THE DEPARTMENT OF JUSTICE'S EFFORTS TO COMBAT IDENTITY THEFT

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 10-21
March 2010

THE DEPARTMENT OF JUSTICE'S EFFORTS TO COMBAT IDENTITY THEFT

EXECUTIVE SUMMARY

The Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime. The Department of Justice (DOJ) and its components, particularly the Federal Bureau of Investigation (FBI) and United States Attorneys' Offices (USAO), along with many other federal, state, and local law enforcement agencies, play a vital role in combating this crime through the investigation and prosecution of identity thieves. DOJ's non-law enforcement components also play an important part in combating identity theft. For example, the Office of Justice Programs (OJP) funds programs that assist identity theft victims and OJP's Bureau of Justice Statistics compiles identity theft-related statistics.

According to recent estimates, identity theft is a growing problem. A Federal Trade Commission report estimated that 8.3 million Americans were victims of identity theft in 2005, resulting in losses of $15.6 billion. In June 2009, a Deputy Assistant Attorney General for the DOJ's Criminal Division testified that a more recent estimate suggested that identity theft was the fastest growing crime in 2008, victimizing more than 10 million Americans.

According to DOJ personnel, federal identity theft investigations most often relate to other federal crimes such as cyber intrusions, health care fraud, mortgage fraud, and credit card fraud. Identity theft can also be a significant element of violent crimes, such as domestic abuse and even terrorism, and a significant number of identity theft-related crimes originate overseas.

In recognition of the harm caused by identity theft, President George W. Bush signed an executive order on May 10, 2006, creating the President's Identity Theft Task Force (President's Task Force). The purpose of the President's Task Force was to "use federal resources effectively to deter, prevent, detect, investigate, proceed against, and prosecute unlawful use by persons of the identifying information of other persons." The President's Task Force was chaired by the Attorney General, with the Chairman of the Federal Trade Commission serving as the co-chair.

In April 2007, the President's Task Force issued a strategic plan that made recommendations to federal agencies involved in combating identity theft, including DOJ and some of its components. The President's Task Force

later issued a follow-up report in September 2008 detailing its efforts to ensure that the recommendations of the strategic plan were implemented. The follow-up report stated that much of the work recommended by the Task Force had been completed and described some efforts that were still ongoing. The Associate Deputy Attorney General who served as the Office of the Deputy Attorney General's point of contact to the President's Task Force told us that the September 2008 report was the Task Force's final report and the Task Force had no plans to reconvene.

OIG Audit Approach

The objective of this audit was to evaluate how DOJ has communicated and implemented its strategy to combat identity theft. To accomplish our objective we interviewed DOJ officials from the DOJ components involved in the Department's efforts to combat identity theft. Specifically, we interviewed officials from the Office of the Deputy Attorney General (ODAG), the Criminal Division, Executive Office for United States Attorneys (EOUSA), two USAOs, the FBI, the Office of Community Oriented Policing Services (COPS), as well as several offices and bureaus within OJP. We also interviewed representatives from several non-DOJ agencies involved in fighting identify theft including the Federal Trade Commission, U.S. Secret Service, U.S. Postal Inspection Service, Social Security Administration, and the not-for-profit National Center for Victims of Crime. In addition, we reviewed DOJ, EOUSA, Criminal Division, FBI, and OJP policies related to identity theft. Finally, we reviewed data provided by EOUSA and the FBI related to identity theft investigations, prosecutions, personnel resources, and victims.

Appendix I contains a more detailed description of our audit objective, scope, and methodology.

Results in Brief

Overall we found that DOJ components responsible for combating identity theft have undertaken various efforts to fight this widespread crime. Several of the initiatives were in response to recommendations made by the President's Task Force, while others were undertaken by the components before the Task Force was established. Although some of these efforts have had success, in other instances the components did not address the recommendations of the President's Task Force. We also found that to some degree identity theft initiatives have faded as priorities.

In addition, we found that DOJ has not developed a coordinated plan to combat identity theft separate from the recommendations of the

President's Task Force. Representatives from every DOJ component involved in this review told us that they have not received guidance from DOJ's leadership since the Task Force concluded its work. Further, DOJ did not assign any person or office with the responsibility to coordinate DOJ's efforts to combat identity theft and to ensure that DOJ components further implement the recommendations of the President's Task Force where appropriate. We believe the DOJ needs to ensure that its efforts to combat identity theft are coordinated and are given sufficient priority.

In our report, we make 14 recommendations to improve DOJ's efforts to combat identity theft. The remaining sections of this Executive Summary provide a further description of our audit findings.

DOJ Leadership

The Associate Deputy Attorney General who served as the ODAG's point of contact to the President's Task Force informed us that DOJ has not developed its own internal strategy to combat identity theft. Instead, DOJ currently considers the President's Task Force's strategic plan and its recommendations as still valid and applicable to DOJ components. However, the Associate Deputy Attorney General also noted that DOJ has not appointed any person or office with the responsibility for coordinating DOJ's identity theft efforts or ensuring that DOJ components consider and implement the President's Task Force recommendations when appropriate. According to the Associate Deputy Attorney General, in the absence of a responsible DOJ official or office, each DOJ component has been expected to implement the President's Task Force recommendations applicable to its operations.

Criminal Division

Pursuant to a request from the Attorney General, in October 2008 the Criminal Division established the Identity Theft Enforcement Interagency Working Group (Identity Theft Working Group).[1] The working group is led by the Criminal Division and meets monthly to discuss identity theft enforcement issues such as trends in prosecutions. Generally, the Identity Theft Working Group participants we interviewed said the meetings were informative and worthwhile. However, even though the Working Group has covered non-enforcement issues at times, some participants expressed concern that the group's primary focus on identity theft prosecutions is too

[1] Appendix II contains a list of the Identity Theft Enforcement Interagency Working Group members.

narrow and they believed that the group should devote greater attention to other matters, such as identity theft victim issues.

The Criminal Division also leads an informal training group that conducts identity theft seminars for state and local law enforcement agencies. Currently, the training group is organized by the Criminal Division's Fraud Section. In its 2008 report, the President's Task Force recognized the success of this training group and recommended that it increase the number of seminars offered each year. However, the training group organizer told us that the group's structure, with each of the participating agencies funding its own participation, makes it difficult to expand the training. Further, all of the training instructors are based in the Washington, D.C., area, making it costly to provide training in certain locations of the United States.

Although the Working Group has considered non-enforcement issues during its monthly meetings, we believe that DOJ should further expand the scope of the Identity Theft Working Group beyond its primary focus on prosecutions to more regularly address other identity theft-related topics, such as victims' issues and training initiatives. In addition, we believe that a more formal DOJ-led training group, with additional support from DOJ, could help to ensure that many more law enforcement officers and victim specialists receive training on how to prevent and investigate identity theft and to assist identity theft victims.

Executive Office for United States Attorneys and United States Attorneys' Offices

According to the President's Task Force, one of the shortcomings in the federal government's ability to understand and respond effectively to identity theft was the lack of comprehensive statistical data on law enforcement's efforts to combat it. In late 2006 EOUSA enhanced its case management and time management systems to better capture identity theft data. However, when we requested from EOUSA the totals for identity theft prosecutions, convictions, and personnel time spent on identity theft prosecutions, EOUSA officials informed us that the information provided should not be considered complete or a reliable indicator of the total of such work because not all USAOs have ensured compliance with the newly implemented collection requirements. An EOUSA official told us that the failure of some of these USAOs to adapt to the new collection requirements may be a result of technical difficulties with the information technology systems currently in use. The following table contains the identity theft prosecution data provided by EOUSA.

Number of Defendants Charged and Convicted Pursuant to the Federal Identity Theft and Aggravated Identity Theft Statutes Fiscal Years 2007 through 2009[2]

	Identity Theft		Aggravated Identity Theft		Totals[3]	
FY	Defendants Charged	Convictions Obtained	Defendants Charged	Convictions Obtained	Defendants Charged	Convictions Obtained
2007	269	103	532	272	744	365
2008	296	144	620	338	882	467
2009	239	138	578	296	769	432

Source: EOUSA

EOUSA also provided data, displayed in the following table, regarding the time spent by prosecutors handling identity theft cases. Again, EOUSA officials cautioned the OIG about the accuracy of these figures because, like the case data presented above, EOUSA officials did not believe that every USAO was properly attributing attorney time spent working on identity theft prosecutions.

Attorney Work Years Charged to Federal Identity Theft and Aggravated Identity Theft Prosecutions Fiscal Years 2007 through 2009[4]

Fiscal Year	Totals
2007	25.68
2008	39.71
2009	45.62

Source: EOUSA

[2] The number of convictions obtained is not a subset of the number of defendants charged during the particular fiscal year because cases charged in one year may be resolved with a conviction in a subsequent fiscal year. Further, convictions obtained are for identity theft and aggravated identity theft only. Instances where a defendant was charged with identity theft or aggravated identity theft and convicted of other charges are not reflected in the conviction totals.

[3] The totals reflected in this table eliminate double counting of defendants who were charged with or convicted of both identity theft and aggravated identity theft.

[4] According to EOUSA, the term "work year" is used when defining the productive efforts of one individual for one year. One work year for a federal employee is typically equal to 2080 hours.

In addition to improving data collection, the President's Task Force recommended that the federal government increase its identity theft prosecutions. It recommended specific steps that should be taken by all USAOs, including: (1) designating an identity theft coordinator for each USAO; (2) increasing use by USAOs of interagency working groups and task forces devoted to identity theft; (3) reevaluating monetary thresholds applied when assessing identity theft cases for prosecution; and (4) encouraging state prosecution of identity theft cases.

However, in our audit 28 of the 94 USAOs reported that they do not lead or do not participate in an identity theft task force or working group. Additionally, 7 of the 94 USAOs did not report to EOUSA whether they participate in an identity theft task force or working group. Furthermore, according to EOUSA, as of October 2009, 53 of the 94 USAOs did not report reevaluating their monetary thresholds or encouraging state prosecution of identity theft.

Although we found that EOUSA has made an effort to implement the recommendations of the President's Task Force, some USAOs have not fully embraced those efforts. We believe that greater leadership from DOJ and EOUSA on the importance of identity theft initiatives could lead to larger emphasis in this area by USAOs. We recommend that EOUSA transmit a follow-up memorandum to all USAOs requiring each office to report on its current identity theft efforts, including the status of its efforts related the President's Task Force recommendations. We believe that gathering such information will allow DOJ and EOUSA to better understand DOJ's overall identity theft enforcement efforts and assist DOJ in prioritizing future identity theft initiatives.

Federal Bureau of Investigation

Although the specific crime of identity theft is not a top FBI priority, the FBI frequently addresses identity theft through the Cyber Division's criminal intrusion program, which is currently a top FBI priority. According to a senior FBI official, the FBI determined that it must prioritize the use of its resources, and he believed that the FBI would have the greatest impact on identity theft by primarily addressing the crime through its Cyber Division.

According to the FBI's fiscal year (FY) 2006 *Financial Crimes Report to the Public*, the FBI investigated 1,255 pending identity theft-related cases in FY 2006. The FBI report stated that those investigations resulted in 457 indictments and 405 convictions of identity theft criminals. We requested similar information from the FBI for FYs 2007 through 2009.

However, the FBI stated that it was unable to provide this information. According to FBI officials, the FBI no longer collects data on investigations or convictions that involve identity theft.

In addition, according to FBI personnel we interviewed, in FY 2005 the FBI's Criminal Investigative Division (CID), in conjunction with the Cyber Division, prepared a comprehensive assessment describing the identity theft threat and periodically updated the assessment until 2007. However, according to FBI officials, the FBI does not currently require such comprehensive assessments on identity theft. Although comprehensive identity theft assessments are not required, FBI officials informed us that it has identity theft intelligence collection requirements. Since FY 2007, these intelligence collection requirements have led to the publication of 21 intelligence assessments and bulletins, which resulted from 428 intelligence information reports. However, the FBI recognized that its identity theft intelligence collection requirements are outdated and need to be reviewed.

We are concerned about the FBI's lack of identity theft data and mandatory comprehensive assessments on the threat of identity theft. Without such data and comprehensive assessments the FBI cannot maintain a current understanding of the threat presented by identity theft or properly coordinate its approach to a crime that cuts across multiple FBI program areas, including counterterrorism, and victimizes millions of Americans each year.

Victim Assistance

Federal law requires that victims of federal crimes be afforded certain rights, and that DOJ officers and employees engaged in the detection, investigation, and prosecution of crime make their best efforts to ensure that crime victims are notified of and accorded their rights under federal law. The most recent version of the Attorney General Guidelines for Victim and Witness Assistance, issued in 2005, included a specific provision relating to identity theft victims. However, we found that this provision has caused confusion among DOJ investigators, prosecutors, and victim specialists regarding their responsibilities to identify and notify victims of identity theft. For example, the identity theft provision of the Attorney General Guidelines does not distinguish between direct and indirect victims of identity theft, although federal law makes this distinction.

We recommend that DOJ, EOUSA, the Criminal Division, and the FBI review relevant federal laws and the current Attorney General Guidelines for Victim and Witness Assistance and issue clear guidance to DOJ components

to ensure that they follow a uniform policy and take the legally required steps to identify and notify victims of identity theft.

