



THE UNITED STATES NATIONAL CENTRAL BUREAU OF INTERPOL

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

Audit Report 09-35
September 2009

THE UNITED STATES NATIONAL CENTRAL BUREAU OF INTERPOL

EXECUTIVE SUMMARY

The International Criminal Police Organization (INTERPOL) facilitates the exchange of information to assist law enforcement agencies in the United States and throughout the world in detecting and deterring international crime and terrorism through a network of 187 member countries.¹ Each INTERPOL member country establishes a National Central Bureau (NCB) to serve as its liaison between the member country's law enforcement agencies and INTERPOL. NCBs work with the police authorities in their countries to transmit, respond to, and execute requests for information and assistance in criminal investigations and police matters to and from other countries' NCBs via the INTERPOL communications network.

The United States National Central Bureau (USNCB) is the entity through which the United States functions as an INTERPOL member and serves as a point of contact for U.S. federal, state, local, and tribal law enforcement for the international exchange of information. The USNCB has a fiscal year (FY) 2009 budget of approximately \$24.5 million and 65 full-time equivalent employees. In addition, as of December 2008 the USNCB had 24 staff members detailed to it from federal, state, and local law enforcement agencies.

To facilitate the exchange of information between international law enforcement agencies, INTERPOL has developed a secure, Internet-based, virtual private network known as I-24/7 through which: (1) NCBs can instantly communicate with other NCBs and the INTERPOL General Secretariat, and (2) INTERPOL member countries can instantly access a wide range of criminal information located in INTERPOL's databases – including terrorism-related information and information on stolen and lost travel documents. This information comes from queries, messages, intelligence, and submissions from law enforcement officials in member countries.

INTERPOL also utilizes a system of color-coded international notices and "diffusions" that share crime-related information with each member

¹ A listing of all INTERPOL member countries can be found in Appendix IV.

country.² This information concerns individuals wanted for serious crimes, missing persons, unidentified bodies, possible threats to public safety, and criminals' modus operandi, as described in the following table. As of February 2009, INTERPOL had nearly 25,000 active notices, of which most were red.

Types of INTERPOL Notices³



Red Notice - Requests to seek the location and arrest of a wanted person with a view to extradition based on an arrest warrant or court decision.



Blue Notice - Collects information about, locates, or identifies a person of interest in a criminal investigation.



Green Notice - Provides warnings about persons who have committed criminal offenses and are likely to repeat these crimes in other countries.



Yellow Notice – Provides information to help locate missing persons, especially minors, or to help identify persons who are not able to identify themselves.



Black Notice - Requests information about unidentified bodies.



INTERPOL-United Nations Security Council Special Notice - Alerts police of groups and individuals who are the targets of U.N. sanctions against Al Qaeda and the Taliban.



Orange Notice - Warns police, public entities, and other international organizations of dangerous materials, criminal acts, or events that pose a potential threat to public safety.

Source: INTERPOL

² A diffusion is a message sent by a member country to other member countries without a formal review conducted by INTERPOL. Frequently, the diffusion is sent to immediately disseminate information pending submission and approval of the more formal notice. A diffusion contains information similar to a notice. However, member countries also use diffusions to request assistance.

³ Notices are published in the organization's four working languages: Arabic, English, French, and Spanish.

Background of INTERPOL

Established in 1923 and currently located in Lyon, France, INTERPOL is an international police organization that seeks to facilitate cross-border police cooperation and support and seeks to assist organizations whose mission is to prevent or combat international crime. INTERPOL provides secure global police communication services, operational police support services, and police training and development.

INTERPOL is governed by a General Assembly, consisting of delegates appointed by member countries, which meets once a year to make all major decisions affecting general policy.⁴ An Executive Committee oversees the execution of the decisions of the General Assembly, as well as the work of the Secretary General.⁵ The Secretary General oversees INTERPOL's day-to-day work of international police cooperation.⁶

INTERPOL is funded primarily by member country annual statutory contributions. To assess each member countries' dues contribution, INTERPOL uses a formula based on the countries' economic well being. This formula was renegotiated in the late 1990s and incorporated a gradual increase in the percentage share paid by the wealthiest nations. The United States' share of the annual INTERPOL budget increased from 5 percent in fiscal year (FY) 2003 to the current rate of 13.26 percent in FY 2006. In 2008, INTERPOL's total statutory budget was approximately \$64.1 million and the United States' contribution to INTERPOL was \$8.5 million. According to USNCB officials, INTERPOL is again proposing an adjustment to the dues formula and it is expected that the United States' contribution will gradually increase from 13.26 percent in 2009 to 17.385 percent in 2014.

In FY 2008, INTERPOL had a staff of 588, representing 84 countries. In addition to 398 contract employees, INTERPOL also had 190 seconded

⁴ Each country has one vote and all votes carry equal weight.

⁵ The INTERPOL Executive Committee has 13 members elected by the General Assembly.

⁶ The Secretary General is nominated by the Executive Committee, confirmed by at least two-thirds of the General Assembly, and serves a 5-year term. Ronald K. Noble, the current Secretary General, was initially elected in 2000 and currently is serving a second term. Secretary Noble is a national of the United States and served as a former Undersecretary for Enforcement with the U.S. Department of Treasury.

staff from member countries.⁷ As of May 2009, the United States had seven individuals detailed to INTERPOL.

Background of the USNCB

The responsibility for management of the USNCB has varied since the USNCB became operational in 1968. It was initially placed under the direction of the Department of the Treasury (Treasury). In 1977, the Department of Justice (DOJ) and Treasury signed a Memorandum of Understanding (MOU) that established joint DOJ and Treasury management of the USNCB. In 1981, an amendment to the MOU placed the USNCB within DOJ, reporting to the Deputy Attorney General, but still under the co-management of Treasury and DOJ. A May 2003 MOU transferred responsibility for the management of the USNCB to DOJ and the Department of Homeland Security (DHS).⁸ The MOU also established senior management positions in the USNCB, which rotate between the two departments every 3 years.⁹

OIG Audit Approach

Our objectives for this audit were to: (1) evaluate the USNCB's efforts to ensure sharing of INTERPOL information among federal, state, local, and tribal law enforcement agencies; (2) review the USNCB's processes for the exchange of INTERPOL information to ensure that requests for assistance and information were handled in an appropriate, efficient, and timely manner; (3) review the USNCB's controls over INTERPOL case information; and (4) examine the USNCB's organizational role and strategic priorities to ensure that they are in line with DOJ priorities.

To accomplish these objectives we interviewed the USNCB Director, Deputy Director, and Assistant Directors; participating agency representatives at the USNCB; DOJ officials in the Office of the Deputy Attorney General, Federal Bureau of Investigation (FBI), and Drug Enforcement Administration (DEA); the INTERPOL Secretary General;

⁷ Seconded staff are individuals who are temporarily assigned to INTERPOL by their national administrations and compensated by their national administrations or by INTERPOL.

⁸ DOJ is responsible for the administrative costs of operating the USNCB.

⁹ The USNCB Director and Deputy Director must serve a term of at least 2 years, but not more than 3 years. The current USNCB Director is a Supervisory Special Agent with DHS's U.S. Immigration and Customs Enforcement, and the Deputy Director is a Chief Inspector with DOJ's U.S. Marshals Service.

officials at the INTERPOL General Secretariat in Lyon, France; and law enforcement officials from the Bundeskriminalamt (BKA) located in Wiesbaden, Germany.¹⁰

to understand its working relationships, the assistance it provides, and its communication with local offices.¹¹ We also distributed a questionnaire to 66 state and local liaison officers across the United States to assess the level of cooperation and satisfaction among the USNCB and its domestic partners.

