discovers a violation of the FCPA and meets the Program's exacting requirements related to voluntary disclosure, full cooperation, and appropriate remediation will be eligible to receive substantial mitigation credit. That mitigation credit may include a 50% reduction from the bottom of the U.S. Sentencing Guidelines fine range, avoidance of a requirement to appoint a corporate monitor for the typical 3- or 5-year period, and a possible declination of prosecution.

In his 9-page memorandum ("FCPA Enforcement Plan") describing the details of the Program, attached, Fraud Section Chief Andrew Weissmann explains that the credit contemplated by the Program is in addition to any fine reduction or mitigation credit applicable based on the Sentencing Guidelines or Principles of Federal Prosecution of Business Organizations, and that a company must still disgorge profits associated with the FCPA violation.

The requirements to qualify for credit in the program are more exacting than those outlined in the Sentencing Guidelines. First, a company must make a voluntary disclosure of the violation, which is defined as one the company is not otherwise required to make, or which is made under imminent threat of disclosure, and which consists of all known relevant facts, including about individuals involved in the violation. Second, full cooperation is required. The FCPA Enforcement Plan describes 11 items required to receive credit for full cooperation, including proactive disclosure of all relevant facts (not just those specifically requested), provision of all facts related to potential criminal conduct by any third party company or individual, and coordination of overseas data collection and witness interviews. Finally, a company must show that it has made timely and appropriate remediation, which includes implementation of an effective compliance and ethics program, appropriate discipline of employees, and any additional steps to show recognition of the seriousness of the misconduct.

A company that does not satisfy the voluntary disclosure requirement but does achieve full cooperation and appropriate remediation will receive, at most, a 25% reduction off the bottom of the Sentencing Guidelines fine range.

The Program is effective for self-disclosures of FCPA violations to the DOJ's Fraud Section for one year beginning April 5, 2016. The Fraud Section will determine by the end of that year whether to extend or modify the Program.

The Program is one of three elements of the Fraud Section's broader FCPA enforcement plan, as outlined in Weissmann's memorandum. Another element, announced last year, is the increase in enforcement resources, in the form of a 50% increase in prosecutors in the FCPA Unit and three new FBI squads devoted to FCPA investigations and prosecutions. The other element is the increased coordination with foreign counterparts by sharing leads, documents, and witnesses across borders. As stated in the FCPA Enforcement Plan and in comments yesterday by Criminal Division Chief Leslie Caldwell, by these efforts, DOJ is trying to send a message that fewer FCPA violations will go undetected, inspire voluntary self-disclosure of foreign bribery, and increase prosecutions of individuals responsible for related criminal activity.

April 5, 2016

U.S. Department of Justice

Criminal Division

Fraud Section

Washington, D.C. 20530

The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance[1]

Bribery of foreign officials to gain or retain a business advantage poses a serious systemic criminal problem across the globe. It harms those who play by the rules, siphons money away from communities, and undermines the rule of law.

Accordingly, the Department of Justice (Department) is committed to enhancing its efforts to detect and prosecute both individuals and companies for violations of the Foreign Corrupt Practices Act (FCPA), which criminalizes various acts of bribery and related accounting fraud. This memorandum sets forth three steps in our enhanced FCPA enforcement strategy.

As the first and most important step in combatting FCPA violations, the Department is intensifying its investigative and prosecutorial efforts by substantially increasing its FCPA law enforcement resources. These new resources will significantly augment the ability of the Criminal Division's Fraud Section and the Federal Bureau of Investigation (FBI) to detect and prosecute individuals and companies that violate the FCPA. Specifically, the Fraud Section is increasing its FCPA unit by more than 50% by adding 10 more prosecutors to its ranks. At the same time, the FBI has established three new squads of special agents devoted to FCPA investigations and prosecutions.[2] The Department's demonstrated commitment to devoting additional resources to FCPA investigations and prosecutions should send a message to

[1] This memorandum is for internal use only and does not create any privileges, benefits, or rights, substantive or procedural, enforceable by any individual, organization, party or witness in any administrative, civil, or criminal matter.

[2] The Fraud Section of the Criminal Division has been given the authority to investigate and prosecute criminal violations of the FCPA, *see* USAM 9-47-110, exclusively administers the FCPA Opinion program and, together with the Securities and Exchange Commission, publishes comprehensive centralized guidance on the FCPA. As recognized by theDepartment, FCPA investigations involve unique challenges that present a compelling need for centralized supervision, guidance, and resolution, including complex issues involving transnational detection, collection of evidence, and enforcement. The Fraud Section, however, will frequently partner with the United States Attorneys' Offices on such matters.

wrongdoers that FCPA violations that might have gone uncovered in the past are now more likely to come to light.

Second, the United States is not going at this alone. The Department is strengthening its coordination with foreign counterparts in the effort to hold corrupt individuals and companies accountable. Law enforcement around the globe has increasingly been working collaboratively to combat bribery schemes that cross national borders. In short, an international approach is being taken to combat an international criminal problem. We are sharing leads with our international law enforcement counterparts, and they are sharing them with us. We are also coordinating to more effectively share documents and witnesses. The fruits of this increased international cooperation can be seen in the prosecutions of both individuals and corporations, in cases involving Archer Daniels Midland, Alcoa, Alstom, Dallas Airmotive, Hewlett-Packard, IAP, Marubeni, Vadim Mikerin, Parker Drilling, PetroTiger, Total, and VimpelCom, among many others.

Third, as set forth below, the Fraud Section is conducting an FCPA enforcement pilot program. The principal goal of this program is to promote greater accountability for individuals and companies that engage in corporate crime by motivating companies to voluntarily self-disclose FCPA-related misconduct, fully cooperate with the Fraud Section, and, where appropriate, remediate flaws in their controls and compliance programs. If successful, the pilot program will serve to further deter individuals and companies from engaging in FCPA violations in the first place, encourage companies to implement strong anti-corruption compliance programs to prevent and detect FCPA violations, and, consistent with the memorandum of the Deputy Attorney General dated September 9, 2015 ("DAG Memo on Individual Accountability"), increase the Fraud Section's ability to prosecute individual wrongdoers whose conduct might otherwise have gone undiscovered or been impossible to prove.