Office of Justice Programs

OJP's Bureau of Justice Statistics (BJS) annually conducts the National Crime Victimization Survey. In July 2004, BJS added identity theft-related questions to this survey. However, we found that the surveys are not published in a timely manner. The 2004 and 2005 results (the first 2 survey years that included identity theft questions) were not published until April 2006 and November 2007, respectively. BJS currently estimates that due to resource limitations the 2006 survey results on identity theft will not be published until the summer of 2010. In addition, in cooperation with the FTC, BJS conducted a more comprehensive identity theft survey covering the first 6 months of 2008. These results will not be published until the fall of 2010.

Timely and accurate statistics inform DOJ on the prevalence and scope of the identity theft problem. Such statistics can also help DOJ and other agencies' law enforcement components recognize trends and areas for enhanced enforcement operations. BJS's reporting takes on greater importance in view of the lack of data being collected by the FBI, as discussed above, and the Federal Trade Commission, which according to officials we interviewed has no plans to conduct future identity theft surveys.

Conclusions and Recommendations

DOJ has not developed its own comprehensive strategy to combat identity theft. Instead, DOJ relies on the President's Task Force strategic plan as being valid and applicable to all DOJ components. Yet, DOJ has not designated any person or office with the responsibility of coordinating DOJ's identity theft efforts, including ensuring that the recommendations of the President's Task Force are appropriately implemented. This lack of a coordinator responsible for the DOJ's identity theft efforts has led to an uncoordinated, and sometimes nonexistent, approach by DOJ components to address identity theft. Additionally, DOJ does not currently have a mechanism to assess whether the recommendations of the Task Force remain relevant, or whether changes in the DOJ's approach are necessary.

We believe that additional DOJ leadership is needed to ensure that DOJ's overall efforts to combat identity theft are coordinated and prioritized. Therefore, we recommend that DOJ coordinate its identity theft efforts, based on a review the President's Task Force's strategic plan and consultation with the relevant components involved in identity theft issues.

DOJ should also reaffirm to all DOJ components that the President's Task Force's strategic plan is applicable to them and that the components should ensure the further implementation of the recommendations where appropriate. We also recommend that DOJ and all components involved in identity theft issues designate an official or office with responsibility for monitoring their agency's identity theft efforts. DOJ should require all such designees to meet periodically with DOJ's designee to consider adjustments to the DOJ's approach to identity theft when appropriate.

Our audit work and findings resulted in 14 recommendations to the Department of Justice and its components to improve their efforts to combat identity theft.

THE DEPARTMENT OF JUSTICE'S EFFORTS TO COMBAT IDENTITY THEFT

TABLE OF CONTENTS

THE DEPARTMENT OF JUSTICE'S EFFORTS TO COMBAT IDENTITY THEFT

Introduction

In 1998, the U.S. Congress made identity theft a federal crime.[5] According to Department of Justice (DOJ) personnel, identity theft is most often investigated when it relates to other crimes, such as cyber intrusions, health care fraud, mortgage fraud, and credit card fraud. Identity theft can also be a significant element of violent crimes, such as domestic abuse and even terrorism, and a significant number of identity theft-related crimes originate overseas.

According to the most recent Federal Trade Commission (FTC) statistics available, approximately 8.3 million Americans were victims of some form of identity theft in 2005.[6] The FTC reported that these identity thefts resulted in losses estimated at $15.6 billion.[7] In June 2009, a Deputy Assistant Attorney General of the DOJ Criminal Division testified before Congress that in 2008 an estimated 10 million Americans were victims of identity theft and it was the fastest growing crime in the United States in 2008.[8]

In response to the growing prevalence of identity theft, on May 10, 2006, President George W. Bush signed an executive order creating the

---

[5] The Identity Theft and Assumption Deterrence Act of 1998, Public Law 105-318 (October 30, 1998), amended 18 U.S.C. § 1028 to include sub-section (a)(7), which defined the crime of identity theft as "knowingly transfer[ring], possess[ing], or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law[.]" In 2004, Congress enacted the aggravated identity theft statute, codified in 18 U.S.C. § 1028A (2004), which enhanced the penalty for using the identification of another in connection with the commission of enumerated felony offenses.

[6] The FTC takes complaints from identity theft victims and shares these complaints with federal, state, or local law enforcement authorities.

[7] Federal Trade Commission, *2006 Identity Theft Survey Report* (November 2007).

[8] Jason M. Weinstein, Deputy Assistant Attorney General, Criminal Division, testified before the United States House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Policy, Census, and National Archives, concerning "Identity Theft: A Victims Bill of Rights" (June 17, 2009).

President's Identity Theft Task Force (President's Task Force).[9] The President's Task Force was chaired by the Attorney General, with the Chairman of the FTC serving as Co-Chair. The stated purpose of the Task Force was to "use federal resources effectively to deter, prevent, detect, investigate, proceed against, and prosecute unlawful use by persons of the identifying information of other persons."[10] Members of the President's Task Force included, among others, the Secretary of Homeland Security, the Postmaster General, and the Commissioner of the Social Security Administration.[11] The Task Force was made up of four subgroups: (1) Subgroup on Criminal Law Enforcement, (2) Subgroup on Education and Outreach, (3) Subgroup on Data Security, and (4) Subgroup on Legislative and Administrative Action.

Less than 1 year after its formation, the President's Task Force issued a strategic plan that made recommendations on combating identity theft to various federal departments and agencies, including DOJ and some of its components.[12] In September 2008, the Task Force issued a follow-up report detailing its efforts to ensure that its recommendations were implemented.[13] According to this report, much of the work recommended by the Task Force was completed but some efforts were still ongoing. The Associate Deputy Attorney General who served as the Office of the Deputy Attorney General's point of contact to the Task Force told the OIG in September 2009 that there were no plans for the President's Task Force to reconvene in the future.

OIG Audit Approach

The objective for this audit was to evaluate how DOJ has communicated and implemented its strategy to combat identity theft. To

[9] Executive Order 13402, *Strengthening Federal Efforts to Protect Against Identity Theft* (E.O. 13402).

[10] Alberto Gonzalez, Attorney General, memorandum for all Identity Theft Task Force members, Implementation of Identity Theft Task Force, May 22, 2006.

[11] The Secretaries of the Departments of Treasury, Commerce, Health and Human Services, Veterans Affairs, and the heads of the Office of Management and Budget, Federal Reserve System, Office of Personnel Management, Federal Deposit Insurance Corporation, Securities and Exchange Commission, National Credit Union Administration, Office of the Comptroller of the Currency, and the Office of Thrift Supervision also served as members of the President's Task Force.

[12] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (April 2007).

[13] The President's Identity Theft Task Force, *Task Force Report* (September 2008).

accomplish our objective we interviewed representatives from several DOJ components responsible for combating identity theft, including the Office of the Deputy Attorney General (ODAG), Criminal Division, Executive Office for United States Attorneys (EOUSA), two United States Attorneys' Offices (USAO), the Federal Bureau of Investigation (FBI), the Office of Community Oriented Policing Services (COPS), and several offices and bureaus within the Office of Justice Programs (OJP).[14] To gain a broader perspective on identity theft issues and DOJ's efforts in combating it, we also interviewed representatives from non-DOJ agencies with responsibilities for combating identity theft, including officials from the FTC, U.S. Secret Service, U.S. Postal Inspection Service, Social Security Administration, and the not-for-profit National Center for Victims of Crime.[15] In addition, we reviewed DOJ, EOUSA, Criminal Division, FBI, and OJP policies related to identity theft. We also reviewed statistics provided by EOUSA and the FBI related to identity theft investigations and prosecutions, personnel resources dedicated to identity theft, and identity theft victims.

In addressing our audit objective, this report first provides an overview of DOJ's overall approach to identity theft and recommendations for improving the overall coordination of the DOJ's efforts to combat this pervasive crime. Following that, we provide analyses of the individual activities of the various DOJ components involved in combating identity theft and make recommendations for those components to strengthen their efforts.

DOJ Leadership

According to the Associate Deputy Attorney General who served as the ODAG's point of contact for the President's Identity Theft Task Force, DOJ has not developed its own internal identity theft strategy, separate from the President's Task Force's strategic plan. The Associate Deputy Attorney General stated that DOJ considers the Task Force's plan to be valid and applicable to DOJ and its components.

However, the Associate Deputy Attorney General also noted that there is no person or entity within DOJ designated with the responsibility for

[14] In addition to meeting with officials from EOUSA, we also met with representatives from the United States Attorneys' Offices for the Northern District of Illinois and the Eastern District of Pennsylvania.

[15] According to its website, the mission of the National Center for Victims of Crime is to forge a national commitment to help victims of crime rebuild their lives. It is a 501(c)(3) not-for-profit organization supported by members, individual donors, corporations, foundations, and government grants.

coordinating DOJ's identity theft efforts, including ensuring that the recommendations of the President's Task Force are considered and implemented. Instead, each DOJ component is expected to consider and implement the recommendations of the President's Task Force as it deems appropriate.

We believe that additional DOJ leadership is needed to ensure that DOJ's overall efforts to combat identity theft are coordinated and prioritized. During our review, representatives from every DOJ component we contacted told us they have not received direction from DOJ to guide their efforts to combat identity theft. Further, while some components have taken steps to implement some of the recommendations of the President's Task Force on their own, not all relevant components were even aware that DOJ considers the President's Task Force strategic plan and recommendations to be its plan to combat identity theft. For example, as discussed in more detail in this report, many USAOs did not reevaluate the monetary thresholds applied in identity theft cases, the FBI is not collecting identity theft-related case statistics, and BJS did not work proactively to expand its data collection on identity theft to individual victims.

Therefore, the DOJ's approach to addressing identity theft has not been coordinated, resulting in identity theft not being treated as a DOJ priority. We believe that each DOJ component should designate an official or office responsible for monitoring their agency's identity theft efforts. Once these officials or offices are designated, DOJ should ensure that all component designees meet periodically with the DOJ designee to assess identity theft trends and make necessary adjustments to DOJ's approach to combating identity theft.

We recommend that the Department of Justice:

1. Coordinate its identity theft efforts based on a review of the President's Task Force's strategic plan and consultation with the relevant components involved in identity theft issues. DOJ should also monitor compliance with the President's Task Force recommendations and ensure further implementation where appropriate.

2. Designate a DOJ official or office as the individual or entity responsible for coordinating DOJ's identity theft efforts. DOJ should also direct each relevant component to designate an individual or office responsible for monitoring their agency's efforts and communicating their efforts to DOJ as requested.

3. Conduct periodic meetings with the components' newly designated identity theft coordinators to ensure that the DOJ's approach to identity theft remains viable and that adjustments are made to DOJ's approach when necessary.

Criminal Division

The Criminal Division is one of the DOJ components responsible for investigating and prosecuting federal criminal offenses, including identity theft.

Identity Theft Enforcement Interagency Working Group

Shortly after identity theft became a federal crime in 1998, the Attorney General's Council on White Collar Crime established an Identity Theft Subcommittee. According to Criminal Division officials, this subcommittee was led by the Fraud Section of the Criminal Division and met regularly until the creation of the President's Task Force in 2006. At that time, the Identity Theft Subcommittee was transformed into the Subgroup on Criminal Law Enforcement of the President's Task Force, chaired by an official from the Criminal Division. After the President's Task Force's September 2008 report, the Criminal Law Enforcement Subgroup was transformed once again at the request of the Attorney General into the Identity Theft Enforcement Interagency Working Group (Identity Theft Working Group).

Currently, the Identity Theft Working Group is chaired by the Deputy Chief of the Criminal Division's Fraud Section and meets once per month. According to the Chair, the Identity Theft Working Group is designed to be a forum for agencies to discuss identity theft enforcement issues, such as notable identity theft prosecutions, or trends that may be developing in the commission of identity theft crimes. The Working Group meetings are regularly attended by representatives from several DOJ components, including EOUSA, multiple USAOs, the FBI, and OJP's Office for Victims of Crime (OVC). ODAG officials have been invited to participate on the Working Group, but have not yet done so. Representatives from the other federal agencies also regularly attend meetings, including: the FTC, the U.S. Secret Service, the U.S. Postal Inspection Service, the Social Security Administration, and the Internal Revenue Service.[16]

[16] During this audit, we attended two meetings of the Identity Theft Working Group. Appendix II contains a list of the working group's regular participants.

DOJ and non-DOJ participants told us that they consider the Identity Theft Working Group a worthwhile initiative. Each of the participants we spoke with said the group's current Chair deserves credit for organizing the Identity Theft Working Group and for his efforts in trying to keep the issue of identity theft relevant to law enforcement efforts throughout the federal government.

However, even though the Working Group has covered non-enforcement issues during some of its monthly meetings, personnel from DOJ components involved in victim issues told us that they believed that the focus of the Identity Theft Working Group is too narrow. These individuals believed that they could be more helpful in regularly bringing identity theft victim issues to the attention of participating investigators and prosecutors. A staff member from the FBI's Office for Victim Assistance said that this office had not been asked to participate on the Identity Theft Working Group. Representatives from COPS stated that they no longer participated in the Identity Theft Working Group because it primarily focuses on identity theft prosecutions, which they said was not relevant to the mission of COPS.