To evaluate the USNCB's processes and controls over the exchange and integration of information, we reviewed the USNCB's policies and procedures for maintaining data within its case management system, and we performed various tests on domestic and foreign law enforcement agency notices and diffusions. We also reviewed records from automated domestic data systems to determine if INTERPOL information was included in the databases in a timely manner and whether the information was accurate, complete, and consistent.

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

Results in Brief

We identified several weaknesses in the USNCB's operations that need improvement. We found that the USNCB has not fully made critical international criminal information, such as information regarding international fugitives and habitual criminals, available to appropriate law enforcement agencies in the United States. For example, the USNCB has not provided domestic law enforcement agencies with information about travel documents that have been reported lost or stolen. This has increased the potential that high-risk, violent criminals can enter undetected and move about freely in the United States.

The USNCB also has not implemented adequate controls or processes to ensure that the INTERPOL information it has made available to domestic

¹⁰ The BKA is the German national police force, which also serves as the NCB for Germany.

¹¹ To facilitate information sharing with law enforcement agencies, the USNCB has established a liaison office in each state, as well as in American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, the U.S. Virgin Islands, and in 11 major cities in the United States. For a list of the 66 state and local liaisons, please see Appendix V.

law enforcement agencies is current, accurate, complete, and timely. For example, when we examined the USNCB's processing of 52 foreign-issued notices and diffusions that met USNCB guidelines for entering a lookout record into the FBI's National Crime Information Center (NCIC), we found that approximately 87 percent did not have a corresponding lookout record in NCIC.¹² In addition, within 92 foreign-issued notices and diffusions we reviewed, we identified 53 inconsistencies in the information contained in the domestic system records.¹³ Consequently, domestic law enforcement data systems likely contain out-of-date or incomplete data and include information on individuals for whom no law enforcement agency has a current investigative interest.

We also identified several weaknesses with the USNCB's internal case management system called ENVOY. When we reviewed a sample of 216 cases selected from notices and diffusions active from October 1, 2005, through May 29, 2008, we found that the USNCB case files in ENVOY were disorganized and inconsistently assembled, and we identified transposition errors, missing data, duplicate entries, and improper classification. We also found documents that were filed in the wrong case file and identified three instances in which information pertaining to two unrelated individuals appeared to have been erroneously combined into a single case file.¹⁴ In addition, we found poor record retention and disposal, including boxes of non-archived paper case files located in the hallways of the USNCB, inadequate management reporting and statistics, a lack of audit trails, and inadequate standardized correspondence. As a result, without better management of its case-related information, the USNCB cannot ensure that accurate information is easily and readily available throughout the USNCB. Additionally, if the USNCB does not properly control access to its information, there is a risk of loss, as well as the possibility the privacy of individuals on whom the information is maintained will be violated.

According to INTERPOL, as of December 31, 2008, the United States was the source of the highest number of active red notices among member countries. However, we reviewed the public websites of the FBI, DEA, and Immigration and Customs Enforcement (ICE), and found 14 of

¹² The National Crime Information Center (NCIC) is a computerized index of criminal justice information (i.e., fugitives, stolen properties, missing persons) maintained by the FBI. NCIC is available to federal, state, local, and tribal law enforcement and other criminal justice agency users and is operational 24 hours a day, 365 days a year.

¹³ Not all of the 92 records we reviewed contained inconsistencies. Some records contained multiple inconsistencies.

¹⁴ For a detailed description of our methodology, see Appendix I.

32 international “most-wanted” fugitives on these sites for whom red notices had not been issued. Information related to these types of cases should be shared with appropriate foreign counterparts through the INTERPOL network because this information can reach places where U.S. law enforcement agencies do not have a physical presence and increase the likelihood that fugitives are captured.

We also found that the USNCB is not able to consistently coordinate the sharing of case-related information because it is often not informed of actions taken by its U.S. law enforcement partners on INTERPOL-related cases. For example, we identified a February 2005 wanted person diffusion issued by another country’s NCB for an individual wanted for homicide and attempted homicide. When the other NCB inquired of the USNCB as to reasons why the subject was allowed to remain free when the individual was encountered, the USNCB was unaware that at least three U.S. federal law enforcement agencies were simultaneously working the case.

As a result of this inadequate communication and coordination, an individual wanted for homicide and attempted homicide was allowed to evade prosecution in another country. We believe better communication and coordination between all of these agencies would have prevented this subject from evading apprehension.

In addition, the USNCB has faced challenges in maintaining reliable communications with its state and local liaisons. Although the USNCB believed that it had established secure electronic communications with these liaisons, we found that several of these connections were not functional. Specifically, when we distributed a questionnaire to each of the USNCB’s 66 liaison offices through the USNCB’s secure electronic connections, only one-third of the offices responded. When we contacted the liaison offices by telephone, we found that 25 of the 66 offices had not received the questionnaire. Subsequently, we determined that some liaisons did not receive the questionnaire because the e-mail messages addressed to them were undeliverable or because there may have been a technical problem with the network used to send the messages. Ultimately, we learned that the USNCB had to send some of our questionnaires via facsimile.

Despite its attempts to ensure that it has an adequate method to communicate with its liaisons, we found that the USNCB does not have a reliable and complete network of connectivity with its liaisons. The USNCB must ensure that these connections are functioning adequately so that it has the ability to communicate important information to its state and local liaison offices.

We also identified weaknesses in the oversight and supervision of the USNCB by DOJ and DHS. We found that the USNCB Executive Committee, which is composed of senior DOJ and DHS officials and is supposed to provide guidance to the USNCB, has not met in more than 5 years. This lack of oversight has prevented the USNCB from developing a comprehensive strategic vision for moving the organization forward.

In addition, we identified weaknesses in the leadership structure of the USNCB, which is co-managed by DOJ and DHS through a Director and Deputy Director who are rotated between the departments every 3 years. This current rotational structure creates problems in compensation and career advancement for USNCB leadership. Under the present format, the Director is a term appointment at the Senior Executive Service (SES) level, while the Deputy Director must be "SES-eligible." As a result, the Deputy Director must spend at least 3 years at the top of the General Schedule (GS-15) level before being considered for the Director appointment at the SES level. This causes the individuals to spend 6 years at two different grades and salaries, only to revert back to the lower GS-15 level at the completion of their service at the USNCB. In addition, this disparity in rank between the USNCB Director and executives at other federal law enforcement agencies may cause these other executives to perceive that the USNCB is less important than an agency headed by a career SES employee.

Our report contains detailed information on the full results of our review of the USNCB. The remaining sections of this Executive Summary summarize our audit findings.

Federal Agency Participation in INTERPOL

The United States' level of participation in INTERPOL depends on the USNCB's relationships with U.S. law enforcement agencies. We found, however, that some federal law enforcement agencies do not fully participate in INTERPOL's red notice program for a variety of reasons. Moreover, the USNCB is often not informed of actions taken by its federal domestic law enforcement partners on INTERPOL-related cases, and as a result the USNCB is hindered in its coordination with other member countries.

Red Notice Program

Not every federal law enforcement agency participates fully in INTERPOL's red notice program. When we reviewed public websites of the DEA, the FBI, and ICE, we noted that 14 out of 32 international fugitives listed on the agencies' websites did not have INTERPOL red notices issued on them. Information related to these types of cases should be shared with appropriate foreign counterparts through the INTERPOL network because it can allow U.S. law enforcement agencies to reach places where they do not have a physical presence and increase the likelihood that fugitives are captured.