We aim to accomplish this goal of greater accountability in part through the increased enforcement measures discussed above – adding additional agents and prosecutors to investigate criminal activity, and enhancing our cooperation with foreign law enforcement authorities where possible. And we also aim to accomplish the same goal by providing greater transparency about what we require from companies seeking mitigation credit for voluntarily self-disclosing misconduct, fully cooperating with an investigation, and remediating, and what sort of credit those companies can receive if they do so consistent with these requirements. Mitigation credit will be available only if a company meets the mandates set out below, including the disclosure of all relevant facts about the individuals involved in the wrongdoing. Moreover, to be eligible for such credit, even a company that voluntarily self-discloses, fully cooperates, and remediates will be required to disgorge all profits resulting from the FCPA violation.

The balance of this memorandum sets forth the Fraud Section's guidance ("Guidance") to our FCPA attorneys about how the Fraud Section will pursue the pilot program. The Guidance first sets forth the standards for what constitutes (1) voluntary self-disclosure of criminality, (2)

full cooperation, and (3) remediation by business organizations, for purposes of qualifying for mitigation credit from the Fraud Section in an FCPA matter. Next, the Guidance explains the credit that the Fraud Section will accord under this pilot to business organizations that voluntarily self-disclose, fully cooperate, and remediate. As set forth below, that credit may affect the type of disposition, the reduction in fine, or the determination of the need for a monitor.

By way of background, the Principles of Federal Prosecution of Business Organizations (the "USAM Principles") have long provided guidance on whether a criminal disposition against a company is appropriate and what form that disposition should take. *See* USAM 9-28.000. In addition, the United States Sentencing Guidelines ("Sentencing Guidelines") provide for reduced fines for business organizations that voluntarily disclose criminal conduct, fully cooperate, and accept responsibility for the criminal conduct. To provide incentives for organizations to self-disclose misconduct, fully cooperate with a criminal investigation, and timely and appropriately remediate, the Fraud Section has historically provided business organizations that do such things with a reduction below the low end of the Sentencing Guidelines fine range. These fine reductions and other incentives have not previously been articulated in a written framework. By setting forth this Guidance, we intend to provide a clear and consistent understanding of the circumstances in which the Fraud Section may accord additional credit in FCPA matters to organizations that voluntarily disclose misconduct, fully cooperate, and timely and appropriately remediate.

The Guidance does not supplant the USAM Principles. Prosecutors must consider the ten factors set forth in the USAM when determining how to resolve criminal investigations of organizations. Prosecutors must also calculate the appropriate fine range under Chapter 8 of the Sentencing Guidelines. This Guidance, by contrast, sets forth the circumstances in which an organization can receive additional credit in FCPA matters, above and beyond any fine reduction provided for under the Sentencing Guidelines, and the manner in which that additional credit should be determined, whether it be in the type of disposition, the extent of reduction in fine, or the determination of the need for a monitor. Organizations that voluntarily self-disclose, fully cooperate, and remediate will be eligible for significant credit in all three categories. But, as noted above, to receive this additional credit under the pilot program, organizations must meet the standards described below, which are more exacting than those required under the Sentencing Guidelines.

The pilot program will be effective April 5, 2016 as part of a one-year program applicable to all FCPA matters handled by the Fraud Section. The Guidance is being applied by the Fraud Section to organizations that voluntarily self-disclose or cooperate in FCPA matters during the pilot period, even if the pilot thereafter expires. By the end of this pilot period, the Fraud Section will determine whether the Guidance will be extended in duration and whether it should be modified in light of the pilot experience. The Guidance applies only to the Fraud Section's FCPA Unit and not to any other part of the Fraud Section, the Criminal Division, the

United States Attorneys' Offices, any other part of the Department of Justice, or any other agency.

Nothing in the Guidance is intended to suggest that the government can require business organizations to voluntarily self-disclose, cooperate, or remediate. Companies remain free to reject these options and forego the credit available under the pilot program.

This Guidance first sets forth the requirements for a company to qualify for credit for voluntary self-disclosure, cooperation, and timely and appropriate remediation under this pilot program, including exceptions to the general rules. It then sets forth the credit that should be accorded if a company meets these criteria.

A. Requirements

1. Voluntary Self-Disclosure in FCPA Matters

Voluntary self-disclosure of an FCPA violation is encouraged. Indeed, in implementing the DAG Memo on Individual Accountability, the Department recently revised the USAM Principles to underscore the importance of voluntary self-reporting of corporate wrongdoing. Under the current USAM Principles, prosecutors are to consider a corporation's timely and voluntary self-disclosure, both as an independent factor and in evaluating the company's overall cooperation and the adequacy of the company's compliance program. USAM 9-28.900.

In evaluating self-disclosure during this pilot, the Fraud Section will make a careful assessment of the circumstances of the disclosure. A disclosure that a company is required to make, by law, agreement, or contract, does not constitute voluntary self-disclosure for purposes of this pilot. Thus, the Fraud Section will determine whether the disclosure was already required to be made. In addition, the Fraud Section will require the following items for a company to receive credit for voluntary self-disclosure of wrongdoing under this pilot:

- The voluntary disclosure qualifies under U.S.S.G. § 8C2.5(g)(1) as occurring "prior to an imminent threat of disclosure or government investigation";
- The company discloses the conduct to the Department "within a reasonably prompt time after becoming aware of the offense," with the burden being on the company to demonstrate timeliness; and
- The company discloses all relevant facts known to it, including all relevant facts about the individuals involved in any FCPA violation.