The Identity Theft Working Group has helped promote identity theft enforcement as a priority for investigators and prosecutors, especially since the President's Task Force concluded its work in September 2008. However, we believe that important identity theft issues highlighted by the President's Task Force may not be receiving adequate attention. While we recognize that the Subgroup on Criminal Law Enforcement of the President's Task Force, the Identity Theft Working Group's predecessor, was purposely designed to focus on enforcement issues, we believe that the Identity Theft Working Group should seek to more frequently address identity theft topics beyond its primary focus on investigation and prosecution issues. As an established entity recognized among numerous federal agencies, the Working Group provides an established forum to regularly address broader identity theft issues related to enforcement, such as education and outreach, data protection, and victim issues. No other forum for some of these issues has existed since the subgroups of the President's Task Force concluded their work.

Training and Outreach Efforts

One of the recommendations made by the President's Task Force was for the federal government to provide specialized training "to first responders and others providing direct assistance to identity theft victims." According to the Chair of the Identity Theft Working Group, the working group does not directly sponsor identity theft training of state and local law enforcement. However, prior to the establishment of the Identity Theft

Working Group, several participants had already formed an informal training group. According to the Chair of the Identity Theft Working Group, he is the informal leader of this group, which consists of instructors from the Criminal Division, FBI, FTC, U.S. Postal Inspection Service, and U.S. Secret Service.

Since its inception in 2002, this training group has provided 1-day identity crime seminars, which include victim assistance topics, to state and local law enforcement officers. Currently, the group attempts to provide the training an average of three to four times per year at locations around the country. However, according to the Working Group's Chair, the seminars are difficult to coordinate because each of the member agencies has to pay its own costs related to the training. In addition, all of the instructors are based in the Washington, D.C., area, requiring them to travel for almost all seminars.

In its final report, the President's Task Force recognized the success and value of the informal training group and recommended that the group's efforts be increased. Members of the training group also told us that they believed their efforts were valuable, and they generally credited the Chair of the Identity Theft Working Group for the success of these efforts. However, one member noted that some agencies have recently assumed a disproportionate percentage of the cost for the training. According to this member, he was concerned that such a trend could become unsustainable and the group's future efforts may be put at risk.

Moreover, we are concerned about the informal structure of the group. Although the group has been successful in continuing its efforts over the last several years as an informal entity, we believe a more formalized structure and DOJ leadership attention could result in more training seminars for state and local officials and greater participation by other federal agencies.

As noted by the Chair of the Identity Theft Working Group, there are thousands of state, local, and tribal law enforcement agencies throughout the United States and many have little or no training budget. As the President's Task Force found, many identity theft victims' first step is to contact local law enforcement. Therefore, it is essential that state, local, and tribal law enforcement agencies are appropriately trained in dealing with identity theft crimes.

We believe that formalizing the training group will elevate its status and encourage greater participation among DOJ and non-DOJ agencies. Increased participation should also lead to additional opportunities to expand the reach of the training to state, local, and tribal law enforcement.

In addition to the efforts of the training group to train U.S. law enforcement officials, the Criminal Division has been involved in other training and outreach efforts for the international law enforcement community to address U.S. identity theft crimes originating overseas. For example, in 2005 the United Nations created an intergovernmental fraud and identity theft working group. The Criminal Division's Fraud Section led the U.S. delegation to that working group. In addition, the Fraud Section participated in a G8-led law enforcement subgroup on identity theft that encouraged member nations to focus more on identity theft crimes.[17] The Deputy Chief of the Fraud Section also advised the United Nations Office on Drugs and Crime regarding identity theft-related issues. The Computer Crime and Intellectual Property Section of the Criminal Division reported that during fiscal years 2008 and 2009 it participated in 12 international cybercrime training events at which it discussed the issue of identity theft.

Recommendations

The Criminal Division has assumed responsibility for examining many of the identity theft enforcement issues that were previously handled by the President's Task Force. However, the Criminal Division can only encourage other agencies to participate in its efforts to combat identity theft. We recommend that the DOJ broaden the focus of the Identity Theft Working Group so that it can address topics previously covered by subgroups of President's Task Force. In addition, a more formalized training group focused on educating state, local, and tribal law enforcement, the likely first responders in many identity theft cases, could help to ensure that many more state and local law enforcement officers and victim specialists receive training on investigating identity theft and assisting its victims. The efforts of the current training group, while successful, have limited reach.

We recommend that the Department of Justice and Criminal Division:

4. Expand the scope of the Identity Theft Enforcement Interagency Working Group to more regularly include identity theft-related topics previously covered by the other subgroups of the President's Identity Theft Task Force, such as education and outreach, data protection, and identity theft victims' issues.

[17] The G-8 is a multilateral group consisting of the world's major industrial democracies. The G-8 addresses a wide range of international economic, political, and security issues.

5. Formalize the identity theft training group currently being led by the Criminal Division and consider ways to expand its reach to state, local, and tribal law enforcement agencies.

Executive Office for United States Attorneys and United States Attorneys' Offices

The 94 United States Attorneys' Offices serve as the nation's principal litigators with responsibility for the prosecution of federal criminal cases. The primary function of EOUSA is to provide general executive assistance to and oversight of the 94 USAOs.

Identity Theft Data Collection

According to the President's Task Force, one of the shortcomings in the federal government's ability to understand and respond effectively to identity theft has been the lack of comprehensive statistical data about law enforcement efforts to combat it. One of the Task Force's recommendations was that federal agencies enhance their gathering of statistical data measuring the criminal justice system's response to identity theft. As part of this review, we asked EOUSA to provide us with the number of defendants charged under the federal identity theft statutes and the number of identity theft convictions obtained pursuant to these statutes during FYs 2007 through 2009.

EOUSA officials told the OIG that its data could not be considered complete or a reliable indicator of its identity theft efforts and that the statistics should be viewed as representing the lowest possible numbers of identity theft cases. EOUSA officials also told us that until December 2006, federal prosecutors tracked cases involving 18 U.S.C. § 1028, without breaking down the number of cases involving the subsection of that statute that dealt with identity theft (18 U.S.C. § 1028(a)(7)). Beginning in December 2006, changes were made to the EOUSA case management system that allowed federal prosecutors to track the specific subsection containing the crime of identity theft. In April 2007, the Acting Director of EOUSA sent a memorandum to all USAOs reminding them that they should take special care to ensure that cases charging identity theft offenses were entered and reported specifically as identity theft matters in the case management system. However, EOUSA officials stated that many USAOs were slow to adapt to this change and that, as a result, the more specific reporting category for identity theft likely understates the number of identity theft cases for FYs 2007 to 2009 because some such cases were likely reported under the broader offense code. One EOUSA official told us that

the failure of some USAOs to adapt to the new collection requirements may be a result of technical difficulties with the information technology systems currently in use.[18]

The following table contains the data provided by EOUSA.

Number of Defendants Charged and Convicted Pursuant to the Federal Identity Theft and Aggravated Identity Theft Statutes Fiscal Years 2007 through 2009[19]

	Identity Theft		Aggravated Identity Theft		Totals[20]	
FY	Defendants Charged	Convictions Obtained	Defendants Charged	Convictions Obtained	Defendants Charged	Convictions Obtained
2007	269	103	532	272	744	365
2008	296	144	620	338	882	467
2009	239	138	578	296	769	432

Source: EOUSA

We obtained from EOUSA data regarding the time spent by prosecutors handling identity theft cases, which is displayed in the following table. However, EOUSA officials cautioned the OIG about the accuracy of these figures because, like the case data presented above, EOUSA officials did not believe that every USAO was properly attributing attorney time spent working on identity theft prosecutions.

[18] EOUSA stated that officials were confident that the number of defendants charged and convictions obtained pursuant to the aggravated identity theft statute were adequately captured because that statute only covers one specific crime.

[19] The number of convictions obtained is not a subset of the number of defendants charged during the particular fiscal year because cases charged in one year may be resolved with a conviction in a subsequent fiscal year. Further, convictions obtained are for identity theft and aggravated identity theft only. Instances where a defendant was charged with identity theft or aggravated identity theft and convicted of other charges are not reflected in the conviction totals.

[20] The totals reflected in this table eliminate double counting of defendants who were charged with or convicted of both identity theft and aggravated identity theft.

Attorney Work Years Charged to Federal Identity Theft and Aggravated Identity Theft Prosecutions Fiscal Years 2007 through 2009[21]	
Fiscal Year	Totals
2007	25.68
2008	39.71
2009	45.62

Source: EOUSA

Because EOUSA officials still question whether USAO data for identity theft cases and activities are being completely captured, we believe that EOUSA should reemphasize to USAOs the importance of this data and the need to ensure full and accurate reporting of their cases and allocation of time among the categories of cases.

Efforts to Increase Identity Theft Prosecutions

One of the key recommendations of the President's Task Force was that the federal government increase identity theft prosecutions. In making this recommendation, the Task Force suggested that certain steps be taken by participating agencies. Four of these steps were directed specifically to the 94 USAOs: (1) designating an identity theft coordinator for each USAO, (2) increasing use by USAOs of interagency working groups and task forces devoted to identity theft, (3) reevaluating monetary thresholds applied to identity theft prosecutions, and (4) encouraging state prosecution of identity theft. In his April 2007 memorandum to all USAOs, the Acting Director of EOUSA asked all USAOs to consider these specific steps and to be prepared to report to EOUSA upon completion of the steps.

According to EOUSA, by July 2006, which was prior to the issuance of the President's Task Force strategic plan, every USAO already had established an identity theft point of contact. In addition, EOUSA reported to us that as of November 2009: (1) 36 of 94 USAOs managed or co-managed an identity theft task force or working group, (2) 5 USAOs were in the process of forming an identity theft working group or task force, and (3) 18 USAOs participated in task forces or working groups focused on identity theft or related crimes that are led by other agencies. Of the remaining 35 USAOs, 28 reported that they do not lead or do not participate

[21] According to EOUSA, the term "work year" is used when defining the productive efforts of one individual for one year. One work year for a federal employee is typically equal to 2080 hours.

in an identity theft task force or working group, and 7 USAOs did not report to EOUSA whether they participated.

With respect to the third and fourth recommendations of the President's Task Force, EOUSA provided documentation to us in October 2009 showing that only 41 of the 94 USAOs reported that they had reevaluated their monetary thresholds for identity theft prosecutions. The same offices informed EOUSA that they had, at a minimum, considered the recommendation to encourage state prosecution of identity theft. The remaining 53 USAOs did not report to EOUSA on their progress on these recommendations.

USAO Site Visits

To better determine how USAOs were responding to the President's Task Force recommendation to increase identity theft prosecutions, we met with the identity theft points of contact in two USAOs located in major metropolitan areas – Chicago and Philadelphia. We found that these districts took very different approaches toward identity theft crimes and the President's Task Force's recommendations.

USAO for the Northern District of Illinois

According to the Criminal Chief of the USAO for the Northern District of Illinois, the district prosecutes very few cases purely pertaining to identity theft. Instead, identity theft crimes in the district are generally connected to financial fraud cases, for which the office has an established monetary threshold for prosecution. The Criminal Chief believed that the district's threshold was appropriate based upon available resources and district priorities.

The identity theft point of contact for the USAO for the Northern District of Illinois, who also serves as the Associate Criminal Chief, told us that serving as the identity theft point of contact for this USAO is generally considered an administrative task. The Associate Criminal Chief was selected as the identity theft point of contact because she was already handling much of the criminal case intake, not because of any particular expertise in identity theft matters.

Additionally, this USAO was 1 of the 28 districts noted above that does not lead or participate in any identity theft task forces or working groups. Both the Criminal Chief and the identity theft point of contact stated that task forces or working groups were beneficial in districts in which law enforcement agencies do not work well together or generally lack

communication channels. These officials said that an identity theft task force or working group was unnecessary in their district because federal and local law enforcement agencies have historically worked very well together.

USAO for the Eastern District of Pennsylvania

The identity theft point of contact for the Eastern District of Pennsylvania was this USAO's Chief of the Financial Institution Fraud and Identity Theft Section. This point of contact told us that the office had eliminated the monetary threshold the USAO previously applied for identity theft prosecutions. In his opinion, the elimination of the monetary threshold has led to several identity theft prosecutions. For example, the district reported prosecuting cases where stolen identities were used to create fraudulent passports. Because such cases typically do not involve significant monetary losses, they often would not be prosecuted when strict monetary thresholds are applied.

In addition to eliminating monetary thresholds, the point of contact for the Eastern District of Pennsylvania said the office had established an identity theft working group that recently transitioned into a task force. According to the point of contact, the task force meets at least once a month and actively trains local law enforcement on identity theft issues. Participants on the task force include personnel from the FBI, U.S. Secret Service, U.S. Postal Inspection Service, Social Security Administration, Department of State, Defense Criminal Investigative Service, Federal Protective Services, Amtrak Police, and multiple state and local law enforcement agencies. According to the point of contact, task force participants have sent many identity theft case referrals to his office.