We talked to various officials about why no red notices had been issued for these fugitives. The USNCB Director, who is also a DHS ICE employee, attributed ICE's failure to coordinate with the USNCB and obtain INTERPOL red notices in these instances to insufficient numbers of experienced personnel being detailed from DHS to the USNCB.

We also spoke with the FBI Assistant Director for International Operations, who stated that all 10 FBI most-wanted fugitives should have a red notice and he did not know why they did not. He also stated that the FBI has directed its agents to issue INTERPOL notices for all outstanding FBI fugitives believed to be in a foreign country and that the FBI special agent in charge of the case or the FBI representative at the USNCB should be responsible for publishing the notice.

When we spoke with the Assistant Director for the USNCB Drug Division, a DEA employee, she said that she has been working to improve the DEA's participation in INTERPOL by conducting training sessions for DEA agents. A DEA headquarters official told us, however, that the agency does not issue INTERPOL notices because of the sensitivity of DEA drug cases and concerns regarding security of case information. While we understand the DEA's desire to protect sensitive information, the information listed on the DEA's public website is accessible to anyone with an Internet connection and therefore cannot be considered sensitive.

The current process for issuing a red notice involves an extensive paper-based application form that must be completed by the nominating law enforcement agent. It is then assigned to and reviewed by a USNCB case agent, reviewed by the USNCB General Counsel, and then submitted to INTERPOL for a secondary review and publishing. The USNCB General Counsel said that an on-line process for the submission of red notice applications and diffusion requests might encourage U.S. law enforcement agencies to increase their participation in the program. He also said that the

FBI has developed its own capability for submitting the applications electronically. However, he stated that he doubted the USNCB has sufficient current resources to develop such a capability.

We agree that that an on-line procedure would streamline the process and make it easier for domestic law enforcement agencies to seek the issuance of red notices, and we believe that the USNCB should plan and budget for this initiative.

Case Resolution Information

We found that the USNCB's ability to adequately coordinate the sharing of case-related information is hindered because it is often not informed of actions taken by its U.S. law enforcement partners on INTERPOL-related cases. For example, officials at both the FBI and DEA said their agents often deal directly with their foreign counterparts when they need information about a case with an international nexus, bypassing the USNCB. According to a USNCB official, this lack of communication with the USNCB significantly impacts the USNCB's ability to coordinate the exchange of information and the United States' response to inquiries from domestic and foreign law enforcement agencies. Additionally, while this flow of information directly between agencies may meet the immediate needs of the agencies involved, the information passed remains "stovepiped" within these agencies instead of being shared with other law enforcement entities that also may have a need for it. Moreover, the USNCB is not informed about the final outcome of INTERPOL investigations, and it thus cannot accurately measure the impact of its efforts and compile meaningful management statistics.

State and Local Law Enforcement Coordination

As the U.S. point of contact for INTERPOL matters, the USNCB must maintain a close relationship with domestic law enforcement agencies. To promote relationships with domestic agencies, the USNCB established 66 state and local liaisons in each U.S. state and territory, as well as in 11 major U.S. cities, who serve as the point of contact for USNCB-related interactions. The USNCB forwards to one or more of the liaisons foreign government requests that require action by a state or local law enforcement agency. The liaisons then forward the requests to the appropriate law enforcement agency in their jurisdiction for processing and response. Additionally, domestic law enforcement agencies that need criminal investigative assistance on cases with an international nexus may forward a request through the appropriate liaison or contact the USNCB directly.

The liaisons and the USNCB communicate using a secure e-mail network. However, when we submitted a survey questionnaire to each of these liaison offices through the secure e-mail network, we found that 25 of the 66 offices had not received it. USNCB officials said they were surprised, and after further inquiry determined that some of the e-mail messages were undeliverable and there may have been a technical problem with the network used to send the messages. Eventually, the USNCB had to send some of our questionnaires to its liaisons via facsimile.

Our concern is that the USNCB was unaware that its connection to its liaisons was unreliable and it had not implemented easily activated controls (such as e-mail receipt confirmations) to ensure that its messages were received. We believe that the USNCB must ensure that these connections are functioning adequately so that it can be certain that it can communicate important information to its state and local liaisons.

In short, we found that the USNCB has not developed, implemented, or maintained a reliable communications network with its liaisons. This deficiency means that critical law enforcement information or requests for assistance are not being effectively disseminated. For example, the USNCB could issue a diffusion to a liaison in a city police agency that a known international fugitive is traveling to that city. But because of the unreliable nature of the communication network, the police agency may not receive the message, no action may be taken on the fugitive, and the USNCB would not know that the message has not been received and no action has been taken. Therefore, it is imperative that the USNCB ensure that its connections to state and local liaison officers are functioning so that criminal and law enforcement information gets conveyed to the appropriate agencies and requests can be responded to in a timely manner.

INTERPOL Database Direct Connectivity

At the beginning of our audit, the USNCB told us that it had made significant progress in providing all state and local law enforcement agencies with the ability to independently query INTERPOL databases through the International Justice and Public Safety Information Sharing Network (Nlets).¹⁵ Specifically, the Assistant Director for the USNCB's State and Local Liaison Division stated that a majority of the 50 State Terminal Control agencies had signed Memoranda of Understanding (MOU) that are required by the USNCB for organizations to gain access to the INTERPOL databases.

¹⁵ Nlets State Terminal Control agencies are law enforcement agencies in each state that are assigned the responsibility for managing access to the Nlets network and ensuring that Nlets's system security and operational policies and procedures are carried out within the state.

Having this connection would provide these agencies with the ability to query INTERPOL's databases and obtain criminal justice-related information, such as information on known and suspected international criminals, wanted international fugitives, and stolen and lost travel documents.¹⁶

We found that although the USNCB had established an Internet connection between INTERPOL and each state through Nlets, each state must first make modifications to its local system before being able to access INTERPOL databases. We determined that as of September 2008 only a limited number of states had fully implemented the necessary modifications to their systems. According to the USNCB Assistant Director for the State and Local Liaison Division, some states were reluctant to make the necessary modifications because of budget and other resource constraints.

We also found that Nlets requires that state or local law enforcement generate separate queries, in addition to a standard query to NCIC, to access the INTERPOL databases. Standard queries made by law enforcement officers to NCIC return information contained in NCIC's files, such as its wanted person and gang files. After law enforcement officers run an NCIC query, unless they have additional information or a reason to believe that an individual may be a person of interest to another country, there is no way for them to know whether they should perform an additional query of INTERPOL's databases to obtain additional information. We believe that requiring officers to perform multiple queries increases the risk that information on these subjects does not reach frontline law enforcement officers who encounter them.

When we informed the USNCB of these findings, the USNCB Director initiated discussions with the FBI to develop a method for state and local law enforcement agencies to directly query the INTERPOL databases via NCIC. The FBI and USNCB made an agreement in October 2008 to conduct a study to determine if NCIC can provide a viable environment for delivering to state and local law enforcement officers increased access to INTERPOL data, including notice, stolen motor vehicle, and lost and stolen travel document information. In April 2009, the USNCB reported that it was in the final stages of testing the requisite infrastructure upgrades for the study and had requested sample data from the FBI's Criminal Justice Information Services (CJIS) component to begin testing the process.¹⁷ The USNCB anticipated that it would begin this testing in May 2009.

¹⁶ A description of all 11 INTERPOL databases can be found on page 8 of the report.

¹⁷ Established in February 1992, the FBI's Criminal Justice Information Services (CJIS) component manages NCIC.