2. Full Cooperation in FCPA Matters

In addition to the USAM Principles, the following items will be required for a company to receive credit for full cooperation under this pilot (beyond the credit available under the Sentencing Guidelines)[3]:

- As set forth in the DAG Memo on Individual Accountability, disclosure on a timely basis of all facts relevant to the wrongdoing at issue, including all facts related to involvement in the criminal activity by the corporation's officers, employees, or agents;

- Proactive cooperation, rather than reactive; that is, the company must disclose facts that are relevant to the investigation, even when not specifically asked to do so, and must identify opportunities for the government to obtain relevant evidence not in the company's possession and not otherwise known to the government;

- Preservation, collection, and disclosure of relevant documents and information relating to their provenance;

- Provision of timely updates on a company's internal investigation, including but not limited to rolling disclosures of information;

- Where requested, de-confliction of an internal investigation with the government investigation;

- Provision of all facts relevant to potential criminal conduct by all third-party companies (including their officers or employees) and third-party individuals;

- Upon request, making available for Department interviews those company officers and employees who possess relevant information; this includes, where appropriate and possible, officers and employees located overseas as well as former officers and employees (subject to the individuals' Fifth Amendment rights);

- Disclosure of all relevant facts gathered during a company's independent investigation, including attribution of facts to specific sources where such attribution does not violate the attorney-client privilege, rather than a general

[3] If a company claims that it is impossible to meet one of these requirements, for example because of conflicting foreign law, the Fraud Section should closely evaluate the validity of that claim and should take the impediment into consideration in assessing whether the company has fully cooperated. The company will bear the burden of establishing why it cannot meet one of these requirements.

narrative of the facts;

- Disclosure of overseas documents, the location in which such documents were found, and who found the documents (except where such disclosure is impossible due to foreign law, including but not limited to foreign data privacy laws);
    - Note: Where a company claims that disclosure is prohibited, the burden is on the company to establish the prohibition. Moreover, a company should work diligently to identify all available legal bases to provide such documents.
- Unless legally prohibited, facilitation of the third-party production of documents and witnesses from foreign jurisdictions; and
- Where requested and appropriate, provision of translations of relevant documents in foreign languages.

Cooperation comes in many forms. Once the threshold requirements of the DAG Memo on Individual Accountability have been met, the Fraud Section should assess the scope, quantity, quality, and timing of cooperation based on the circumstances of each case when assessing how to evaluate a company's cooperation under this pilot. For example, the Fraud Section does not expect a small company to conduct as expansive an investigation in as short a period of time as a Fortune 100 company.[4] Nor do we generally expect a company to investigate matters unrelated in time or subject to the matter under investigation in order to qualify for full cooperation credit. An appropriately tailored investigation is what typically should be required to receive full cooperation credit; the company may, of course, for its own business reasons seek to conduct a broader investigation.[5]

As set forth in USAM 9-28.720, eligibility for full cooperation credit is not predicated upon waiver of the attorney-client privilege or work product protection and none of the requirements above require such waiver. Nothing in the Guidance or the DAG Memo on Individual Accountability alters that policy, which remains in full force and effect. Furthermore, not all companies will satisfy all the components of full cooperation, either because they decide

[4] Where a company of any size asserts that its financial condition impairs its ability to cooperate more fully, the company will bear the burden to provide factual support for such an assertion.

[5] For instance, absent facts to suggest a more widespread problem, evidence of criminality in one country, without more, would not lead to an expectation that an investigation would need to extend to other countries. By contrast, evidence that the corporate team engaged in criminal misconduct in overseeing one country also oversaw other countries would normally trigger the need for a broader investigation. In order to provide clarity as to the scope of an appropriately tailored investigation, the business organization (whether through internal or outside counsel, or both) is encouraged to consult with Fraud Section attorneys.

to cooperate only later in an investigation or they timely decide to cooperate but fail to meet all of the criteria listed above. In general, such companies should be eligible for some cooperation credit under this pilot if they meet the DAG Memo on Individual Accountability criteria, but the credit generally will be markedly less than for full cooperation, depending on the extent to which the cooperation was lacking.

3. Timely and Appropriate Remediation in FCPA Matters

Remediation can be difficult to ascertain and highly case specific. In spite of these difficulties, encouraging appropriate and timely remediation is important to reducing corporate recidivism and detecting and deterring individual wrongdoing. The Fraud Section's Compliance Counsel is assisting us in refining our benchmarks for assessing compliance programs and for thoroughly evaluating an organization's remediation efforts.

In evaluating remediation efforts under this pilot program, the Fraud Section will first determine whether a company is eligible for cooperation credit; in other words, a company cannot fail to cooperate and then expect to receive credit for remediation despite that lack of cooperation. The following items generally will be required for a company to receive credit for timely and appropriate remediation under this pilot (beyond the credit available under the Sentencing Guidelines):

- Implementation of an effective compliance and ethics program, the criteria for which will be periodically updated and which may vary based on the size and resources of the organization, but will include:
    - Whether the company has established a culture of compliance, including an awareness among employees that any criminal conduct, including the conduct underlying the investigation, will not be tolerated;
    - Whether the company dedicates sufficient resources to the compliance function;
    - The quality and experience of the compliance personnel such that they can understand and identify the transactions identified as posing a potential risk;
    - The independence of the compliance function;
    - Whether the company's compliance program has performed an effective risk assessment and tailored the compliance program based on that assessment;
    - How a company's compliance personnel are compensated and promoted compared to other employees;
    - The auditing of the compliance program to assure its effectiveness; and

- The reporting structure of compliance personnel within the company.

- Appropriate discipline of employees, including those identified by the corporation as responsible for the misconduct, and a system that provides for the possibility of disciplining others with oversight of the responsible individuals, and considers how compensation is affected by both disciplinary infractions and failure to supervise adequately; and

- Any additional steps that demonstrate recognition of the seriousness of the corporation's misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risks.

B. Credit for Business Organizations under the Pilot Program

1. Limited Credit for Full Cooperation and Timely and Appropriate Remediation in FCPA Matters Without Voluntary Self-Disclosure

If a company has not voluntarily disclosed its FCPA misconduct in accordance with the standards set forth above, it may receive limited credit under this pilot program if it later fully cooperates and timely and appropriately remediates. Such credit will be markedly less than that afforded to companies that do self-disclose wrongdoing, as described immediately below in category B.2. Specifically, in circumstances where no voluntary self-disclosure has been made, the Fraud Section's FCPA Unit will accord at most a 25% reduction off the bottom of the Sentencing Guidelines fine range.

2. Credit for Voluntary Self-Disclosure, Full Cooperation, and Timely and Appropriate Remediation in FCPA Matters

When a company has voluntarily self-disclosed misconduct in an FCPA matter in accordance with the standards set forth above; has fully cooperated in a manner consistent with the DAG Memo on Individual Accountability and the USAM Principles; has met the additional stringent requirements of the pilot program; and has timely and appropriately remediated, the company qualifies for the full range of potential mitigation credit.