As the following table illustrates, between FYs 2007 and 2009, the Eastern District of Pennsylvania charged many more defendants with identity theft crimes and obtained more than 20 times the number of convictions as the Northern District of Illinois.

Number of Defendants Charged and Convicted Pursuant to Federal Identity Theft and Aggravated Identity Theft Statutes by the Northern District of Illinois and the Eastern District of Pennsylvania Fiscal Years 2007 through 2009[22]

Fiscal Year	Northern District of Illinois		Eastern District of Pennsylvania	
	Charged	Convicted	Charged	Convicted
2007 10		1	34	19
	13	0	15	40
2009 23		3	33	27

Source: EOUSA

We believe this data reflects the different approaches and priorities of these two districts in addressing identity theft. The elimination of monetary thresholds by the Eastern District of Pennsylvania, coupled with the multiple referrals from participating agencies on its identity theft task force, likely explain the higher number of defendants charged and convictions obtained in that district. Conversely, the lower number of defendants charged and convictions obtained by the Northern District of Illinois may correlate with the application of monetary thresholds and its lack of participation on identity theft task forces or working groups.

Finally, a significant achievement of the USAO for the Eastern District of Pennsylvania's identity theft task force was the development of the National Identity Crime Law Enforcement network (NICLE), which is funded primarily by the U.S. Postal Inspection Service.[23] NICLE allows for real-time connection of investigators and is principally used to help coordinate identity theft investigations. As of August 2009, NICLE contained 6.5 million records and was used by approximately 190 police departments, 26 state agencies in 5 states, and 12 federal agencies. Therefore, participation in NICLE is limited.

[22] The number of convictions obtained is not a subset of the number of defendants charged during the particular fiscal year because cases charged in one year may be resolved with a conviction in a subsequent fiscal year. Further, convictions obtained are for identity theft and aggravated identity theft only. Instances where a defendant was charged with identity theft or aggravated identity theft and convicted of other charges are not reflected in the conviction totals.

[23] NICLE grants participating agencies access to U.S. Postal Inspection Service identity theft case data, victim reports, and investigative data from various law enforcement agencies. The database is currently housed on the Regional Information Sharing Systems Network (RISSNET), and can only be accessed through the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN).

We discussed NICLE with the DOJ official who served as the ODAG's point of contact to the President's Task Force. He stated to us that DOJ is assessing NICLE as an option to address the Task Force's recommendation that law enforcement agencies consider establishing a National Identity Theft Law Enforcement Center. The official expressed some reservations about whether DOJ was the appropriate location for NICLE to be housed. We recommend that DOJ, with the assistance of EOUSA, assess NICLE and its capabilities as part of DOJ's approach to combating identity theft.

Identity Theft Training for Federal Prosecutors

One of the specific recommendations made to DOJ by the President's Task Force was to establish a standard training course focused on identity theft. According to EOUSA, an identity theft seminar had already been established at DOJ's training center for prosecutors and was first offered to Assistant U.S. Attorneys in October 2005. EOUSA informed us that the course was offered once in 2007, twice in 2008, and is scheduled to be offered in August 2010.

Identity Theft Victim Assistance

Federal law requires that victims of federal crimes be afforded certain rights, and that DOJ officers and employees engaged in the detection, investigation, or prosecution of crime to make their best efforts to see that crime victims are notified of and accorded their rights under federal law.[24] The Attorney General Guidelines for Victim and Witness Assistance (Attorney General Guidelines) contain a specific section, Article X, devoted to assisting victims of identity theft.[25]

EOUSA's Victim Witness Staff is responsible for providing primary support to USAOs' victim and witness staff. As of FY 2008, EOUSA reported that there were 215 Victim Witness Coordinators (VWC) throughout the nation. These VWCs typically become responsible for working with crime victims after charges are filed in a criminal case. According to the Assistant Director for EOUSA's Victim Witness Staff, in typical identity theft cases, VWCs are responsible for notifying identified victims of their rights under federal law and referring them to identity theft-related resources.

[24] 18 U.S.C. § 3771(c)(1)(2009).

[25] Attorney General Guidelines for Victim and Witness Assistance, Article X.

VWCs are also responsible for entering victims of identity theft into the automated Victim Notification System (VNS) when required.[26] Article X of the Attorney General Guidelines, which specifically addresses identity theft victims, states that, "all individuals who have had financial or personal information compromised in an identity theft crime should be identified, and their names and contact information should be entered into VNS." However, according to the Assistant Director for EOUSA's Victim Witness Staff, VNS is not always used to notify identified victims of their rights, especially in cases where there are large numbers of identity theft victims, such as in large computer hacking or financial fraud cases. EOUSA's Assistant Director told us that under those circumstances, Article II of the Attorney General Guidelines allows for methods other than VNS to be used in criminal cases with large numbers of victims. The Assistant Director also noted that VNS simply cannot handle the large numbers of entries that Article X suggests could be required. For example, she said that in a large-scale computer intrusion case there can potentially be a million victims of identity theft. Neither EOUSA nor USAOs have the resources needed to make that many entries into VNS.

The following table shows the number of identity theft victims entered into VNS during FYs 2007 through 2009.

Identity Theft Victims Entered into VNS Fiscal Years 2007 through 2009[27]

Fiscal Year	Identity Theft Victims
2007	10,861
2008	13,523
2009	21,729

Source: EOUSA

EOUSA cautioned that these figures may not be accurate because the capability for USAOs to specifically track identity theft cases was not implemented until December 2006. In addition, these figures do not include cases in which identity theft was charged but the identity theft program code was not used. According to EOUSA officials, this may occur when identity theft is not the primary charge in a particular case.

[26] VNS, a cooperative effort among the FBI, U.S. Postal Inspection Service, USAOs, and the Federal Bureau of Prisons, is an automated system that is designed to generate notifications to victims after critical events in the investigation and prosecution of cases with which they are associated.

[27] According to EOUSA, FY 2007 data is only partial because the codes used by USAO to specifically track identity theft cases were not instituted until December 18, 2006.

Recommendations

Although EOUSA has made an effort to implement many of the recommendations of the President's Task Force, it appears that some USAOs have not fully embraced those efforts. We recognize that resources and priorities can vary widely among districts. Nonetheless, we believe that the differing priority given and approaches taken to identity theft by the USAOs in the Northern District of Illinois and the Eastern District of Pennsylvania illustrate that the implementation of the President's Task Force recommendations can have an effect on identity theft enforcement efforts. Furthermore, because DOJ considers the President's Task Force plan applicable to DOJ components, DOJ should ensure that all USAOs consider implementing the President's Task Force's recommendations and provide reports regarding their identity theft strategy and efforts.

We recommend the Department of Justice and EOUSA:

6. Transmit a memorandum to all USAOs requiring each office to report on its current identity theft efforts, including the status of its efforts related to the implementation of the President's Task Force recommendations. USAOs should also report on the steps taken by the district to ensure that its case management data and attorney time allocation data on identity theft is fully and accurately reported.

7. Perform a comprehensive assessment of NICLE to determine whether it should be housed in DOJ and expanded nationally.

Federal Bureau of Investigation

Many of the FBI personnel we interviewed consider identity theft to be an ancillary crime that typically occurs as part of larger crimes, including computer intrusions, mortgage fraud, health care fraud, and terrorism. Because identity theft can be an element of these different types of crimes, Special Agents investigating a variety of cases can encounter identity theft in their investigations.

Identity Theft Program Control

Historically, responsibility for the FBI's identity theft program resided in its Criminal Investigative Division (CID). However, in November 2007, program control of identity theft was transferred from the CID to the Cyber Division. According to the internal FBI communication that formally

transferred the identity theft program to the Cyber Division, this transfer of the program was intended to focus the FBI's resources on the highest priority identity theft related investigations. Since this transfer, two notable changes have occurred in the FBI's approach to identity theft. First, as discussed in greater detail below, the FBI no longer tracks data on the number of identity theft investigations opened or convictions obtained. In addition, as of 2007, the FBI stopped updating a comprehensive assessment of the identity theft threat. That assessment had been prepared at the request of the FBI Deputy Director and released by the CID, in conjunction with the Cyber Division, in FY 2005.

Two supervisory-level FBI employees with substantial knowledge about identity theft told us that they did not agree with the decision to transfer control of the FBI's identity theft program to the Cyber Division. These employees also did not agree with the FBI's decision to no longer conduct comprehensive assessments of the identity theft threat on a regular basis. When we raised these concerns with a senior FBI official, he stated that the FBI must prioritize the use of its resources and he believed that the FBI would have the greatest impact on identity theft by housing the program in the division that targeted criminal elements operating on the internet. Although the specific crime of identity theft is not an FBI priority, Cyber Division officials informed us that identity theft is routinely addressed in the FBI's criminal intrusion program, which is currently a top FBI priority. Cyber Division officials noted that identity theft is also addressed through its internet fraud program.

FBI officials told us that the FBI has intelligence collection requirements for identity theft. However, comprehensive assessments that reach across multiple program areas are not currently required. According to these FBI officials, the FBI's identity theft intelligence collection requirements have led to the publication of 21 intelligence assessments and bulletins, which resulted from 428 intelligence information reports. FBI officials acknowledged, however, that the FBI's current intelligence collection requirements for identity theft are out of date and should be updated.

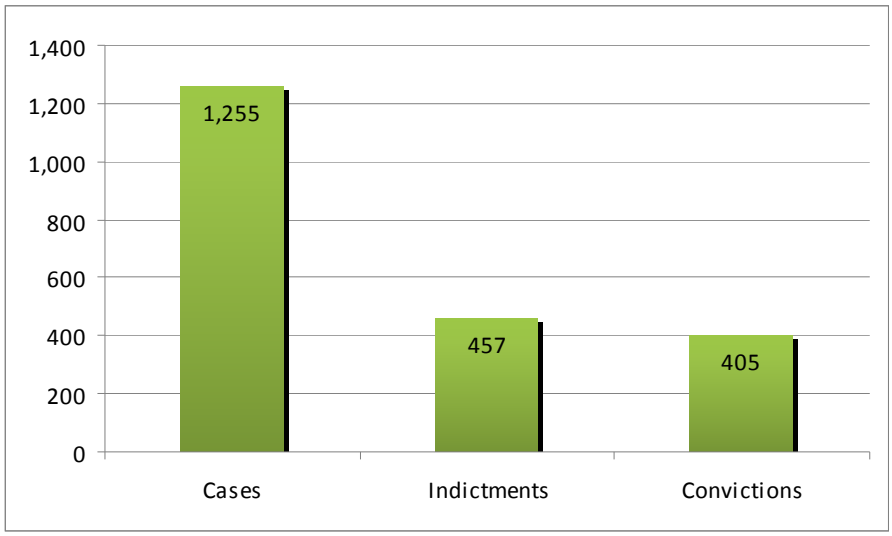
The internal FBI communication that formally requested the transfer of program control from CID to the Cyber Division stated that the identity theft crime problem, by its very nature, cuts broadly across all operational divisions and investigative programs of the FBI and requires a coordinated corporate approach in the FBI's response. In view of the recognition that identity theft cuts across FBI divisions and programs, we believe there is an increased need for periodic comprehensive identity theft assessments to be conducted and updated. Without such assessments, there is not an adequate mechanism for gathering and synthesizing the information about

identity theft from all the affected divisions and programs, and the FBI's ability to make informed decisions and assign the appropriate level of priority to identity theft matters is diminished. We recommend that the FBI conduct periodic comprehensive assessments on identity theft.

FBI Identity Theft Data

In FY 2006, the FBI reported identity theft investigation statistics in its *Financial Crimes Report to the Public*. The reported figures are displayed in the following exhibit.

FBI IDENTITY THEFT CASE DATA
FY 2006



Source: FBI 2006 *Financial Crimes Report to the Public*

When we requested similar data for FYs 2007 through 2009, the FBI informed us that it could not provide such data. Several of the FBI officials with whom we spoke, including the Assistant Directors for the FBI's Cyber Division and CID, were unaware that the FY 2006 statistics even existed. These officials said they did not believe that the FBI ever collected identity theft data.

We discussed this lack of identity theft data for FYs 2007 through 2009 with officials from CID and the Cyber Division. FBI officials stated that they would try to determine whether it was possible for CID to compile identity theft statistics for the investigations that were under CID control during the requested timeframe. CID later informed us that system limitations prevented it from compiling such data. The Unit Chiefs of CID's Health Care Fraud and Economic Crimes Units stated that they did not believe identity theft was common in their investigations. The Unit Chief for the National

Mortgage Fraud Unit, however, estimated that broader identity-related crimes were discovered in 80 percent of the investigations overseen by that unit. However, she was unsure how many of those crimes involved the more specific crime of identity theft.

At our request, the Cyber Division reviewed computer intrusion investigations to determine the percentage of such cases that involved identity theft. The Cyber Division reported to us that 62 percent of the pending 1,180 computer intrusion investigations during FYs 2007 through 2009 involved the crime of identity theft.