International Criminal Information Sharing Processes

USNCB analysts review information received from foreign law enforcement agencies and enter a “lookout record” in or provide appropriate international criminal data from INTERPOL to domestic agencies or related domestic systems, such as the FBI’s Foreign Fugitive File and Missing Person File within its NCIC system, DHS’s Traveler Enforcement Compliance System (TECS) and United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, the U.S. Department of State’s (State Department) Consular Lookout and Support System (CLASS), and the National Counterterrorism Center’s (NCTC) Terrorist Identities Datamart Environment (TIDE).¹⁸ The information in these databases is regularly used in various screening processes. For example, DHS Customs and Border Protection (CBP) agents encounter individuals at various U.S. ports-of-entry and search TECS to determine if a person can be granted access to the United States. When an individual who appears to match the subject of an INTERPOL notice or diffusion is identified, foreign or domestic law enforcement agencies receive a return message through the agency database informing them of the preliminary match and directing them to call the USNCB. Staff at the USNCB’s 24-hour call center verify with the originating law enforcement agency that the information is current, accurate, and reliable.

Information Not Shared with U.S. Agencies

It is critical that international criminal information is appropriately and timely disseminated to domestic law enforcement officers and to U.S. government personnel deciding on the admissibility of individuals attempting to cross a U.S. border. We found that although the USNCB has made some INTERPOL information accessible to these law enforcement agencies, it has not done so for all of the information that it receives.

For example, the USNCB assists with border protection by entering or facilitating the entry of foreign notices and diffusions into border screening systems such as TECS and CLASS. However, the USNCB does not fully share INTERPOL information with NCIC and therefore complete information is not always available to domestic law enforcement personnel who might encounter notice or diffusion subjects who have already entered the United States. Specifically, we found that the USNCB does not enter a record into NCIC for the subjects of foreign-issued green notices. These individuals (including habitual criminal offenders, child molesters, and child pornographers) are considered career criminals who have committed, or are

¹⁸ A description of each of the aforementioned data systems is contained in Appendix VIII.

likely to commit, offenses in several countries. We therefore believe that the subjects of green notices should be entered into NCIC. If this is done, although the individuals may be allowed to enter the country, if the individuals commit criminal acts in the United States, law enforcement officers investigating those acts will have more information as they attempt to solve the crimes.

According to the USNCB Compliance Officer, the USNCB has not sought, nor has the FBI authorized, the USNCB to enter information into NCIC files other than the Foreign Fugitive and Missing Person Files. Because the career criminals identified in green notices are neither foreign fugitives nor missing persons they are not entered into NCIC. USNCB officials stated that they have not sought approval from the FBI to enter information into other NCIC files, such as the Sexual Offender or the Violent Gang and Terrorist Organization File. When we asked the USNCB Director about entering the subjects of green notices into NCIC, he said that doing so would be a good idea.

We believe that the potential threat to the U.S. posed by individuals who are the subject of foreign-issued green notices makes it essential that information about them be shared with domestic law enforcement agencies. We therefore recommend that the USNCB explore options to ensure that information on the types of foreign criminals identified in green notices is available to all law enforcement agencies.

In addition, the USNCB stated that although it could enter lookout records into NCIC for subjects of foreign-issued diffusions, it does not because INTERPOL-member countries often do not update diffusion information. While we recognize that some member countries do not ensure that the information contained in its diffusions remains accurate and current, the USNCB maintains a 24-hours per day, 7 days per week call center that the USNCB directs domestic law enforcement agencies to contact before taking any law enforcement action based upon INTERPOL information. The call center verifies with the originating law enforcement agency that the information is current, accurate, and reliable. With the existence of the call center and given the risk inherent with allowing dangerous criminals to enter or remain in the country, we believe that the USNCB should explore options for including foreign diffusions in NCIC.

We also found that the USNCB has not pursued including in NCIC important information contained in the INTERPOL Stolen and Lost Travel Documents database (SLTD), such as lost or stolen passports. According to the USNCB, INTERPOL rules do not allow for the downloading of SLTD data into national databases because this would impede INTERPOL member

countries' ability to automatically update the data and receive automatically generated notifications when their records are viewed. Notwithstanding this requirement, we believe it is important that the USNCB develop an acceptable method to provide domestic law enforcement agencies with access to the information in the SLTD because inadmissible aliens may enter the United States using a stolen or lost passport from a visa waiver country.¹⁹

In short, in our judgment the USNCB does not ensure that certain critical information from INTERPOL is made available to frontline U.S. screening agencies. By not entering important information into available databases or sharing it with other law enforcement agencies, the United States misses opportunities to capture foreign career criminals or prevent them from entering the country.

Data Quality Deficiencies

To examine the USNCB's sharing of INTERPOL information with domestic law enforcement agencies, we judgmentally selected 216 foreign and domestic notices and diffusions that were active between October 1, 2005, and May 29, 2008.²⁰ Our examination showed that the USNCB has not implemented adequate controls or processes to ensure INTERPOL information is being made available to U.S. agency systems in an accurate, current, and timely manner. In addition, we found that the U.S. agency systems likely contain out-of-date or incomplete data, include information in which law enforcement agencies have no current interest, and may include information that violates INTERPOL's guidelines for handling information. These guidelines establish record-purging requirements and take into consideration member countries' privacy laws to help ensure that data is not improperly retained or utilized.

We found that the USNCB did not enter eligible foreign notices and diffusions into U.S. databases, as required by USNCB guidelines. Specifically, we examined the USNCB's processing of 115 foreign-issued notices and diffusions and found that 92 met the criteria for entry of a lookout into TECS. However, we found that 21 of the 92 cases, or approximately 23 percent, did

¹⁹ The Visa Waiver Program was created to facilitate international travel and is a substitute entry mechanism for non-immigrant, short-term business and tourism visas only; it does not apply to students, temporary workers, and others who require visas to enter the United States.

²⁰ Our sample consisted of 42 domestic notices, 59 domestic diffusions, 62 foreign notices, and 53 foreign diffusions. The complete methodology of our analysis can be found in Appendix I.

not have a lookout record entered in TECS. In addition, although 52 of the 115 cases met the criteria for entry into NCIC, our analysis revealed that 45 of the 52 cases, or approximately 87 percent, did not have a lookout record entered in NCIC.

USNCB officials were unable to provide an explanation for the 21 records missing from TECS. However, for the 45 records missing from NCIC, the officials said the USNCB was erroneously applying a restrictive set of criteria for including the records in NCIC. They believed that the subject's height, weight, and hair color were required for entry, but the FBI does not require the USNCB to enter these fields if either the subject's photograph or fingerprints are available.

We also assessed whether the USNCB entered records into these systems in a timely manner. According to USNCB internal policies, if a foreign notice or diffusion contains sufficient information and meets the criteria for entry into TECS and NCIC, USNCB analysts are required to enter a lookout record immediately upon receipt of the foreign communication. We found that of 71 lookout records entered into TECS by the USNCB that we reviewed, only 31 percent were entered within 1 day, while more than 40 percent were entered more than 30 days after initial receipt. USNCB officials attributed these delays to an increasing workload, limited resources, and the necessity of translating some INTERPOL documents into English.

Using our sample of 92 foreign-issued notices and diffusions that met the criteria for entry in TECS or NCIC, we examined the corresponding domestic system records to determine if the USNCB entered basic information such as name, date of birth, gender, passport number and country, warrant information, additional identification numbers, and physical characteristics in the databases. We compared the information contained in the foreign-issued notice or diffusion to data entered by the USNCB into TECS, NCIC, or ENVOY. Out of 92 records we reviewed, we identified 53 inconsistencies in the information contained in the domestic system records.²¹ When we discussed our findings with USNCB officials, they were unable to provide an explanation for the inconsistencies. Additionally, although USNCB internal case management policies require supervisory review within 48 hours of entry, we found that most case files had no evidence of any supervisory review.