In such cases, if a criminal resolution is warranted, the Fraud Section's FCPA Unit:

- may accord up to a 50% reduction off the bottom end of the Sentencing Guidelines fine range, if a fine is sought; and

- generally should not require appointment of a monitor if a company has, at the time of resolution, implemented an effective compliance program.

Where those same conditions are met, the Fraud Section's FCPA Unit will consider a declination of prosecution.[6] As noted above, this pilot program is intended to encourage companies to disclose FCPA misconduct to permit the prosecution of individuals whose criminal wrongdoing might otherwise never be uncovered by or disclosed to law enforcement. Such voluntary self-disclosures thus promote aggressive enforcement of the FCPA and the investigation and prosecution of culpable individuals. Of course, in considering whether declination may be warranted, Fraud Section prosecutors must also take into account countervailing interests, including the seriousness of the offense: in cases where, for example, there has been involvement by executive management of the company in the FCPA misconduct, a significant profit to the company from the misconduct in relation to the company's size and wealth, a history of non-compliance by the company, or a prior resolution by the company with the Department within the past five years, a criminal resolution likely would be warranted.

As stated above, this Guidance applies only to the Fraud Section's FCPA Unit during the term of this pilot program. It does not apply to any other part of the Fraud Section, the Criminal Division, the United States Attorneys' Offices, any other part of the Department of Justice, or any other agency.

Andrew Weissmann
Chief, Fraud Section
Criminal Division

[6] As noted above, to qualify for any mitigation credit under this pilot (whether in categories B.1 or B.2), the company should be required to disgorge all profits from the FCPA misconduct at issue.

AN A.S. PRATT PUBLICATION
MARCH 2016
VOL. 2 • NO. 3

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 2 **NUMBER 3** **March 2016**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3000
Fax Number . . . . . (518) 487-3584
Customer Service Web site . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3000

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt);
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

An A.S. Pratt® Publication

Editorial Office
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
www.lexisnexis.com

MATTHEW BENDER

(2016–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

PRATT'S GOVERNMENT CONTRACTING LAW REPORT is published twelve times a year by Matthew Bender & Company, Inc. POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 630 Central Avenue, New Providence, NJ 07974.

Corporations as Whistleblowers: Leveraging Corporations to Fight Corporate Crime

By John R. Marti and Alex Hontos*

Slowly and surely, Congress and federal agencies are pressuring corporations into becoming part of the government's team combating corporate crime. In this article, the authors address the following questions: how did we get here, why the change, and what could come next? Understanding these questions is critical for organizations and their counsel as they assess where to invest compliance resources, how to respond to government inquiries and whistleblower complaints, and, more fundamentally, how to measure risk in the new investigate-and-disclose environment.

Over the past decade, the Department of Justice has obtained record breaking criminal and civil settlements targeting corporate misconduct. This success has not, however, been matched by successful prosecutions of corporate officers. The result—fierce political and public criticism.[1] The Department's reaction to this pressure is not new or revolutionary but exhibits a return to a longstanding strategy—leverage defendants into cooperating against other defendants. Yet this strategy comes with a twist—now the Department is leveraging corporations into cooperating against their officers and employees and thereby shifting more of the burden for investigating corporate crime, including the conduct of corporate employees, onto the backs of corporations.

BACKGROUND

Throughout our country's history, a natural person was under no obligation to incriminate himself by voluntarily telling law enforcement about his own

---

* John R. Marti is a partner at Dorsey & Whitney LLP, helping organizations respond to external and internal enforcement problems. From 1997 to 2015, he served as a white collar prosecutor with the U.S. Department of Justice, first as a trial attorney in the Fraud Section, Criminal Division, and from 2000 to 2015 with the U.S. Attorney's Office for the District of Minnesota, where he also served as the Acting U.S. Attorney and the First Assistant U.S. Attorney. Alex Hontos is an associate at the firm, focusing his practice on the intersection of industry and government. From 2009 until 2014, he served as a trial attorney in the Civil Division at the United States Department of Justice in Washington, D.C., where he represented the United States in government-contract claims, bid protests, and fraud claims. The authors may be contacted at marti.john@dorsey.com and hontos.alex@dorsey.com, respectively.

[1] *E.g.,* Russell Mokhiber, *The Failure to prosecute corporate crime undermines U.S. justice*, Reuters (April 30, 2013), http://blogs.reuters.com/great-debate/2013/04/30/the-failure-to-prosecute-corporate-crime-undermines-u-s-justice/.

misconduct.[2] A corporation historically was understood to be a private enterprise with many legal attributes of a natural person. As such, a corporation was generally under no affirmative obligation to disclose its own criminal conduct.[3] If a corporation's agents engaged in misconduct, the corporation would conduct an internal investigation to identify the scope and nature of the misconduct but, like a private citizen, it did not have to share that information with the government. If a corporation disclosed its misconduct, it would incriminate itself and possibly its employees. If the corporation did not self-disclose, there was limited risk that the government might discover the misconduct. In evaluating the costs and benefits, the corporation might remain silent hoping misconduct would not be discovered before the statute of limitation expired.

Congress and regulatory agencies have attempted to influence a corporation's decision in favor of disclosure. Congress has used a carrot-and-stick approach, enacting statutes to add severe criminal, civil and administrative penalties, and collateral consequences like suspension and debarment from receiving government contracts or assistance funds that are the corporate equivalent of the death penalty, while creating incentives for corporations to self-disclose. The Department of Justice and other agencies have also issued internal policies hoping to do the same.[4] The goal of these strategies was to pressure corporations to self-disclose misconduct before a government investigation started. Pressuring self-disclosure has become a key element in the government's strategy in combating corporate crime.

The result—corporations that relent to the leverage and seek "cooperation credit" by self-incriminating may mitigate or avoid severe penalties. Corpora-

---

[2] *E.g.*, *State v. Wilson*, 80 Vt. 249, 67 Atl. 533 (1907) ("Mere neglect to inform the proper authorities of the commission of a crime and the identity of the felon is not in itself an offense, but such conduct becomes indictable only where the failure to report is coupled with an 'evil motive' to obstruct justice.").