We are concerned about the FBI's inability to produce current and accurate data on identity theft crimes investigated by the FBI. The FBI's 2005 intelligence assessment concluded that, "identity theft has emerged as a dominant and pervasive financial crime that exposes individuals and businesses to significant losses and undermines the credibility and operation of the entire U.S. financial system." Yet, the lack of updated, reliable data on its identity theft investigations impairs the FBI's ability to quantify the prevalence and impact of the crime and to determine the appropriate investigative priority for identity theft. We recommend that the FBI resume collection and reporting of comprehensive data on its identity theft investigations, including data on cases for which identity theft elements are ancillary to the primary crime being investigated.

FBI Identity Theft Victim Assistance

Like the USAOs, the FBI must comply with federal laws and Attorney General Guidelines related to identity theft victim assistance. According to the Attorney General Guidelines, identification of victims is primarily the responsibility of the investigative agency. The Guidelines state that new technology and traditional law enforcement methods can be used to identify victims "regardless of whether the case involves large-scale mass violence crimes or large-scale economic crimes." Article X of the Attorney General Guidelines, which pertains to identity theft victims, states that individuals "do not have to know that their identity was misused in order to be victims, nor does the victim have to have incurred a financial loss to be considered a victim."

However, Cyber Division personnel told us that the Division generally considers the primary victim in large scale computer intrusion cases to be the institution whose system was breached. Individuals whose identities were stolen or compromised in connection with the intrusion are generally considered by the Cyber Division to be secondary or indirect victims. One supervisor stated that when they deal with large-scale computer intrusion

investigations they "do what they can" to assist individual identity theft victims. Another FBI official stated that the FBI cannot always focus on identifying the individual victims, especially in large-scale computer intrusion cases, because it does not have the resources to identify what can sometimes be over one million potential victims. For CID investigations, CID policy states that it is the responsibility of the compromised institution or business to identify and notify individual identity theft victims.

We discussed the FBI's approach to assisting identity theft victims with personnel from the FBI's Office for Victim Assistance, who noted that the FBI's current identity theft victim policies are inconsistent with the Attorney General Guidelines. They believed that the FBI's approach did not comply with Article X of the Attorney General Guidelines, which does not differentiate between direct and indirect victims in cases of identity theft. However, these Office for Victim Assistance personnel recognized that there are different definitions of "victims" under the primary federal statutes covering victim assistance and Article X of the Attorney General Guidelines.

Based on our discussions with FBI personnel, analysis of FBI policy and documentation, and review of the Attorney General Guidelines for Victim and Witness Assistance, we found confusion within the FBI about who qualifies as an identity theft "victim" for identification and notification purposes. This has led to an inconsistent approach to the FBI's efforts to identify victims of identity theft. In fact, we learned of recent instances where the FBI and USAOs have disagreed on identity theft victim identification and notification requirements. For example, in a recent identity theft case the FBI and local USAO disagreed on whether to notify an estimated 17,000 victims. According to the FBI, it believed that the victims should be notified, but the USAO believed notification was not required. The disagreement was later resolved by the Office of the Deputy Attorney General, which determined that the victim notification was not required.

We recommend that DOJ, EOUSA, the Criminal Division, and the FBI review relevant federal laws and the current Attorney General Guidelines for Victim and Witness Assistance and issue clear guidance to the affected components to ensure that DOJ and its components follow a uniform policy and take the legally required steps to identify and notify victims of identity theft.

NCIC Identity Theft File

In April 2005, the FBI added the Identity Theft File to the National Crime Information Center (NCIC).[28] The NCIC Identity Theft File allows law enforcement to flag stolen identities and identify imposters. An identity theft victim must consent to having their personal and biographic information entered into the Identity Theft File as a victim profile.[29] The victim profile is available to law enforcement officers through a routine NCIC query. A password created by the victim is included in the entry of the victim's information so that the victim can prove to law enforcement that the victim is the true owner of the identity. According to FBI officials, the law enforcement agency that enters the record should inform the victim that victim profiles are automatically purged 5 years after entry. However, victims may request that their profiles remain active as long as the criteria for entry remain satisfied.

The following table shows the number of active victim profiles in the NCIC Identity Theft File and the number of profiles purged since the creation of the file in April 2005, as reported by the FBI's Criminal Justice Information Services Division (CJIS).

NCIC Identity Theft File
Active and Purged Victim Profiles by Fiscal Year[30]

Fiscal Year	Active	Purged	Total
2005	302	20	322
2006	1,341	146	1487
2007	2,426	600	3026
2008	3,878	782	4660
2009	4,008	779	4787
TOTAL	**11,955**	**2,327**	**14,282**

Source: FBI Criminal Justice Information Services Division

[28] NCIC is a computerized database of criminal justice information that is available at all times to virtually every law enforcement agency nationwide.

[29] To qualify for entry into the NCIC Identity Theft File, the report taken by the law enforcement agency must meet the following three criteria: (1) someone is using a means of identification for the victim, (2) the identity of the victim is being used without the victim's permission, and (3) the victim's identity is being used or intended to be used to commit an unlawful activity.

[30] Data for FY 2005 includes victim profiles entered or purged from April 2005 through September 2005. Data for FY 2009 is current through September 1, 2009.

According to CJIS, which manages NCIC, only 13 of the 11,955 active victim profiles in NCIC were entered by federal law enforcement agencies, including the FBI. Additionally, only 13 of the 2,327 purged records were entered by federal law enforcement.

According to the FBI Program Director for the Office for Victim Assistance, the FBI assisted over 32,000 victims of identity theft between late 2003 and June 2009. The Program Director stated that all FBI Victim Specialists should provide identity theft victims with information about the NCIC Identity Theft File. However, when we asked other FBI personnel about the file, we found that an overwhelming number of these individuals had never heard of the file, including the Section Chiefs for the FBI's Cyber Criminal Section and Financial Crimes Section.

To better understand why so few of the FBI personnel with whom we spoke were aware of the NCIC Identity Theft file and why so few victim profiles were entered by the FBI, we discussed the training and outreach efforts about the file with CJIS staff. According to CJIS personnel, there is a training team that is responsible for training all federal, state, and local law enforcement agencies on the use of NCIC and the multiple files it contains. Generally, the NCIC training team provides requesting law enforcement agencies with training options for all NCIC files. The requesting agency then chooses the specific NCIC files it wants the training session to cover. According to one of the trainers, state and local law enforcement agencies choose to receive instruction on the NCIC Identity Theft File less than 50 percent of the time, and FBI field offices have never requested such training. This individual also noted that while new FBI agents receive training about NCIC at the FBI Academy, only a few minutes of that instruction is spent on the Identity Theft File.

We also asked representatives from other DOJ and non-DOJ federal agencies if they had ever heard of the NCIC Identity Theft File. As in the FBI, an overwhelming number of the individuals we interviewed had never heard of the file. The only exceptions were those who took part in the identity theft training group led by the Criminal Division. These individuals noted that the training they provide to state and local law enforcement personnel includes a segment on the NCIC file. When we explained the NCIC Identity Theft File to one high-ranking DOJ official familiar with victims' rights issues, the official stated that the FBI appears to have missed an opportunity to help victims by not adequately promoting the file.

The low number of victim profiles in the NCIC Identity Theft File suggests that the file is underutilized by federal, state, and local officials.

We believe this underutilization is primarily the result of a lack of training and outreach about the file.

We believe the FBI should conduct a full evaluation of the usefulness of the NCIC Identity Theft File to determine its continued viability. If the FBI determines that the Identity Theft File is a valuable part of its identity theft enforcement efforts, it should ensure that all FBI Special Agents and Victim Specialists receive training on the file and that the file is being populated. The FBI should also develop additional outreach plans to ensure that state and local law enforcement agencies are aware of the file's existence.

Other Identity Theft-Related Initiatives

Although the specific crime of identity theft is not among the FBI's top priorities, FBI officials told us it is often addressed in other broader-based FBI cyber crime initiatives, which the FBI considers to be priority activities.

Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3) is a partnership between the FBI and the National White Collar Crime Center.[31] IC3's mission is to serve as the central clearinghouse and repository for complaints from industry and private citizens regarding cyber crime. According to its 2008 Annual Report, 2.5 percent of the 275,284 online complaints received by IC3 in calendar year 2008 involved identity theft.[32] The FBI Acting Unit Chief for IC3 said these complaints are referred for investigation, when appropriate, to the FTC, FBI field offices, and other law enforcement agencies. IC3 also prepares cyber crime trend reports that it shares with the law enforcement community. IC3 regularly publishes online public service announcements aimed at educating the American public about identity theft risks and prevention.

InfraGard

According to its website, InfraGard is a partnership between the FBI and the private sector. It includes an association of businesses, academic

[31] According to its website, the National White Collar Crime Center is a non-profit membership organization dedicated to supporting law enforcement in the prevention, investigation, and prosecution of economic and high-tech crime.

[32] According to the Acting Unit Chief for IC3, these complaints were categorized as identity theft by the individual filing the complaint. If a subsequent investigation was opened by a law enforcement agency, such as the FBI, the investigation could have been categorized differently.

institutions, state and local law enforcement agencies, and other participants that share information and intelligence to prevent hostile acts against the United States. While InfraGard does not have a specific identity theft-related function, according to the FBI Unit Chief who oversees InfraGard, it provides a mechanism through which member institutions that are hacked or otherwise compromised can securely share information to help prevent similar events. Such information may be shared with the FBI, although there is no requirement that members do so.

Training and Outreach Efforts

The Cyber Division provides numerous training sessions in the United States and throughout the world. Although these training sessions typically cover the broader topic of cyber crime, many also cover the more specific crime of identity theft. According to the Assistant Director for the Cyber Division, the Cyber Division tries to focus its international training efforts in countries where the FBI believes cyber criminals pose the greatest risk.

Recommendations

We are concerned that the FBI's focus on the problem of identity theft has diminished since 2007. The FBI does not currently consider the specific crime of identity theft to be among its top priorities. However, identity theft is investigated in a significant number of its priority programs including computer intrusion and mortgage fraud investigations, in addition to other types of high priority investigations such as its national security investigations.

Because identity theft cuts across many different types of criminal activity and is reported to be one of the fastest growing crimes in the United States, we believe the FBI should refocus attention on this issue. Specifically, we recommend that the FBI generate periodic comprehensive assessments related to the identity theft threat. In addition, the FBI should maintain data regarding its identity theft investigations to help ensure that the FBI has information necessary to determine the appropriate priority to assign to its identity theft program.

In addition, we recommend that DOJ, EOUSA, the Criminal Division, and the FBI review relevant federal laws and the Attorney General Guidelines for Victim and Witness Assistance and issue clear guidance to ensure that the DOJ components take appropriate steps to identify and notify victims of identity theft. Finally, if the FBI determines that the NCIC Identity Theft File remains a valuable law enforcement and victims' assistance tool, the FBI should ensure that its FBI personnel receive more

information about this file so that identity theft victims are informed of the file and its purpose.

We recommend that the FBI:

8. Reassess its intelligence collection requirements for identity theft and conduct periodic comprehensive assessments on the identity theft threat.

9. Maintain statistics on identity theft investigations, including cases with ancillary identity theft elements.

10. Perform an evaluation of the NCIC Identity Theft File to determine its continued viability. If the FBI determines that the NCIC Identity Theft File is still viable, the FBI should ensure that appropriate FBI personnel are trained on its use.

We recommend that the Department of Justice, Criminal Division, EOUSA, and FBI:

11. Review relevant laws and Attorney General Guidelines for Victim and Witness Assistance and issue clear guidance to all DOJ components to ensure compliance with the law and Guidelines and that uniform steps are taken by DOJ personnel to identify and notify victims of identity theft.

Office of Justice Programs

The Office of Justice Programs (OJP) awards a broad range of grants relating to crime prevention and control, improving justice systems, increasing knowledge about crime, and assisting crime victims. Among the offices and bureaus within OJP are the Bureau of Justice Statistics (BJS), the Office for Victims of Crime (OVC), the Bureau of Justice Assistance (BJA), the National Institute of Justice (NIJ), the Office of Juvenile Justice and Delinquency Prevention (OJJDP), and the Community Capacity Development Office (CCDO). We interviewed personnel from each of these OJP offices to determine what efforts they have taken to address identity theft.

Identity Theft Statistics

The mission of BJS is to collect, analyze, publish, and disseminate information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government. As part of that effort, every

year BJS conducts the National Crime Victimization Survey (NCVS).[33] In July 2004 BJS added identity theft-related questions to the NCVS. The following chart shows the results of the most recent surveys and the number of months it took BJS to publish the results. Although BJS continues to include questions related to identity theft in the NCVS, we were informed that funding and resource limitations will delay the reporting of the 2006 identity theft results until the summer of 2010.