²¹ Not all of the 92 records we reviewed contained inconsistencies. Some records contained multiple inconsistencies.

Inadequate Message Handling

During our discussions with USNCB officials regarding the deficiencies in the USNCB's handling of INTERPOL data, the officials attributed many of the problems and delays to the need to translate documents, increasing workload, and limited personnel and financial resources. However, during our review of the USNCB's procedures, we noted that many of the problems were attributable to the USNCB's manual data entry processes, which were overly labor-intensive, time-consuming, and prone to errors, transpositions, and omissions.

The notices and diffusions that the USNCB receives from INTERPOL and other member countries generally consist of electronic messages with attached documents. To share this information electronically with domestic law enforcement agencies, USNCB analysts manually copy or enter the data from the message or document – field-by-field – and paste it in the appropriate databases. Conversely, when sending a notice or diffusion to INTERPOL or other member countries, the USNCB must first extract the electronic data from its databases and then convert the information into an electronic message or document.

When we discussed this issue with INTERPOL officials in Lyon, France, they acknowledged that this manual process was inefficient. INTERPOL officials indicated that they had experienced problems similar to those at the USNCB, including issues related to notice and diffusion translation, workload, and limited resources. INTERPOL officials also told us that to address these issues, they had developed an international standard for the transmission of law enforcement information and implemented a new software messaging application that will completely automate the notice and diffusion process. Officials said this new system, called I-Link, should eliminate the manual entry and manipulation of data by both INTERPOL and USNCB analysts.

During our audit, I-Link was launched on January 19, 2009, and underwent a 2-month trial during which the USNCB tested the red notice form application. Although a few of the NCBs are using I-Link, the USNCB stated that as of May 2009 most of the NCBs were still testing the I-Link system.

However, during the testing period the USNCB found that the program was not easy to use and it identified several legal issues related to the wording of the notices. In addition, the USNCB identified significant problems with data integrity and accuracy. The USNCB stated that it has reported these issues to the INTERPOL I-Link project manager. The USNCB continues to attend the I-Link advisory group meetings and is working with

INTERPOL to attempt to resolve the issues. However, the USNCB did not provide an estimated date that it would fully implement the I-Link system.

Deficient Internal Case Management System

ENVOY is the computer database that the USNCB uses to maintain and organize all documentation – including notices and diffusions – related to assistance or information requests from international law enforcement agencies. ENVOY is intended to provide the USNCB with records management, workflow management, automated workflow processes, and records search and reporting capabilities. However, according to the USNCB Chief Information Officer (CIO), the USNCB experienced significant operational issues with the initial version of ENVOY, including system instability, a lack of software documentation, and limited reporting capability.²² Although some of its issues have been resolved, ENVOY still lacks reporting capability, and the USNCB has significant problems tracking basic workload statistics, including the number of active notices and diffusions. The USNCB CIO also stated that because of a lack of funding, the USNCB has adopted a phased approach and has made incremental improvements to ENVOY.

During our review of ENVOY, we found three areas needing attention:

- **Record Retention and Disposal.** USNCB policy requires that records be retained on-site for 2 years after a case closing. After 2 years, the records are to be archived and stored at an off-site facility. If there is no case activity within 5 years after transfer to an off-site facility, the documents can be destroyed. However, we found that records not transferred off-site after 2 years and boxes of paper case files were still being held at the USNCB. Additionally, the USNCB Compliance Officer told us that none of the electronic case files in ENVOY have ever been archived. Because the USNCB does not archive or restrict access to outdated information in its case management system, it has not ensured that the obsolete data is not accessed by USNCB analysts and agents. Therefore, personal data on individuals for whom there is no active law enforcement investigative interest may still be accessed, contrary to INTERPOL policies.
- **Management Reporting and Statistics.** The USNCB needs a case management system that can compile basic workload statistics, such as the number of cases opened for notices and diffusions. However,

²² ENVOY was initially implemented in 1999 to replace the USNCB's previous case management system, the INTERPOL Case Tracking System.

ENVOY cannot track the number of notices and diffusions opened or the time elapsed between key events in its case processing, such as when the USNCB receives a notice or diffusion, when the case is opened, and when lookout records are entered in U.S. agency databases. This deficiency hampers the USNCB's ability to accurately measure its performance, determine resource needs, and set benchmarks for improvement. The USNCB CIO said there is no way to track this information because ENVOY has limited reporting capabilities. As a result, the USNCB has developed workaround processes to generate and compile its management statistics. However, we found that these ad-hoc processes are often inaccurate and unreliable.

- **Audit Trails and Standardized Correspondence.** During our review of ENVOY, we noted that the system does not maintain information on historical transactions within the database. As a result, the USNCB is unable to determine what actions were performed by which analyst or supervisor. Without knowing who created or modified a record, there is no way to go back and determine why a particular action was taken (or not taken) or a modification was made to a record. Additionally, the USNCB would be unable to identify an individual who made repeated mistakes and provide them training. The USNCB has designed standardized templates for its analysts to use when preparing routine correspondence and the electronic process saves a copy of the correspondence to the case file. However, several analysts stated that they do not use the electronic processes and have developed their own templates for routine correspondence. As a result, the diffusions generated by some of the USNCB analysts may not contain the information necessary to conduct an investigation, as well as not comply with statutes of the INTERPOL Constitution, U.S. laws, and the provisions of the Freedom of Information and Privacy Acts. We also noted that the electronic process frequently created multiple copies of the same USNCB-prepared correspondence, all of which were saved in the case file. Saving multiple copies of the same or similar documents to the case file can result in delayed investigations while analysts attempt to determine which version of the document contains the most accurate and current information. Further, the process also overstates the number of diffusions generated and therefore overstates the USNCB's reporting of the total number of diffusions processed in a given period.

Although the USNCB hoped to deploy a new case management system by December 2008, the CIO informed us that as of January 2009 the new case management system had been delayed because of other information

technology priorities. In April 2009 the USNCB stated that it had resolved several technical difficulties that were encountered during development, and after hiring an additional developer to help expedite the delivery schedule, officials said they anticipate that the upgrade will be completed by mid to late August 2009.

New Quality Assurance Program

In February 2008 the USNCB implemented a new quality assurance program that we believe is an important first step to enhancing the accuracy of its information. The new program requires a more thorough review of cases and more documentation of the reviews completed. It also requires more involvement in the review process by division supervisors and assistant directors. The inaccuracies that we identified in the USNCB's case files underscore the need for these additional reviews to ensure that the information provided by the USNCB is reliable.

Department's Lack of Support and Oversight

The May 2003 MOU, which gave DOJ and DHS joint responsibility for managing the USNCB, also established an Executive Committee for overseeing the USNCB consisting of the Deputy Attorney General, Deputy Secretary of DHS, and the USNCB Director. The Executive Committee was to meet semi-annually and make all USNCB policy and personnel decisions, except those delegated to the Director.

However, according to an Office of the Deputy Attorney General (ODAG) official responsible for USNCB matters, the Executive Committee has not met for at least 5 years. As a result, we believe that the USNCB has not received sufficient guidance and oversight to ensure that it effectively discharges its responsibilities. We identified four areas that we believe need DOJ and DHS oversight.