[3] *Trustees of Dartmouth College v. Woodward*, 17 U.S. 518, 636 (1819) (Marshall, C. J.) ("A corporation is an artificial being, invisible, intangible, and existing only in contemplation of law . . . ."); *Marbury v. Brooks*, 20 U.S. [7 Wheat.] 556, 5 L. Ed. 522 (1822) (Marshal, C.J.) ("It may be the duty of a citizen to . . . proclaim every offense which comes to his knowledge; but the law which would punish him in every case, for not performing this duty, is too harsh").

[4] Over the past 25 years, the Department of Justice has issued numerous internal policies attempting to enhance the Department's leverage in combatting corporate crime while avoiding corporate push back for over aggressive law enforcement—particularly as law enforcement has sought access to corporate internal investigations protected by privilege. Jim Letten and Carol Montgomery, *The Yates Memo: What New Challenges To Expect*, January 3, 2016, http://www.law360.com/articles/738741/the-yates-memo-what-new-challenges-to-expect.

tions that chose to conceal or not disclose the misconduct may face draconian penalties. The government is offering bounties to employees with knowledge of the misconduct to turn in their employers. A corporation that adopts a strategy of remaining silent succeeds only if the misconduct remains undetected, and this has become a very risky strategy.

Incentivizing corporations to voluntarily self-incriminate is now a key enforcement strategy for federal corporate prosecutors. In 2015, the Deputy Attorney General of the Department of Justice, Sally Yates, instructed federal prosecutors to "leverage resources" in combatting corporate criminal conduct by pressuring corporations to incriminate themselves prior to the government becoming aware of possible misconduct, and by encouraging corporations to become whistleblowers against their employees.[5]

Yet a corporation is vulnerable to government investigations in one way that a natural person is not. A corporation does not have a Fifth Amendment right to remain silent.[6] Once the government becomes aware of corporate misconduct, prosecutors may subpoena the corporation to produce the incriminating information. As the Supreme Court noted, "[t]reating corporations as natural persons under the Fifth Amendment would have a detrimental impact on the Government's efforts to prosecute 'white-collar crime,' one of the most serious problems confronting law enforcement authorities."[7] Simply stated, a corporation can be compelled to tattle on itself and its employees. Slowly and surely, Congress and federal agencies are pressuring corporations into becoming part of the government's team combating corporate crime.

How did we get here, why the change, and what could come next? Understanding these questions is critical for organizations and their counsel as they assess where to invest compliance resources, how to respond to government inquiries and whistleblower complaints, and, more fundamentally, how to measure risk in the new investigate-and-disclose environment.

HOW DID WE GET HERE?

The federal government has long struggled with combatting corporate crime.

---

[5] Deputy Attorney General Sally Yates Memorandum, Individual Accountability for Corporate Wrongdoing, September 9, 2015 (hereinafter "Yates Memorandum") ("These challenges make it all the more important that the Department fully leverage its resources to identify culpable individuals at all levels in corporate cases."), http://www.justice.gov/dag/file/769036/download.

[6] *Hale v. Henkel*, 201 U.S. 43 (1906). While corporations can be compelled to disclose facts, corporations may assert attorney–client privilege, and may generally not be compelled to disclose privileged material.

[7] *Braswell v. United States*, 487 U.S. 99, 100 (1988).

During the Civil War, Congress became concerned about the government's inability to counter an explosion in procurement fraud by war profiteers, mostly in the defense industry. In 1863, Congress responded by enacting the False Claims Act ("FCA"). The FCA prohibited the submission of false claims for payment where federal funds are involved. Congress incentivized whistleblowers to disclose fraud to the government by providing substantial bounties to strategically leverage whistleblowers to augment the federal government's own investigative resources.

As one court noted, Congress "let loose a posse of ad hoc deputies to uncover and prosecute frauds against the government."[8]

In the 1980s, again in response to numerous news stories about widespread fraud in the defense industry,[9] Congress encouraged prosecutors to combat procurement fraud in the defense industry through a specialized unit, the Defense Procurement Fraud Unit.[10] Congress also amended the FCA to significantly expand incentives to whistleblowers and penalties for corporate wrongdoers.[11] And the Department of Defense and Department of Justice instituted a Voluntary Disclosure Program to reward corporations that voluntarily disclosed fraud to the government with a possible mitigation of penalties, while promising severe penalties (including debarment) for those corporations that concealed misconduct.[12]

This strategy of leveraging corporations to self-disclose misconduct expanded into numerous other areas, including the Foreign Corrupt Practices Act (1977),[13] the Antitrust Division's Leniency Program (1978),[14] the U.S.

---

[8] *United States ex rel. Milam v. Univ. of Tex. M.D. Anderson Cancer Center*, 961 F.2d 46, 49 (4th Cir. 1992).

[9] Final Report of the Packard Commission, June 1986 (issued after public criticism of DoD purchases of $600 toilet seats and $400 hammers), http://www.ndia.org/Advocacy/AcquisitionReformInitiative/Documents/Packard-Commission-Report.pdf.

[10] The DPFU was heavily criticized for its ineffectiveness in investigating defense industry corporations. *See* http://www.justice.gov/sites/default/files/jmd/legacy/2014/05/31/hear-j-99-56-1985.pdf.

[11] The law was again amended in 1986, again due to issues with military spending. Under President Ronald Reagan's military buildup, reports of massive fraud among military contractors had become major news, and Congress acted to strengthen the FCA. James B. Helmer Jr., *False Claims Act: Incentivizing Integrity for 150 Years for Rogues, Privateers, Parasites and Patriots*, 81 U. Cin. L. Rev. (2013).

[12] U.S. Attorney's Manual, Criminal Resource Manual Section 931 (Department of Defense Voluntary Disclosure Program), http://www.justice.gov/usam/criminal-resource-manual-931-department-defense-voluntary-disclosure-program.

[13] FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act, By the Criminal

Sentencing Guidelines and Principles of Prosecution for Business Organizations (1991),[15] and the EPA's Audit Policy (1995).[16] In the aftermath of the Enron, WorldCom and other financial and accounting frauds, Congress enacted the Sarbanes-Oxley Act of 2002 which included disclosure and whistleblower protections.[17] In the aftermath of the 2008 financial collapse, Congress again responded by creating the Dodd/Frank Whistleblower Program (2011).[18]

In each instance, the government created incentives to encourage corporate self-disclosure and incentivize whistleblowing. But the government has not always relied upon voluntary incentives, and at times has mandated that corporations both investigate and then disclose criminal conduct before the government otherwise learns about the conduct. If the government could compel corporations to disclose incriminating information in response to a subpoena, Congress decided to compel self-disclosure in response to statute.