BUREAU OF JUSTICE STATISTICS
NATIONAL CRIME VICTIMIZATION SURVEYS
IDENTITY THEFT INFORMATION

Period Covered by Survey	Estimated Households Victimized by Identity Theft[34]	Publication Date	Time Elapsed between Survey and Publication
July 2004 through December 2004	3.6 million	April 2006	16 months
January 2005 through December 2005	6.4 million	November 2007	23 months
January 2006 through December 2006	Unknown	Projected mid-2010	42+ months

Source: OIG analysis of BJS information

Additionally, in 2006 BJS began planning for a more comprehensive one-time survey supplement specifically focused on identity theft. This supplement, developed in partnership with BJA, NIJ, FTC, and OVC, was conducted in 2008. The supplement collected information from individuals age 16 years and older from the same households that received the survey for the first 6 months of 2008. However, due to data processing problems the results of the identity theft supplement are not expected to be published by BJS until at least the fall of 2010. According to BJS, there are currently no plans to conduct future identity theft supplements to the survey. According to BJS officials, additional identity theft supplements would require new funding.

[33] According to BJS's website, the NCVS is the nation's primary source of information on criminal victimization. Each year data is obtained from a nationally representative sample of 76,000 households (comprising nearly 135,300 persons) on the frequency, characteristics, and consequences of criminal victimization in the United States.

[34] This statistic represents the estimated number of households that had at least one member victimized by identity theft during that period.

A specific recommendation of the President's Task Force was for BJS to expand the scope of the NCVS to collect information about the characteristics, consequences, and extent of identity theft for individuals ages 12 and older. The Task Force noted that the NCVS only collected data from the household respondent and did not capture data on multiple victims in the household or multiple episodes of identity theft. Such individualized identity theft data was collected in the one-time 2008 identity theft supplement and by the FTC in surveys conducted in 2003 and 2006. However, we were informed by FTC officials in September 2009 that the FTC is no longer conducting identity theft surveys. BJS told us that it would like to regularly capture data about individual victims, but it had no plans to expand the collection from the NCVS beyond household data. BJS cited resource limitations as the reason for its inability to expand its work.

OJP's Identity Theft Working Group

In 2004, OJP formed its own internal identity theft working group, which was primarily organized by a representative from the Office for Victims of Crime (OVC) and chaired by a Deputy Assistant Attorney General for OJP. The OJP working group addressed internal OJP matters, such as protection of OJP employee data, as well as external matters, such as the funding of identity theft programs and research. The working group also attempted to ensure that OJP bureaus and offices did not duplicate efforts on identity theft issues. Working group meetings were attended by representatives from OJP bureaus and offices, including BJS, NIJ, OJJDP, and CCDO. In addition, representatives from other DOJ offices, including COPS and the Office on Violence Against Women regularly attended.

The OJP working group meetings were held on a regular basis until late 2007, when the primary organizer from OVC was placed on a 1-year assignment outside of OVC. During the period that this individual was on assignment meetings were not organized and the working group's activities ceased. By the time the OVC representative completed her assignment, the then Deputy Assistant Attorney General was no longer taking a leadership role on the working group and no further meetings were scheduled.

However, the newly appointed Deputy Assistant Attorney General informed us that she is aware of the working group's prior efforts and supports resurrecting the working group. When we met with the Deputy Assistant Attorney General in August 2009, she said that a working group meeting was scheduled for September 2009. When we later inquired about that scheduled meeting, we were informed that the meeting took place in December 2009. We recommend that OJP ensure that its Identity Theft Working Group continues to meet regularly to make certain that each office

and bureau is appropriately considering future identity theft-related initiatives.

Identity Theft-Related Funding Efforts

In recent years, OJP has supported various identity theft initiatives. For example, in 2006 OVC disseminated the FTC's *Deter*, *Detect*, *Defend* consumer awareness kit to over 4,500 victim service providers nationwide, attended the National Association of Victim Assistance Administrators Conference to encourage program expansion to victims of identity theft, and supported the ID Theft Victim Verification Passport Program through the Ohio Attorney General's Office. In addition, NIJ funded a comprehensive identity theft research review, which was released in July 2007. BJA, in partnership with the National Crime Prevention Council, aired a televised public service campaign related to identity theft. OJJDP has provided funding for non-profit organizations that have developed internet-safety websites designed to protect children from internet crime, including identity theft. CCDO hosted law enforcement conferences in 2006 and 2007 that included sessions for vulnerable victim populations on identity theft.

We were informed of two upcoming OJP efforts specifically targeting identity theft: OVC's plan to provide funding in 2010 for a competitive grant program entitled "National Network to Support Identity Theft Victim Assistance", and a BJS-funded study that will examine identity fraud and charges brought under the Identity Theft Assumption and Deterrence Act.[35]

Several OJP officials told us that identity theft was a popular topic following the creation of the President's Task Force. However, they indicated that interest in identity theft initiatives faded within the law enforcement community after the work of the task force was completed.

Recommendations

BJS plays a key role, along with the FTC, in examining the impact of identity theft on U.S. citizens each year. We are concerned about the timeliness of the identity theft statistics reported by BJS. As noted earlier, BJS does not expect to report on the identity theft results from the FY 2006 survey and the 2008 identity theft supplemental survey until sometime in 2010. We believe there is a significant risk that these figures will be stale when they are published because they will not provide a reliable assessment of the current impact of identity theft on U.S. households. Furthermore, we

[35] Pub. L. No. 105-318 (1998).

were informed by FTC officials in September 2009 that they are no longer conducting the identity theft survey that was conducted in 2003 and 2006.

We believe the identity theft data collected by BJS is more important than ever. Therefore, we recommend that DOJ work with BJS to evaluate the timeliness of BJS's identity theft statistics. DOJ and BJS should also consider the President's Task Force recommendation to expand the scope of the NCVS to gather data about individual identity theft victims. Finally, we believe that OJP should ensure that its identity theft working group continues to meet regularly to assess whether future initiatives from BJA, NIJ, OJJDP, and CCDO should target identity theft specifically.

We recommend that the Department of Justice, OJP, and BJS:

12. Ensure that identity theft statistics gathered through the National Crime Victimization Survey are reported in a timely manner.

13. Evaluate the feasibility of regularly collecting identity theft data for individual victims instead of households.

We recommend that OJP:

14. Ensure that its Identity Theft Working Group continues to meet regularly to make certain that each office and bureau is appropriately considering future identity theft-related initiatives.

Community Oriented Policing Services

COPS is the DOJ component responsible for advancing the practice of community policing by the nation's state, local, and tribal law enforcement agencies. COPS awards grants to law enforcement agencies to hire and train community policing professionals, acquire and deploy crime-fighting technologies, and develop and test policing strategies.

According to COPS officials, they have had limited involvement in identity theft issues. These officials provided examples of two COPS identity theft initiatives. First, in June 2004, COPS published a guide book on identity theft that summarized how local police can reduce the harm caused by identity theft. Second, COPS sponsored an identity theft study titled, "*A National Strategy to Combat Identity Theft*." This study was conducted by Johns Hopkins University and publicly released in May 2006. According to COPS personnel, no other identity theft initiatives are planned for the immediate future.

Conclusion

We believe that DOJ's current approach to combating identity theft is not adequate based on the prevalence of the crime. Identity theft was recently reported to be fastest growing crime in 2008, affecting an estimated 10 million Americans annually. As the President's Task Force recognized, the harm caused to these millions of victims is not only financial in nature, but it can be emotionally traumatic because of the countless hours spent repairing damage to the victims' names and credit histories. As the Deputy Assistant Attorney General for DOJ's Criminal Division stated in 2009, identity theft is a problem "that continues to evolve as criminals develop more sophisticated and diverse methods to access and exploit the personal information of others."

For these reasons, we believe DOJ should take a more proactive approach to ensure that it is addressing this growing crime in a more coordinated, strategic, and effective manner. In this audit report, we therefore provide 14 recommendations to improve the Department's approach to combating identity theft.

OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Objectives

The objective of this audit was to evaluate how the Department of Justice has communicated and implemented its strategy to combat identity theft.

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our audit objective, we interviewed officials at the Office of the Deputy Attorney General, Criminal Division, EOUSA, two USAOs, FBI, OJP, and COPS. We also interviewed personnel from non-DOJ agencies including the U.S. Secret Service, Federal Trade Commission, Social Security Administration Office of the Inspector General, and the U.S. Postal Inspection Service. To further accomplish our objective we reviewed data obtained from EOUSA and FBI relating to identity theft investigations, prosecutions, and victims.

EOUSA Identity Theft Data

We requested that EOUSA provide us with data for FYs 2007 through 2009 regarding the number of: (1) identity theft cases prosecuted by USAOs, (2) identity theft convictions obtained by USAOs, (3) EOUSA/USAO personnel utilized to prosecute identity theft cases, and (4) identity theft victims entered into the Victim Notification System.

According to EOUSA officials, the data provided by EOUSA could only be considered baseline data as USAOs were not uniformly recording identity theft data during the requested time period. Accordingly, we did not test or verify the validity of the data provided by EOUSA and our report does not contain conclusions that are based on analyses of the data.

FBI Identity Theft Data

According to its *Fiscal Year 2006 Financial Crimes Report to the Public*, the FBI reported that 1,255 investigations resulted in 457 indictments and 405 convictions of identity theft criminals in FY 2006. When we requested similar data for FYs 2007 through 2009, we were informed by the FBI that it could not provide such data. According to FBI officials, the only identity theft data it could provide was an estimate of the percentage of computer intrusion cases that contained an identity theft element. Accordingly, we did not test or verify the validity of the data provided by the FBI and our report does not contain conclusions that are based on analyses of the data.

Internal Controls and Compliance with Laws and Regulations

Our audit objectives were informational in nature. Our assessment of internal controls was limited to our review of identity theft data provided by EOUSA and the FBI and to DOJ components' application of the Attorney General Guidelines for Victim and Witness Assistance. As noted in the body of this report, we identified our concerns with the accuracy of the data provided to us. However, we did not perform an independent, overall assessment of the reliability of the data in EOUSA's or the FBI's automated systems. Nonetheless, we believe that the overall results presented have utility for looking at the DOJ's overall efforts to combat identity theft. In addition, we identified our concerns with the apparent confusion that exists among DOJ personnel regarding the application of the Attorney General Guidelines in cases of identity theft. Further, we determined that examining compliance with laws and regulations was not significant to our objectives, and our audit did not reveal any instances of fraud or noncompliance.

IDENTITY THEFT ENFORCEMENT INTERAGENCY WORKING GROUP PARTICIPATING AGENCIES
AS OF JANUARY 2010

Department of Health and Human Services

- Office of Inspector General

Department of Homeland Security

- Immigration and Customs Enforcement
- Office of Policy
- U.S. Secret Service

Department of Justice

- Criminal Division
  - Computer Crime and Intellectual Property Section
  - Domestic Security Section
  - Fraud Section [Working Group Chair]
- Executive Office for U.S. Attorneys
- Federal Bureau of Investigation
  - Cyber Division
- Office of Justice Programs
  - Bureau of Justice Statistics
  - Office for Victims of Crime
- Office of Legal Policy
- U.S. Attorney's Offices (ca. 40)

Department of State

- Bureau of Consular Affairs
  - Office of Fraud Prevention Programs
  - Passport Services
    - Customer Service Division
    - Office of Passport Integrity and Internal Control
- Diplomatic Security Service
- Office of the Legal Adviser

Department of the Treasury

- Internal Revenue Service
  - Criminal Investigation
  - Online Fraud Detection and Prevention
  - Office of Privacy, Information Protection and Data Security
- Office of Critical Infrastructure Protection and Compliance Policy
- Office of Privacy and Civil Liberties
- Treasury Inspector General for Tax Administration

Department of Transportation

- Federal Motor Carrier Safety Administration
  - Commercial Driver's License Division

Federal Deposit Insurance Corporation

Federal Reserve Board

Federal Trade Commission

Bureau of Consumer Protection
Division of Privacy and Identity Protection

National District Attorneys Association

Securities and Exchange Commission

Division of Trading and Markets

Social Security Administration

Office of the Inspector General

U.S. Postal Inspection Service

DEPARTMENT OF JUSTICE AND COMPONENT RESPONSES

MEMORANDUM

TO: Raymond J. Beaudet
Assistant Inspector General for Audit
Office of Inspector General

FROM: Scott N. Schools
Associate Deputy Attorney General
Office of the Deputy Attorney General

SUBJECT: Department of Justice Responses to the OIG's Draft Report:
"The Department of Justice's Efforts to Combat Identity Theft"

The Office of the Deputy Attorney General (ODAG) very much appreciates the opportunity to review and respond to the Office of Inspector General (OIG) draft audit report entitled, "The Department of Justice's Efforts to Combat Identity Theft " (Report). In the transmittal memorandum that accompanied the draft report, OIG requested separate responses from the addressees. This memorandum transmits those separate responses and provides the substantive responses of ODAG to Recommendations 1-3 and a coordinated response to Recommendation 11, which was directed to the Department of Justice (Department or DOJ) generally as well as to the Criminal Division, the Executive Office for United States Attorneys (EOUSA), and the Federal Bureau of Investigation (FBI). Recommendations 12 and 13 were directed to the Department generally as well as to the Office of Justice Programs (OJP) and the Bureau of Justice Statistics. The Department's responses to those recommendations are reflected in OJP's submission. ODAG reviewed and concurred with the attached responses.