Leadership

The USNCB is co-managed by DOJ and the DHS through a Director and Deputy Director who are rotated between the departments every 3 years. This current rotational structure creates problems in compensation and career advancement for USNCB leadership. Under the present format, the Director is a term appointment at the Senior Executive Service (SES) level, while the Deputy Director must be "SES-eligible." As a result, the Deputy Director must spend at least 3 years at the top of the General Schedule (GS-15) level before being considered for the Director appointment at the SES level. This causes the individuals to spend 6 years at two different

grades and salaries, only to revert back to the lower GS-15 level at the completion of their service at the USNCB. In addition, we were told that this disparity in rank between the USNCB Director and executives at other federal law enforcement agencies may cause executives in other agencies to perceive that the USNCB is less important than an agency headed by a career SES employee. The structure may also affect those candidates who apply for the position. For example, the FBI official who was a representative to the INTERPOL Executive Committee said the leadership structure of the USNCB makes FBI employees reluctant to apply for the Director's position.

Strategic Planning and Alignment with DOJ Priorities

The USNCB has a strategic plan that covers fiscal years (FY) 2005 through 2010. However, although we found that the USNCB strategic plan includes some of the essential components of a standard strategic plan, such as strategic objectives, the plan lacks a comprehensive vision or a strategic direction for the USNCB.

In addition, the USNCB's current strategic plan does not clearly link to DOJ's overall strategic priorities. The USNCB's present functions most closely align with DOJ's Strategic Goal II to "prevent crime, enforce the federal laws, and represent the rights and interests of the American people." However, because transnational crime has been linked increasingly with terrorism and INTERPOL has expanded its role in sharing terrorism-related information, we believe the USNCB strategic plan should also address the relevant aspects of DOJ's Strategic Goal I to "prevent terrorism and promote the nation's security."

We believe the USNCB needs a comprehensive vision or a strategic direction that takes into account an expanding mission in sharing transnational criminal information and the increased importance of sharing terrorism-related information, as well as changes in technology and the global uses of information.

Senior USNCB officials agreed with the need for a more comprehensive strategic plan, but stated that they lack sufficient resources to develop it. However, we believe a formal strategic plan that addresses organizational and resource planning, management, and performance measurement is an important step that the USNCB should pursue.

Information Technology

The USNCB has struggled to adequately plan for information technology (IT) development. According to a 2004 Justice Management Division report, the USNCB's budget requests for FYs 2000 through 2004 failed to "make the case for how its IT enhancement request supported its own or DOJ's program goals."²³

We believe that the USNCB needs to anticipate its future IT needs by developing a formal, written requirements documents that addresses current and future IT needs.

Funding and Staffing

In FY 2009, the USNCB's overall budget was approximately \$24.5 million, of which \$8.2 million went to pay the United States' membership dues to INTERPOL. However, we found that several factors have impacted the USNCB's operational budget and the USNCB's ability to perform critical functions.

Specifically, as a result of a change in the formula used by INTERPOL to calculate each member country's dues, the U.S. commitment for INTERPOL dues (as a percentage of its overall budget) increased from \$1.7 million in FY 2001 to \$8.2 million in FY 2009.²⁴ In addition, INTERPOL requires that member countries pay their dues in euros. Since 2002, the dollar has generally declined in value relative to the euro, resulting in an effective increase in the United States' contribution to INTERPOL. As a result of the INTERPOL dues increases, the conversion from dollars to euros, and the decline in value between the dollar and euro, the USNCB's budget for operations, as a percentage of its total budget, has declined from 77 percent in FY 2001 to 67 percent in FY 2009.

The decline in its operational budget has resulted in the USNCB becoming more dependent on staff with specialized skills detailed from participating domestic agencies to assist with USNCB operations. However,

²³ U.S. Department of Justice, Justice Management Division, *Management Review of INTERPOL – USNCB August 2004 – Draft*, (2004) 12. Although labeled as a draft report, according to an official at the Justice Management Division, this is the final report.

²⁴ INTERPOL's operations are primarily financed by member-country annual statutory contributions. To assess each member country's dues contribution, INTERPOL uses a formula based on each country's economic well being. This formula was renegotiated in the late 1990s and incorporated a gradual increase in the percentage share paid by the wealthiest nations. The U.S. share of the annual INTERPOL budget increased from 5 percent in FY 2002 to 13.26 percent in FY 2006.

we found that the participating agencies do not provide detailees on a consistent basis and that number of staff and length of assignment vary widely. In addition, according to the USNCB Director, these agencies have not entered into agreements with the USNCB regarding staffing commitments. As a result, the USNCB is unable to ensure that it has a sufficient number of skilled staff to accomplish its mission. The USNCB Director said he believes that these federal agencies are reluctant to sign agreements because they are also facing budgetary restrictions and want to retain the flexibility to recall staff back to their agencies as needed. USNCB officials told us that they are working to establish formal agreements with federal law enforcement agencies regarding staff commitments and length of assignments.

Conclusion and Recommendations

We found weaknesses in how the USNCB shares INTERPOL information with U.S. law enforcement agencies, and we determined that the USNCB has not implemented procedures to ensure that the INTERPOL information it makes available to domestic law enforcement agencies is current, accurate, and timely. In addition, we identified a lack of participation in INTERPOL from some U.S. federal law enforcement agencies.

We also identified significant operational deficiencies in the USNCB's internal case management system, ENVOY, including problems with record retention and disposal, management reporting and statistics, and maintaining audit trails.

In addition, senior DOJ and DHS officials have not provided sufficient guidance and support to the USNCB. This has led to a lack of vision for the USNCB's role and mission. We believe that the USNCB needs such oversight and guidance to develop comprehensive strategic and IT plans.

Our audit work and findings resulted in 4 recommendations to the Department and 23 recommendations to the USNCB to assist the USNCB in improving its planning and operations, and to maximize the sharing of INTERPOL information among U.S. law enforcement agencies.

This page intentionally left blank.

THE UNITED STATES NATIONAL CENTRAL BUREAU OF INTERPOL

TABLE OF CONTENTS

| | |
|---|-----------|
| INTRODUCTION | 1 |
| INTERPOL – United States National Central Bureau | 3 |
| International Criminal Information Data Flow and Data Uses | 6 |
| Overview of Notices and Diffusions | 9 |
| Prior Reviews | 13 |
| Audit Approach..... | 14 |
| FINDINGS AND RECOMMENDATIONS..... | 16 |
| I. FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT COOPERATION AND PARTICIPATION | 16 |
| Federal Law Enforcement Agency Participation | 16 |
| State and Local Law Enforcement Coordination..... | 24 |
| Conclusion | 31 |
| Recommendations | 32 |
| II. EXCHANGE OF INTERPOL INFORMATION | 34 |
| Overview of the USNCB’s Information Sharing Processes | 34 |
| Information Not Shared with U.S. Law Enforcement Agencies..... | 36 |
| USNCB Processing of INTERPOL Information | 45 |
| INTERPOL Rules for Processing Information | 53 |
| INTERPOL Enhancements to Information Exchange Efforts | 54 |
| USNCB Quality Assurance Efforts | 57 |
| Conclusion | 59 |
| Recommendations | 60 |
| III. CONTROLS OVER USNCB CASE INFORMATION | 62 |
| USNCB Internal Case Management | 62 |
| Records Management | 66 |
| New Electronic Case Management System | 71 |
| Conclusion | 72 |
| Recommendations | 73 |

| | |
|---|------------|
| IV. USNCB MISSION AND PRIORITIES | 74 |
| Strategic Needs of the USNCB | 74 |
| Conclusion | 83 |
| Recommendations | 83 |
| APPENDIX I - AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY | 85 |
| APPENDIX II - STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS | 93 |
| APPENDIX III - STATEMENT ON INTERNAL CONTROLS..... | 94 |
| APPENDIX IV - INTERPOL MEMBER COUNTRIES | 95 |
| APPENDIX V - USNCB STATE & LOCAL LIAISONS..... | 98 |
| APPENDIX VI - USNCB QUESTIONNAIRE AND RESPONSES..... | 100 |
| APPENDIX VII - INTERPOL NOTICES | 111 |
| APPENDIX VIII - DATABASES USED IN DOMESTIC INTERNATIONAL CRIMINAL INFORMATION SHARING | 115 |
| APPENDIX IX - UNITED STATES NATIONAL CENTRAL BUREAU RESPONSE | 117 |
| APPENDIX X - DEPARTMENT OF JUSTICE RESPONSE | 129 |
| APPENDIX XI - OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND ACTIONS NECESSARY TO CLOSE THE REPORT | 132 |

INTRODUCTION

The International Criminal Police Organization (INTERPOL) is a worldwide network that facilitates the exchange of information to assist law enforcement agencies to detect and deter international crime and terrorism.²⁵ As of May 2009, 187 countries participated in INTERPOL.