When the securities markets collapsed in the late 1920s because of systemic fraud, Congress established affirmative mandatory disclosure obligations for businesses and individuals who participated in the nation's securities markets. To protect investors, Congress enacted a series of securities laws with mandated disclosures designed to force companies to make public information that investors would find pertinent to making investment decisions.[19]

Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission, November 14, 2012, p. 52 ("both DOJ and SEC place a high premium on self-reporting, along with cooperation and remedial efforts, in determining the appropriate resolution of FCPA matters"), http://www.justice.gov/criminal-fraud/fcpa-guidance.

[14] http://www.justice.gov/atr/leniency-program.

[15] Paula Desio, *An Overview of the Organizational Guidelines, United States Sentencing Commission* ("when the Commission promulgated the organizational guidelines, it . . . incorporat[ed] into the sentencing structure the preventive and deterrent aspects of systematic compliance programs. The Commission did this by mitigating the potential fine range-in some cases up to 95 percent-if an organization can demonstrate that it had put in place an effective compliance program. This mitigating credit under the guidelines is contingent upon prompt reporting to the authorities and the non-involvement of high level personnel in the actual offense conduct"), http://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/ORGOVERVIEW.pdf.

[16] Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations, 60 Fed. Reg. 66706 (Dec. 22, 1995).

[17] 18 U.S.C.A. 1513(e).

[18] 17 CFR 240.21F-1 et seq. (the SEC provides monetary awards to eligible individuals who come forward with high-quality original information that leads to a Commission enforcement action in which over $1,000,000 in sanctions is ordered. The range for awards is between 10 percent and 30 percent of the money collected).

[19] Miller, Alison B., *Navigating the Disclosure Dilemma: Corporate Illegality and the Federal*

Congress enacted the Bank Secrecy Act in 1970 to mandate that financial institutions in the United States assist federal agencies to detect and prevent money laundering. In doing so, Congress created a duty on financial institutions to *investigate* criminal conduct.[20]

In the past decade, the federal government has broadened mandatory-disclosure requirements in the areas of procurement and assistance. When doing business with the government, Congress directed that corporations no longer have the discretion to decide whether to self-disclose.

In 2008, Congress passed the "Close the Contractor Fraud Loophole Act,"[21] which required that the Federal Acquisition Regulations be amended to "require timely notification by federal contractors of violations of federal criminal law or overpayments in connection with the award or performance of covered contracts or subcontracts, including those performed outside the United States and those for commercial items." Failure by a corporation to self-disclose could result in suspension and debarment.

In 2009, Congress enacted the Fraud Enforcement and Recovery Act ("FERA") which amended the FCA. Under the FERA, corporations that innocently obtain an overpayment of federal funds, but fail to timely report and return the overpayment, are subject to substantial damages and penalties under the FCA as "reverse false claims."[22] In 2013, on the assistance side of federal spending, the Office of Management and Budget issued its own mandatory disclosure rule which mandates that recipients of federal grants disclose "all violations of Federal criminal law involving fraud, bribery, or gratuity violations."[23]

Mandatory disclosure requirements give regulators and prosecutors leverage in discovering and investigating corporate crime. That was precisely the point. Yet the growth in disclosure incentives and mandates has not been accompanied by a growth in government investigative resources.

WHY THE CHANGE?

Complex corporate investigations require substantial law enforcement resources. Despite this reality, in at least the past 15 years, Congress and federal

---

Securities Laws, 102 Georgetown Law Journal 1647 (2014) (discussing corporate obligations to disclose criminal conduct under the federal securities laws).

[20] Public Law 91-508.

[21] Close the Contractor Fraud Loophole Act, Pub. L. No. 110-252, 122 Stat. 2386 (2008).

[22] 31 U.S.C. § 3729(a)(1)(G).

[23] 2 CFR 200.113 (Mandatory Disclosures).

law enforcement have contributed comparatively fewer resources to combatting corporate crime, all during a period when corporate crime dominated the news.

Following the terrorist attacks of September 11, 2001, federal law enforcement dramatically and appropriately realigned resources to answer the international terrorism threat. By FY 2004, the FBI had approximately 500 fewer agents investigating white collar crime matters than in 2000.[24] This rapid and dramatic realignment resulted in a 40 percent reduction in case initiations for financial crimes as compared to FY 2000.[25] The second largest generator of federal white collar criminal case referrals is the Internal Revenue Service's Criminal Investigations Division, which saw a similar drop in staffing, from 3,363 special agents in FY 1995 to a projected 2,139 agents in FY 2016.[26] The Securities and Exchange Commission's staffing levels also did not keep pace with industry growth.[27]

In 2008 and the years following, while the FBI and the Department of Justice were publicly pronouncing that they were committed to prosecuting mortgage fraud, mortgage fraud was a low priority in many FBI field offices.[28] At the same time, the federal government saw exploding deficits and a severe constriction in funding.[29] A Department of Defense Office of Inspector General report in March 2008 observed that investigation of contracting fraud is one area of many "that have dropped in priority and have largely been neglected."[30] The result—the Transactional Records Access Clearinghouse ("TRAC") at Syracuse University noted that as of 2015 "[f]ederal prosecution of individuals identified by the government as white collar criminals is at the

---

[24] DOJ OIG Report 05-37, Chapter 5, https://oig.justice.gov/reports/FBI/a0537/chapter5.htm#foc.

[25] DOJ OIG Report 05-37, Chapter 5, https://oig.justice.gov/reports/FBI/a0537/.

[26] IRS CI Fiscal Year 2014 National Operations Annual Business Report, page 5, https://www.irs.gov/pub/foia/ig/ci/REPORT-FY2014-IRS-CI-Annual-Report.pdf.

[27] SEC: In Brief, FY 2013 Congressional Justification, p.2, https://www.sec.gov/about/secfy13congbudgjust.pdf.