The Report evaluates the Department's prosecution efforts based in part on numbers of cases brought and defendants prosecuted. The Department's efforts to combat identity theft often are directed at large scale identify theft organizations and operations. Such prosecutions are resource intensive and can result in a reduction in the actual number of cases prosecuted even though a single prosecution of a large scale identity theft offender can have a much larger impact than multiple smaller prosecutions. For example, since the OIG initiated the audit in June 2009, (1) four defendants were charged in the Northern District of Georgia with identity theft and other crimes as a result of their alleged participation in an international hacking ring involving a $9 million fraud, (2) six defendants and alleged members of the Bonanno crime family pleaded guilty to racketeering activities including identity theft in the Southern District of Florida, (3) the FBI arrested 33 defendants in an international identity theft ring targeting online bank accounts, and (4) a computer hacker accused of masterminding one of the largest cases of identity theft in United States history pleaded guilty in the District of Massachusetts. These examples are illustrative of the quality of the cases behind the numbers referenced in the Report.

The Report notes that other federal, state and local law enforcement agencies also play a

vital role in combating identity theft. Although the OIG interviewed representatives from several non-DOJ agencies involved in addressing identity theft, the audit team advised that a full review of the efforts of non-DOJ agencies was not within the scope of the OIG's review. Although the Department generally agrees with the recommendations contained in the Report, we likewise want to be sure to emphasize that our law enforcement partners at the United States Secret Service, the United States Postal Inspection Service, and state and local law enforcement agencies play a critical role in the overall effort to combat identity theft. The Department relies on these efforts to support and supplement the Department's strategy.

These observations are included in this response merely to provide some additional context to the Report. The Department recognizes the importance of a well-coordinated approach to investigating and prosecuting identity theft and meeting the needs of victims. Such an approach was reflected in the President's Identity Theft Task Force Strategic Plan to Combat Identity Theft released in April 2007. The steps taken to implement that plan were described in the Task Force Report that was issued in September 2008. In particular, the Strategic Plan included a law enforcement strategy, much of which was implemented as reflected in the Task Force Report. Many of the law enforcement initiatives implemented subsequent to the issuance of the Strategic Plan remain in place. However, the Department agrees that greater coordination and oversight from the Department would enhance the Department's efforts to combat identity theft and agrees with the recommendations contained in the Report. The Department's specific responses to Recommendations 1-3 and 11 are set forth below.

Recommendation 1: That the Department of Justice coordinate its identity theft efforts based on a review of the President's Task Force's strategic plan and consultation with the relevant components involved in identity theft issues. DOJ should also monitor compliance with the President's Task Force recommendations and ensure further implementation where appropriate.

Response: The Department agrees with and will implement this recommendation. The Department considers this recommendation resolved.

Recommendation 2: That the Department of Justice designate a DOJ official or office as the individual or entity responsible for coordinating DOJ's identity theft efforts. DOJ should also direct each relevant component to designate an individual or office responsible for monitoring their agency's efforts and communicating their efforts to DOJ as requested.

Response: The Department previously identified an individual responsible for having oversight responsibilities for the Department's identity theft strategy; however, the Department will identify an individual to assume a more active role in coordinating the Department's identity theft efforts in a manner consistent with Recommendation 1. In addition, the Department agrees with and will direct the relevant components to designate an individual or office responsible for monitoring their agency's efforts and communicating their efforts to the Department as requested. T he Department considers this recommendation resolved.

Recommendation 3: That the Department of Justice conduct periodic meetings with the components' newly designated identity theft coordinators to ensure that the DOJ's approach to identity theft remains viable and that adjustments are made to DOJ's approach when necessary.

Response: The Department agrees with and will implement this recommendation. The Department considers this recommendation resolved.

Recommendation 11: That the Department of Justice, Criminal Division, EOUSA, and FBI review relevant laws and Attorney General Guidelines for Victim and Witness Assistance and issue clear guidance to all DOJ components to ensure compliance with the law and Guidelines and that uniform steps are taken by DOJ personnel to identify and notify victims of identity theft.

Response: The Department and the identified components agree that clear guidance should be issued consistent with applicable law and Department policy regarding identifying and providing services to victims of identity theft. This effort may include reviewing and revising as necessary the Attorney General Guidelines for Victim and Witness Assistance or issuing guidance that clarifies what is required under existing guidelines and applicable law. The Department will coordinate this effort with the Office for Victims of Crime and other relevant components. The Department considers this recommendation resolved.

In conclusion, the Department concurs with all of the recommendations in the Report. ODAG appreciated the professionalism exhibited by your staff in working jointly with our representatives to complete this audit. Please feel free to contact me should you have any questions.

Enclosures

U.S. Department of Justice

Criminal Division

Washington, D.C. 20530

March 18, 2010

MEMORANDUM

TO: Raymond J. Beaudet
Assistant Inspector General for Audit
Office of the Inspector General

FROM: Mythili Raman
Principal Deputy Assistant Attorney General and Chief of Staff

SUBJECT: Criminal Division Response to Draft Office of Inspector General Draft Audit Report the Department of Justice's Efforts to Combat Identity Theft

This memo sets forth the responses to the recommendations pertaining to the Criminal Division in the Office of the Inspector General (OIG) draft audit report entitled *The Department of Justice's Efforts to Combat Identity Theft*. We understand that certain recommendations that relate to multiple components of the Department will be addressed by other offices, such as the Office of the Deputy Attorney General.

1. *Recommendation 4*. Expand the scope of the Identity Theft Enforcement Interagency Working Group (ITEIWG) to more regularly include identity theft-related topics previously covered by the other subgroups of the President's Identity Theft Task Force, such as education and outreach, data protection, and identity theft victims, issues.

Criminal Division Response: The Criminal Division agrees to ensure that the ITEIWG will continue to address the full range of identity theft topics that are of concern to its members, including complaint reporting and analysis, investigation, prosecution, sentencing, prevention and education, data protection, and victim assistance. It should be noted that before the date of the exit conference, the Federal Bureau of Investigation (FBI) Office of Victim Assistance accepted an invitation to join the ITEIWG, and the Office of Community Oriented Policing Services agreed to be placed on the ITEIWG email list for notices of future meetings. The Criminal Division considers this recommendation resolved.

2. *Recommendation 5*. Formalize the identity theft training group currently being led by the Criminal Division and consider ways to expand its reach to state, local, and tribal law enforcement agencies.

Criminal Division Response: The Criminal Division agrees with this recommendation. The ITEIWG has already formally created a Training Subgroup to track and seek to develop additional training opportunities for federal, state, local, and tribal law enforcement agencies and has contacted Working Group members to solicit representatives for this subgroup. The Criminal Division considers this recommendation resolved.

If you have further questions concerning this response, please do not hesitate to contact this Office.

U.S. Department of Justice

Executive Office for United States Attorneys
Office of the Director

Main Justice Building, Room 2244A *(202) 514-2121*
950 Pennsylvania Avenue, N. W.
Washington, D.C. 20530

MEMORANDUM

DATE: March 19, 2010

TO: Raymond J. Beaudet
Assistant Inspector General for Audit

FROM: Norman Wong
Deputy Director / Counsel to the Director
Executive Office for United States Attorneys

SUBJECT: Response to OIG's Report Entitled:
"Department of Justice's Efforts to Combat Identity Theft"

This memorandum is submitted by the Executive Office for United States Attorneys (EOUSA) in response to the report by the Office of Inspector General (OIG) entitled "Department of Justice's Efforts to Combat Identity Theft." EOUSA appreciates OIG's efforts to promote integrity, efficiency, and effectiveness in the enforcement of federal criminal and civil laws. It is in this spirit that EOUSA accepts and will endeavor to carry out OIG's recommendations to the best of its ability.

Unlike most other DOJ components, EOUSA and the United States Attorneys' offices (USAOs) do not constitute a single hierarchical organization with a headquarters office directing policy decisions and resource management. Rather, each United States Attorney (USA) is the chief law enforcement officer in his or her district. Each USA, unless serving in an acting or interim capacity, is appointed by the President and confirmed by the Senate. As a holder of high office, the USA is afforded significant discretion to manage his or her office according to locally perceived priorities and needs, consistent with overarching Departmental priorities. The 94 USAOs vary in size from 20 employees to over 800 employees. Each office has a unique identity and local "office cultures" vary greatly.

It is in this context that EOUSA interacts with the USAOs to "[p]rovide general executive assistance and supervision to the offices of the U.S. Attorneys." 28 C.F.R. § 0.22. The LIONS case management system is maintained by EOUSA as a tool to assist the United States Attorneys in assessing staff caseloads and managing their offices. For this reason, the United States Attorneys maintain flexibility in the manner in which they may enter data about criminal cases being prosecuted in their districts. Because the LIONS system was not designed as a statistical system, it can be an imperfect tool for responding to specific, detailed inquiries seeking comprehensive, uniform nationwide data sought for purposes other than case management. We appreciate that OIG took this

into consideration in preparing this report.

Recommendations

EOUSA welcomes this review as an opportunity to make the recommended improvements in these areas. EOUSA will endeavor to implement both of the report's recommendations to the best of its ability.

6. *Transmit a memorandum to all USAOs requiring each office to report on its current identity theft efforts, including the status of its efforts related to the implementation of the President's Task Force recommendations. USAOs should also report on the steps taken by the district to ensure that its case management data and attorney time allocation data on identity theft is fully and accurately reported.*

EOUSA will prepare and disseminate such a memorandum within 90 days. To the extent that there is a technical change or an alteration in the policy and practice regarding the entry of case data in the LIONS system, EOUSA will communicate with your office regarding any additional time that may be required.

7. *Perform a comprehensive assessment of NICLE to determine whether it should be housed in DOJ and expanded nationally.*

EOUSA would be pleased to participate in a Departmental assessment of the NICLE system.

U.S. Department of Justice
Federal Bureau of Investigation
Washington, D. C. 20535-0001

March 22, 2010

Raymond J. Beaudet
Assistant Inspector General
for Audit
Office of the Inspector General
U.S Department of Justice
Suite 5000
1425 New York Avenue, N.W.
Washington, D.C. 20530

Dear Mr. Beaudet:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your draft audit report entitled, "The Department of Justice's Efforts to Combat Identity Theft" (hereinafter "Report").

We are pleased that the Report acknowledges the FBI=s decision to place its identity theft program within the Cyber Division in order to focus the FBI's resources on the highest priority identity theft investigations. In doing so, the FBI has focused its efforts on those identity theft cases which involve the most victims, the greatest financial loss, and the highest degree of organized criminal activity. We are also pleased that the Report recognizes how frequently identity theft issues are addressed through these high priority criminal intrusion cases. As the OIG notes, 62 percent of the 1,180 pending computer intrusion investigations during fiscal years 2007 to 2009 involved identity theft.

Additionally, the FBI is pleased that this Report reflects the FBI's other broad-based identity theft initiatives, including the Internet Crime Complaint Center (IC3), which regularly publishes online public service announcements aimed at educating the public about identity theft risks and prevention. The FBI is proud that it is successfully addressing identity theft on several different levels - from public service announcements to sophisticated computer intrusion investigations aimed at stealing identities.

In conclusion, based upon a review of the Report, the FBI concurs with the four recommendations directed to the FBI. The FBI appreciates the professionalism exhibited by your staff to complete this Report. Enclosed herein are the FBI's responses to the recommendations. Please feel free to contact me at 202-324-2901 should you have any questions or need further information.

Sincerely yours,

Amy Jo Lyons
Assistant Director
Inspection Division

OIG REVIEW of the DEPARTMENT of JUSTICE'S EFFORTS
to COMBAT IDENTITY THEFT
FBI RESPONSE TO
RECOMMENDATIONS CONTAINED in the FINAL DRAFT

Report Recommendation #8: "Reassess its intelligence collection requirements for identity theft and conduct periodic comprehensive intelligence assessments covering identity theft."

FBI Response to the Final Draft: Concur. The FBI will update its intelligence collection requirements for identity theft and conduct a threat assessment on "Identity Theft." The FBI considers this recommendation resolved.

Report Recommendation #9: "Maintain statistics on identity theft investigations, including cases with ancillary identity theft elements.

FBI Response to the Final Draft: Concur. The FBI will examine ways to use case management procedures to improve the tracking of identity theft cases so that statistics on identity theft investigations, including cases with ancillary identity theft elements, can be maintained. The FBI considers this recommendation resolved.

Report Recommendation #10: "Perform an evaluation of the NCIC Identity Theft File to determine its continued value. If the FBI determines that the NCIC Identity Theft File is still viable, the FBI should ensure that appropriate FBI personnel are trained on its use."

FBI Response to the Final Draft: Concur. The FBI will perform an evaluation of the NCIC Identity Theft File to determine its continued viability and take appropriate action. The FBI considers this recommendation resolved.

Report Recommendation #11: "Review relevant laws and Attorney General Guidelines for Victim and Witness Assistance and issue clear guidance to all DOJ components to ensure compliance with the law and Guidelines and that uniform steps are taken by DOJ personnel to identify and notify victims of identity theft." (*Recommendation Directed at DOJ, Criminal Division (DOJ), EOUSA, and the FBI*.)

FBI Response to the Final Draft: Please refer to ODAG submission for joint response.