Overview of INTERPOL

Established in 1923 and currently located in Lyon, France, INTERPOL is an international police organization that seeks to facilitate cross-border police cooperation and support and to assist all organizations whose mission is to prevent or combat international crime. INTERPOL provides secure global police communication services, operational police support services, and police training and development.

INTERPOL is funded primarily by member country annual statutory contributions. To assess each member countries' dues contribution, INTERPOL uses a formula based on the countries' economic well being. This formula was renegotiated in the late 1990s and incorporated a gradual increase in the percentage share paid by the wealthiest nations. The United States' share of the annual INTERPOL budget increased from 5 percent to 13.26 percent over 4 years, reaching the full negotiated dues contribution rate of 13.26 percent in Fiscal Year (FY) 2006. In 2009 INTERPOL's total statutory budget was approximately \$64.1 million and the United States' contribution to INTERPOL was \$8.2 million.

In FY 2008, INTERPOL had a staff of 588, representing 84 countries. In addition to 398 contract employees, INTERPOL also had 190 seconded staff from member countries.²⁶ As of May 2009, the United States had seven individuals detailed to the INTERPOL General Secretariat.

INTERPOL is governed by its General Assembly, which consists of delegates appointed by member countries. The General Assembly meets

²⁵ Article 3 of the INTERPOL constitution prohibits member countries from intervening in or investigating matters considered to be racial, military, political, or religious in nature. Until 1984, INTERPOL interpreted this article as excluding most acts of terrorism from its jurisdiction. At its 1984 general assembly meeting, the INTERPOL membership categorized international terrorist acts as law enforcement matters not covered by Article 3. This allowed INTERPOL member countries to exchange information and provide assistance to combat terrorism.

²⁶ Seconded staff are individuals who are temporarily assigned to INTERPOL by their national administrations and compensated by their national administrations or by INTERPOL.

once a year to make all major decisions affecting general policy.²⁷ The Executive Committee oversees the execution of the decisions of the General Assembly, as well as the work of the Secretary General.²⁸ The Secretary General is responsible for overseeing INTERPOL's day-to-day work of international police cooperation.²⁹ INTERPOL has seven sub-regional bureaus, which are located in Abidjan, Côte d'Ivoire (West Africa); Buenos Aires, Argentina (South America); Harare, Zimbabwe (Southern Africa); Nairobi, Kenya (East Africa); San Salvador, El Salvador (Central America); and Yaoundé, Cameroon. In addition, there are liaison offices in Bangkok, Thailand, the World Health Organization, Europol, and the United Nations in New York.³⁰

Each member country of INTERPOL establishes a National Central Bureau (NCB) to serve as its liaison between the member country's law enforcement agencies and INTERPOL. NCB's transmit, respond to, and execute requests for information and assistance in criminal investigations and police matters to and from other countries' NCBs via the INTERPOL communications network. "Advisers" are experts in a purely advisory capacity, who may be appointed by the Executive Committee and confirmed by the General Assembly. An overview of INTERPOL's organizational structure is found in Exhibit 1-1.

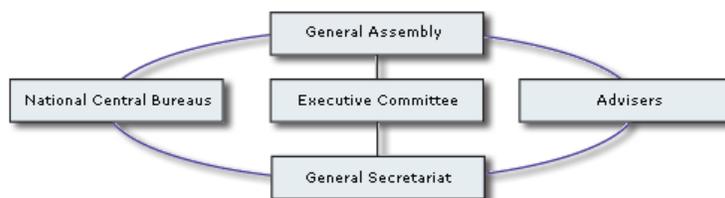
²⁷ Each country has one vote.

²⁸ The INTERPOL Executive Committee has 13 members elected by the General Assembly. Currently, a senior Federal Bureau of Investigation (FBI) official – although retired from the FBI – serves as the representative to the Executive Committee for the Americas. This position expires in October 2009, and elections to fill this position will be held by INTERPOL at the next meeting of the General Assembly.

²⁹ The Secretary General is nominated by the Executive Committee, approved by the General Assembly, and serves a 5-year term. Ronald K. Noble, the current Secretary General, was initially elected in 2000 and currently is serving a second term. Secretary Noble is a national of the United States and served as a former Undersecretary for Enforcement with the U.S. Department of Treasury.

³⁰ The World Health Organization is the directing and coordinating authority for health matters within the United Nations system. The European Police Office (Europol) was set up to help the law enforcement services of the European Union (EU) combat serious organized crime that affects two or more EU countries.

EXHIBIT 1-1
INTERPOL Organizational Structure



Source: INTERPOL

United States National Central Bureau of INTERPOL

The United States National Central Bureau (USNCB) is the entity through which the United States functions as a member of INTERPOL. Located in Washington, D.C., the USNCB is co-managed by DOJ and the Department of Homeland Security (DHS).³¹ The USNCB’s mission is to facilitate international law enforcement cooperation by acting as the U.S. representative to INTERPOL. The USNCB receives and disseminates law enforcement-related information between other INTERPOL NCBs and U.S. law enforcement agencies, responds to requests for information or assistance by law enforcement agencies and other entities that coordinate with INTERPOL, and coordinates information for investigations of an international nature.

The responsibility for management of the USNCB has varied since the USNCB became operational in 1968. It initially was placed under the direction of the Department of the Treasury (Treasury). In 1977, the Department of Justice (DOJ) and Treasury signed a Memorandum of Understanding (MOU) that established joint DOJ and Treasury management of the USNCB. In 1981, an amendment to the MOU placed the USNCB within DOJ, reporting to the Deputy Attorney General, but still under the co-

³¹ In 1938, Congress designated the FBI as the official U.S. representative to INTERPOL. During World War II, INTERPOL’s activities were disrupted. The United States rejoined the organization and became an official member in 1947. The USNCB was created in 1968 under the direction of the U.S. Department of the Treasury (Treasury). In 1977, Treasury and the U.S. Department of Justice (DOJ) signed a Memorandum of Understanding (MOU) to establish joint management of the USNCB. A subsequent amendment to the MOU signed in 1981 placed the USNCB within DOJ, reporting to the Deputy Attorney General, under the co-management of Treasury and DOJ. Following the creation of DHS, DOJ and DHS signed an MOU in May 2003 that established the USNCB as a separate component of DOJ under the supervision of the Deputy Attorney General. DOJ is responsible for the administrative costs of operating the USNCB.

management of Treasury and DOJ. A May 2003 MOU transferred responsibility for the management of the USNCB to DOJ and the Department of Homeland Security (DHS).³²

Budget and Staffing

The USNCB's FY 2009 budget is approximately \$24.5 million. Approximately one third of the USNCB's total budget goes to pay INTERPOL dues. For 2009, the U.S. commitment for INTERPOL dues was almost \$8.2 million.