[28] DOJ OIG Report 14-12, Audit of the Department of Justice's Efforts to Address Mortgage Fraud, March 2014, https://oig.justice.gov/reports/2014/a1412.pdf.

[29] DOJ OIG Top Management and Performance Challenges Facing the Department of Justice, November 10, 2015, https://oig.justice.gov/challenges/2015.pdf#nameddest=1.

[30] Department of Defense Inspector General Growth Plan for Increasing Audit and Investigative Capabilities Fiscal Years 2008–2015 March 31, 2008, http://www.dodig.mil/IGInformation/IGInformationReleases/DoD%20IG%20March%2031%202008%20Report%20(FY08-15%20Growth%20Plan).pdf.

lowest level in the last twenty years . . . ."[31] Significantly, "[d]espite repeated claims to the contrary by top officials at the U.S. Department of Justice, the government's criminal prosecution of corporate violators has declined substantially in the last decade, falling by almost one third (29%) between FY 2004 and FY 2014."[32]

While law enforcement was being excoriated to do more to combat corporate crime and other misconduct, law enforcement agencies had fewer resources dedicated to combatting white collar crime, and fewer successes. The end result—only one top banker went to jail.[33] As one observer noted, "if . . . the Great Recession was in material part the product of intentional fraud, the failure to prosecute those responsible must be judged one of the more egregious failures of the criminal justice system in many years."[34]

Subject to intense criticism but lacking additional resources, the Department of Justice has returned to leverage—by pressuring corporations into taking on what historically has been a law enforcement responsibility and deputizing corporations as partners with law enforcement in the war on corporate crime. Corporations, and their employees, are now "G-men" too, or at least that is where the regulatory and enforcement landscape is trending.

WHAT COULD COME NEXT?

Corporate Whistleblowing

History has demonstrated that in every era involving the perception of substantial corporate wrongdoing, state and federal governments have responded by seeking more leverage. Absent a corporate Fifth Amendment privilege, the government may freely mandate that corporations tell law enforcement about internal criminal conduct, subject to available privileges. As history has demonstrated, the federal government increased incentives for disclosure. Next, governments adopted mandated disclosures. And now, with the Yates Memorandum, the Department of Justice is incentivizing corporations to become whistleblowers against their officers and employees. To

---

[31] http://trac.syr.edu/tracreports/crim/398/.

[32] http://trac.syr.edu/tracreports/crim/406/.

[33] Eisinger, Jesse, "Why Only One Top Banker Went to Jail for the Financial Crisis," New York Times Magazine, April 30, 2014, http://www.nytimes.com/2014/05/04/magazine/only-one-top-banker-jail-financial-crisis.html.

[34] Rakoff, Jed S., "The Financial Crisis: Why Have No High-Level Executives Been Prosecuted?" New York Review of Books, January 9, 2014 issue, http://www.nybooks.com/articles/2014/01/09/financial-crisis-why-no-executive-prosecutions/.

incentivize this behavior, federal prosecutors are holding out promises of amnesty or lesser sanctions. In effect, the Yates Memorandum has established a bounty system for corporations to whistle-blow on their employees.[35]

Splitting the Corporation/Officer Relationship

The government's pressure to leverage corporations against their employees is a similar strategy to that used to combat criminal conspiracies. Federal prosecutors have long used a threat of severe penalties to induce criminal conspirators to turn on one another. "[T]he Department of Justice views mandatory minimum penalties as an "essential" and "critical tool" in obtaining "cooperation from members of violent street gangs and drug distribution networks."[36] This argument is similar to the reasoning in the Yates Memorandum. For the first time, the Department of Justice's policy promises severe penalties in order to leverage corporations to turn on their employees in hopes of a sentencing benefit.

Furthermore, federal prosecutors may well increase suits against corporate officers under the FCA for civil damages (regardless of ability to pay). By suing corporate officers besides the corporation, prosecutors would likely inject conflict into the corporation-employee relationship, and may induce officers to cooperate against the corporation or other officers for some benefit.

Corporate Internal Investigations

Given the proliferation of mandatory disclosure requirements, and the multiplication of voluntary disclosure incentives, the time has come when corporations should assume that "internal" complaints and the facts discovered as a result of "internal" investigations will be disclosed. That is not to say that corporations will always be required to disclose and privileges may well still apply. But corporations should conduct internal investigations with the understanding that much of what is discovered and documented may end up in the hands of a prosecutor or an Inspector General or contracting officer. These pressures will affect the nature and tone of *Upjohn* warnings as well.[37]

---

[35] Perhaps the Deputy Attorney General has let loose a posse of corporations acting as ad hoc deputies to uncover and prosecute frauds against the government by corporate officers and employees.

[36] Report to the Congress: Mandatory Minimum Penalties in the Federal Criminal Justice System, United States Sentencing Commission, October 2011, page 89, http://www.ussc.gov/news/congressional-testimony-and-reports/mandatory-minimum-penalties/report-congress-mandatory-minimum-penalties-federal-criminal-justice-system.

[37] *Upjohn Co. v. United States*, 449 U.S. 383 (1981) (attorneys interviewing corporate employees give the Upjohn warning—also known as the corporate Miranda warning—to the

But Newton's Third Law teaches that with every action there is an equal and opposite reaction. Corporations may find that internal investigations are complicated when corporate officers (who are necessary witnesses) refuse to cooperate knowing that the interviews may be turned over to law enforcement. For some officers, remaining silent knowing that they may lose their job may be preferable to the consequences of confessing to misconduct in an internal investigation. And even if officers do cooperate, this tension will certainly undermine the trust necessary for effective employee/employer relationships and the continuity of business operations.

More Disclosure Requirements

Disclosure requirements are waxing, not waning. Expect Congress and agencies to place additional specific duties on corporations requiring additional disclosures. Historically, creating additional and expensive law enforcement overhead costs has been a reactive strategy that has not eliminated corporate criminal conduct.

Shifting investigative responsibility to corporations, and then requiring corporations to disclose findings, is perceived as far more cost effective in an era of sequestration and continuing resolutions.