MEMORANDUM TO: Raymond J. Beaudet
Assistant Inspector General for Audit
Office of the Inspector General
United States Department of Justice

FROM: Laurie O. Robinson
Assistant Attorney General

SUBJECT: Response to Office of the Inspector General's Draft Audit Report, *Audit of the Department of Justice's Efforts to Combat Identity Theft*

This memorandum provides a response to the recommendations directed to the Office of Justice Programs (OJP) included in the Office of the Inspector General's (OIG's) draft audit report entitled, *Audit of the Department of Justice's Efforts to Combat Identity Theft*. The draft audit report contains 14 recommendations, of which three recommendations pertain to the OJP.

The OJP's response to Recommendation Numbers 12, 13, and 14 are detailed below. For ease of review, the recommendations are restated in bold and are followed by our response.

12. Ensure that identity theft statistics gathered through the National Crime Victimization Survey are reported in a timely manner.

The OJP agrees with the recommendation and concurs that it is important to timely publicize identity theft statistics. While data releases from the National Crime Victimization Survey (NCVS) have not been timely, the Bureau of Justice Statistics (BJS) is working to improve this situation. BJS is committed to reducing the time required to initially release all data, including the identity theft estimates produced from the ongoing NCVS and the Identity Theft Supplement to the NCVS. Accordingly, BJS anticipates releasing the 2006 through 2008 identity theft statistics on its website by June 2010. The OJP considers this recommendation resolved and requests written acceptance of this action from your office.

13. Evaluate the feasibility of regularly collecting identity theft data for individual victims instead of households.

The OJP agrees with the recommendation. BJS is currently conducting an evaluation to determine the feasibility of collecting data on identity theft from individual victims. BJS will compare the identity theft data collection procedures for the individual and household approaches, and determine the best approach. Additionally, BJS will report their findings to the OIG as they become available. The OJP considers this recommendation resolved and requests written acceptance of this action from your office.

14. Ensure that its Identity Theft Working Group continues to meet regularly to make certain that each office and bureau is appropriately considering future identity theft-related initiatives.

The OJP agrees with the recommendation. OJP has planned regular bi-monthly meetings of its Identity Theft Working Group for the remainder of 2010 to discuss issues surrounding victimization, enforcement, training, funding, prevention, outreach, and research. Experts in these areas will attend these meetings to share their knowledge with the group. A meeting of the Identity Theft Working Group, which included representatives from U.S. Federal Trade Commission, was held on March 10, 2010, in coordination with Consumer Protection Week (see Attachment). The OJP considers this recommendation closed and requests written acceptance of this action from your office.

Thank you for your continued cooperation. If you have any questions regarding this response, please contact Maureen A. Henneberg, Director, Office of Audit, Assessment, and Management, on (202) 616-3282.

Attachment

cc: Beth McGarry
Deputy Assistant Attorney General
for Operations and Management

Marylou Leary
Principal Deputy Assistant Attorney General

Michael Sinclair
Acting Director
Bureau of Justice Statistics

Joye E. Frost
Acting Director
Office for Victims of Crime

Marcia K. Paull
Chief Financial Officer

Maureen A. Henneberg
Director
Office of Audit, Assessment, and Management

Jeffery A. Haley
Deputy Director, Audit and Review Division
Office of Audit, Assessment, and Management

Richard A. Theis
Assistant Director, Audit Liaison Group
Justice Management Division

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to the Office of the Deputy Attorney General (ODAG), the Criminal Division, the Executive Office for United States Attorneys (EOUSA), the Federal Bureau of Investigation (FBI), the Office of Justice Programs (OJP), and the Office of Community Oriented Policing Services (COPS). The responses we received from the ODAG, Criminal Division, EOUSA, FBI, and OJP are incorporated in Appendix III of this final report.[36] In these responses, the agencies concurred with our recommendations and discussed the actions they will implement in response to our findings. We will address later in this appendix the specific responses to each of our recommendations and the actions necessary to close the recommendations. First, however, we will respond to certain language in the ODAG's response that did not pertain to a specific recommendation.

Analysis of the ODAG Response

The ODAG stated in its response that the OIG evaluated DOJ's prosecution efforts based, in part, on numbers of cases brought and defendants prosecuted. For clarification, our report does not evaluate DOJ's prosecution efforts based on the numbers of identity theft cases brought or defendants prosecuted. We offer no opinion in our report as to whether the actual number or substance of DOJ's prosecutions is appropriate. Instead, EOUSA data on the number of cases brought and convictions obtained are provided to illustrate that EOUSA's data on federal identity theft prosecutions is incomplete and not a reliable indicator of DOJ's prosecution efforts. We believe that improved data collection for identity theft prosecutions will allow DOJ and EOUSA to better understand DOJ's overall identity theft efforts and assist DOJ in prioritizing future identity theft initiatives.

The specific data reported for the Northern District of Illinois and the Eastern District of Pennsylvania was likewise not offered as an indicator of whether the actual number of cases or substance of the prosecutions brought in these districts was appropriate. This specific data was offered for comparison purposes to illustrate that implementation of the President's Task Force recommendations, as in the Eastern District of Pennsylvania, may

[36] Our report did not include any recommendations addressed to COPS, and COPS did not formally respond to our report.

achieve the desired result of increased numbers of identity theft prosecutions and convictions.

Summary of Actions Necessary to Close Report

Recommendation Number:

1. **Resolved.** The ODAG concurred with our recommendation to coordinate its identity theft efforts based on a review of the President's Task Force strategic plan and consultation with the relevant components involved in identity theft issues. The ODAG also agreed to monitor compliance with the President's Task Force recommendations and ensure further implementation where appropriate.

   This recommendation can be closed when we receive evidence that the ODAG has taken steps to better coordinate DOJ's identity theft efforts. In addition, the ODAG must provide the OIG evidence demonstrating that DOJ is monitoring compliance with the President's Task Force recommendations. Further, in instances where DOJ and the relevant component have determined that implementation of a particular Task Force recommendation is impractical, the ODAG should provide a written explanation as to why the recommendation cannot or will not be implemented.

2. **Resolved.** The ODAG concurred with our recommendation and stated that it will identify an individual to assume a more active role in coordinating the DOJ's identity theft efforts in a manner consistent with Recommendation 1. The ODAG also stated that it will direct the relevant components to designate an individual or office responsible for monitoring their agency's efforts and communicating those efforts to DOJ when requested.

   This recommendation can be closed when we receive evidence that DOJ has: (1) assigned an individual responsible for assuming a more active role in coordinating its identity theft efforts, and (2) directed the relevant DOJ components to assign an individual or office responsible for monitoring their agency's identity theft efforts.

3. **Resolved.** The ODAG concurred with our recommendation to conduct periodic meetings with the components' newly designated identity theft coordinators to ensure that DOJ's approach to identity theft remains viable and that adjustments are made to DOJ's approach when necessary. This recommendation can be closed when we receive

evidence that meetings with the components' newly designated identity theft coordinators are conducted periodically.

4. **Resolved.** The Criminal Division concurred with our recommendation that DOJ and the Criminal Division expand the scope of the Identity Theft Enforcement Interagency Working Group (Identity Theft Working Group) to more regularly include identity theft-related topics previously covered by other subgroups of the President's Identity Theft Task Force, such as education and outreach, data protection, and identity theft victims' issues. The Criminal Division stated in its response that it will ensure that the Identity Theft Working Group continues to address the full range of identity theft topics that are of concern to its members, including complaint reporting and analysis, investigation, prosecution, sentencing, prevention and education, data protection, and victim assistance.

   This recommendation can be closed when we receive evidence that identity theft-related topics including prevention and education, data protection, and victim assistance are included in the Identity Theft Working Group monthly meetings regularly.

5. **Resolved.** The Criminal Division concurred with our recommendation that DOJ and the Criminal Division formalize the identity theft training group currently being led by the Criminal Division and consider ways to expand its reach to state, local, and tribal law enforcement agencies. According to the Criminal Division's response, the Identity Theft Working Group has already created a training subgroup to track and develop additional training opportunities for federal, state, local, and tribal law enforcement agencies.

   This recommendation can be closed when we receive evidence documenting the formal establishment of the training subgroup. The Criminal Division should also provide a list of the training subgroup member agencies as well as evidence of initial training activities led by this subgroup.

6. **Resolved.** EOUSA concurred with our recommendation that DOJ and EOUSA transmit a memorandum to all USAOs requiring each office to report on its current identity theft efforts, including the status of its efforts related to the implementation of the President's Task Force recommendations. EOUSA also agreed that DOJ and EOUSA should require all USAOs to report on the steps taken by their district to ensure that its case management data and attorney time allocation data on identity theft is fully and accurately reported. In its response

EOUSA stated that it will prepare and disseminate such a memorandum within 90 days. This recommendation can be closed when we are provided with a copy of the memorandum and each USAO's response to the memorandum.

7. **Resolved.** EOUSA concurred with our recommendation that DOJ and EOUSA perform a comprehensive assessment of NICLE to determine whether it should be housed in DOJ and expanded nationally. This recommendation can be closed when we receive the results of the assessment of the NICLE database and when we are provided DOJ's determination on expanding the database nationally.

8. **Resolved.** The FBI concurred with our recommendation that it reassess its intelligence collection requirements for identity theft and conduct periodic comprehensive assessments on the identity theft threat. In its response the FBI stated that it will update its intelligence collection requirements for identity theft and conduct a threat assessment on identity theft. This recommendation can be closed when we receive evidence that the FBI's identity theft intelligence collection documents have been updated and that a comprehensive identity theft threat assessment has been performed. The FBI should also document the frequency with which it intends to update its identity theft-specific threat assessment.

9. **Resolved.** The FBI concurred with our recommendation to maintain statistics on identity theft investigations, including cases with ancillary identity theft elements. The FBI stated in its response that it will examine ways to use case management procedures to improve the tracking of identity theft cases so that statistics on identity theft investigations, including cases with ancillary identity theft elements, can be maintained. This recommendation can be closed when we are provided evidence that the FBI has established a mechanism through which it captures data on its identity theft investigations, including investigations with ancillary identity theft elements.

10. **Resolved**. The FBI concurred with our recommendation and stated in its response that it will perform an evaluation of the NCIC Identity Theft File to determine its continued viability. The FBI also agreed that if it determines the file is still viable it will ensure that the appropriate personnel are trained on its use. This recommendation can be closed when we are provided the FBI's assessment of the NCIC Identity Theft File as well as its determination on the file's continued use.

11. **Resolved.** DOJ, the Criminal Division, EOUSA, and the FBI all concurred with our recommendation to review the relevant laws and Attorney General Guidelines for Victim and Witness Assistance, issue to all DOJ components clear guidance for complying with the law and Guidelines, and ensure uniform steps are taken by DOJ personnel to identify and notify victims of identity theft. In its response, the ODAG stated that this effort may include reviewing and revising as necessary the Attorney General Guidelines for Victim and Witness Assistance or issuing guidance that clarifies what is required under existing guidelines and applicable law. The ODAG also stated that DOJ would coordinate this effort with the Office for Victims of Crime and other relevant DOJ components.

    This recommendation can be closed when we are provided a copy of the guidance issued to all DOJ components that clarifies responsibilities pertaining to identifying and notifying identity theft victims and helps components ensure compliance with applicable law and Attorney General Guidelines. Additionally, DOJ should inform the OIG of any revisions to the Attorney General Guidelines for Victims and Witness Assistance that are related to identity theft victims.

12. **Resolved.** OJP concurred with our recommendation that DOJ, OJP, and the Bureau of Justice Statistics (BJS) ensure that identity theft statistics gathered through the National Crime Victimization Survey are reported in a timely manner. In its response OJP acknowledged that data releases from the National Crime Victimization Survey have not been timely and that BJS is working to improve this situation. Accordingly, BJS anticipates releasing the 2006 through 2008 identity theft statistics on its website by June 2010. This recommendation can be closed when we receive evidence showing that the identity theft statistics for 2006 through 2008 have been released to the public. In addition, BJS should describe any planned action designed to ensure that identity theft statistics for subsequent years are reported in a timely manner.

13. **Resolved.** OJP concurred with our recommendation that DOJ, OJP, and BJS evaluate the feasibility of regularly collecting identity theft data for individual victims instead of households. OJP stated in its response that BJS currently is conducting an evaluation to determine the feasibility of collecting identity theft data from individual victims. This recommendation can be closed when we are provided with the results this evaluation. Additionally, if it is determined that BJS cannot collect data for individual identity theft victims, BJS should provide the OIG with a detailed explanation supporting this determination.

14. **Resolved.** OJP concurred with our recommendation to ensure that its identity theft working group continues to meet regularly to make certain that each office and bureau is appropriately considering future identity theft-related initiatives. In its response OJP stated that for the remainder of 2010 it has planned regular bi-monthly meetings of its working group to discuss issues surrounding victimization, enforcement, training, funding, prevention, outreach, and research. OJP also provided evidence that its identity theft working group held a meeting on March 10, 2010. This recommendation can be closed when OJP provides evidence that its working group continues to meet on a regular basis and that its offices and bureaus, through these meetings or otherwise, are considering future identity theft initiatives.