Prosecutions for Not Disclosing

Where mandatory disclosures exist, federal prosecutors might prosecute for knowing failure to disclose. Yet there is little evidence that prosecutors have pursued corporate "misprision of felony" cases.[38] Under this statute, corporations that knowingly conceal and do not disclose knowledge of a felony may commit a felony. Currently, prosecutors only occasionally charge misprision in a white collar case, and even this decision reflects not a desire to charge misprision for its own sake but as a result of plea bargaining. With more mandatory disclosure requirements, look for aggressive federal prosecutors to leverage misprision as a short cut to a successful prosecution.

CONCLUSION

We should not be surprised that the Department of Justice is pressuring corporations to whistle-blow. Because of the Department's difficulties in combatting corporate crime and its reduced resources, the Department is turning to proven strategies and techniques—whistleblowing and leverage. Yet corporations are not criminal organizations, and the key question as the

---

employees so that they know that the corporation, not the employee, holds the privilege).

[38] 18 U.S.C. § 4.

Department continues to squeeze corporations is whether this strategy will be effective, counterproductive, or even politically palatable. Newton's Third Law has yet to fully play out. There is certainly more to come. But for organizations currently facing a government inquiry or responding to internal allegations of misconduct, or merely trying to determine where to invest compliance resources, understanding that we have entered a new paradigm, albeit one with deep historical roots, is critical to appropriately allocating resources and assessing risk.

February 24, 2016

Yates Memo in Action: No Cooperation Credit in FCPA Enforcement for Failing to Disclose Key Facts

Nelson Dong and John Marti

A recent case illustrates both the ongoing corruption risks for U.S. companies doing business in developing countries such as China and the Government's tougher stance on settling white collar crime cases. In this case, the U.S. Securities and Exchange Commission (SEC) and the U.S. Department of Justice (DOJ) alleged that two subsidiaries of PTC Inc. (PTC), a Massachusetts-based business software company, had bribed Chinese company officials with vacations to the United States and gifts and then actively concealed such illicit payments with elaborate false records, in violation of the Foreign Corrupt Practices Act (FCPA). PTC recently agreed to pay to the SEC and DOJ a combined $28.1 million to settle these alleged FCPA violations.

The DOJ investigation resulted in a deferred prosecution agreement (DPA) between DOJ and two of PTC's subsidiaries – Parametric Technology (Shanghai) Software Company Ltd. and Parametric Technology (Hong Kong) Ltd. – in exchange for PTC paying $14.5 million in criminal fines and improving its compliance program. PTC also agreed to pay $13.6 million in disgorgement of profits and interest in its separate civil settlement with the SEC.

The two federal agencies claimed that, between 2006 and 2011, PTC's two Chinese subsidiaries provided nearly $1.5 million in travel and hospitality expenses and extravagant gifts while bringing officials of several Chinese state-owned enterprises (SOEs) to the United States. Although PTC claimed the officials were training at its Massachusetts headquarters, the visits were actually disguised pleasure trips to destinations such as New York, Hawaii, Las Vegas, and California, according to the SEC and DOJ. During the trips, the Chinese officials typically spent only one day at PTC's headquarters but all the rest of their time in the United States touring and playing golf. PTC's subsidiaries in Shanghai and Hong Kong then reimbursed those officials for all their entertainment and travel expenses via third-party business partners and actively sought to conceal those payments as bona fide business expenses or sales commissions.

"PTC failed to stop illicit payments despite indications of potential corruption by agents working with its Chinese subsidiaries, and the misconduct continued unabated for several years," said Kara Brockmeyer, who heads the SEC Enforcement Division's FCPA Unit, in a statement on the settlement. The alleged bribes allowed PTC to obtain $13 million in contracts with Chinese SOEs, according to the agency announcements.

The SEC also announced its first DPA with an individual accused of FCPA violations. The agency said it will keep allegations against Yu Kai Yuan, a former employee at one of PTC's Chinese subsidiaries, on hold for three years for his assistance with the federal investigations.

This case reveals the unfortunate characteristic in many developing economies that many company officials are susceptible to (and even openly encouraging of) bribery in exchange for their favors in making business decisions. Moreover, in China, approximately fifty percent of that nation's huge economy is still operated through SOEs. SEC and DOJ enforcement staff have long considered that SOEs are government instrumentalities under the FCPA, making nominally "company" officials the legal equivalent of government agency employees. Consequently, bribing such corporate officials who might otherwise appear to be in the private sector and then concealing the bribes by false bookkeeping entries will bring such activity squarely within the FCPA.

Consistent with the DOJ's policy announced in last fall's Yates Memorandum, PTC did not receive voluntary disclosure credit or full cooperation credit because, at the time of its initial disclosure to the Government, it failed to disclose relevant facts that it had learned in connection with a prior internal investigation and did not disclose those facts until DOJ uncovered additional information independently and brought them to PTC's attention. (DOJ Press Release). Thus, the approximately $28.1 million in combined penalties, disgorgement, and interest paid by PTC was well over double the $13 million in contracts in China obtained by the two PTC subsidiaries through the improper payments and gifts.

Corporate management, especially financial officers, audit staff, compliance directors, and corporate counsel, should thus draw at least five key lessons from this PTC case:

- The FCPA will be applied forcefully to bribery cases involving bribes to "company" officials where, in mixed economies such as China, they are officials in SOEs and thus will be treated as if they were directly employed as government officials;
- The FCPA penalizes payment of "anything of value" to obtain foreign business and, although the officials did not receive outright cash payments, they did receive lavish paid trips that were virtual vacations, thinly disguised as business trips, as well as extravagant gifts;
- The FCPA can reach illicit conduct that occurs through foreign subsidiaries of U.S. companies as well as directly within the U.S. parent entity;
- A company can essentially declare its criminal intent under the FCPA to Government enforcement staff when it engages in elaborate ruses and false bookkeeping entries in a conscious and widespread effort to conceal its misconduct; and

- Even when a company's compliance staff uncovers misconduct and seeks to make a voluntary disclosure thereof to the Government, they must do so with complete candor and thus not hold back material information that the Government may later discover, causing the company to lose much of the credit it might otherwise have gained from such a disclosure under the Yates Memorandum standards, and resulting in harsher financial penalties when the company wants to enter into a DPA or other settlement of the case.

The administrative proceeding before the SEC is *In the Matter of PTC Inc.*, file number 3-17118.