The USNCB has an authorized staffing level of 65 permanent, full-time equivalent positions. The USNCB is also heavily dependent upon staff detailed from participating agencies. The detailees serve as their home agencies' liaisons and provide valuable agency-specific expertise. As of December 2008, the USNCB staff was supplemented by 24 detailed employees from other federal agencies, including DOJ's United States Marshals Service (USMS) and DHS's Immigration and Customs Enforcement (ICE), as well as one local agency.³³

Organizational Structure

The USNCB is co-managed by DOJ and DHS, with two senior management positions – the Director and Deputy Director – rotating between DOJ and DHS every 3 years.³⁴ As a result, the USNCB Director must be from a different department than his or her predecessor and the Deputy Director. For example, if the Director is from a DOJ agency, then the Deputy Director must be from a DHS agency.

As shown in Exhibit 1-2, the USNCB is divided into five operational divisions and a command center, which are responsible for handling domestic and foreign requests for assistance. These requests generally involve the location and arrest of known fugitives and criminals, criminal record checks on subjects of interest to law enforcement and applicants for various types of licenses and employment that involve a public security or

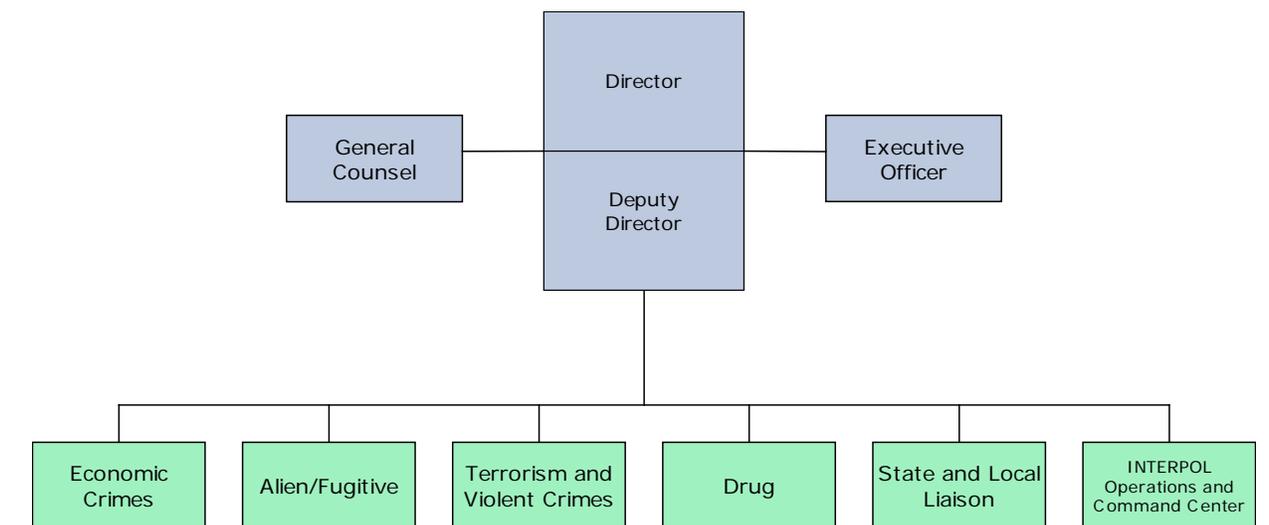
³² DOJ is responsible for the administrative costs of operating the USNCB, with the exception of costs associated with detailed employees and their travel.

³³ As of December 2008, the White Plains, New York, Police Department had one person detailed to the USNCB. It was the only non-federal agency with a USNCB detailee.

³⁴ The Director and Deputy Director serve a term of at least 2 years, but not more than 3 years. The current Director is a Supervisory Special Agent with DHS's U.S. Immigration and Customs Enforcement, and the Deputy Director is a Chief Inspector with DOJ's U.S. Marshals Service.

safety nexus, as well as requests to obtain evidence or conduct interviews for judicial and law enforcement purposes.

EXHIBIT 1-2
USNCB Organizational Structure



Source: USNCB

The Economic Crimes, Alien/Fugitive, Terrorism and Violent Crimes, and Drug divisions focus on specific crime areas and are staffed primarily by USNCB analysts and law enforcement agents with subject matter expertise temporarily detailed to the USNCB from DOJ, DHS, and other federal, state, and local agencies.

The State and Local Liaison Division performs coordination and outreach to state and local law enforcement agencies and oversees the INTERPOL State and Local Police Liaison Program, which consists of an INTERPOL liaison office in each state, U.S. territory, and an increasing number of major cities in the United States.³⁵ The Division conducts training for U.S. state and local officials on international investigative assistance and new developments in international law enforcement.

The USNCB's INTERPOL Operations and Command Center (IOCC) coordinates the receipt and dissemination of correspondence from foreign NCBs, the INTERPOL General Secretariat, and domestic law enforcement agencies. The IOCC operates 24 hours a day, 7 days a week.

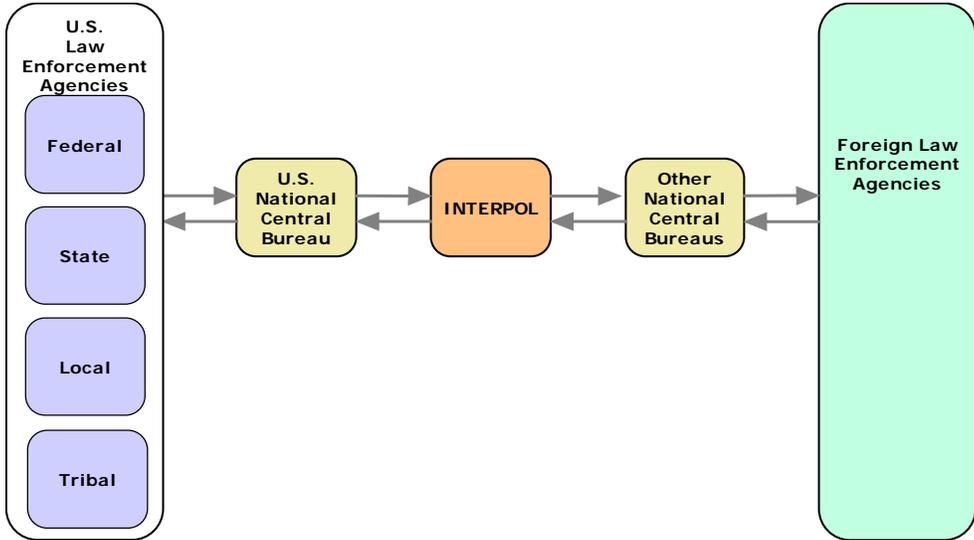
³⁵ See Appendix V for a complete list of the USNCB state and local liaison offices.

International Criminal Information Data Flow and Data Uses

INTERPOL has developed a secure, Internet-based, virtual private network known as I-24/7 that serves as the conduit for INTERPOL-related communications. Through I-24/7, INTERPOL provides its 187 member countries with direct access to a wide range of criminal information contained in a variety of databases managed by INTERPOL. The information in the databases comes from queries, messages, intelligence, and submissions from law enforcement officials in member countries. Member countries also use I-24/7 to request assistance with locating wanted, missing, or lost individuals.

As shown in Exhibit 1-3, INTERPOL’s data flow is a two-way process. Data flows from domestic law enforcement agencies to international partners and from international partners to domestic law enforcement agencies.

EXHIBIT 1-3
Overview of the INTERPOL Data Flow Process



Source: OIG depiction of information obtained from the USNCB

According to INTERPOL, member countries use INTERPOL’s databases to share international criminal- and terrorism-related information for use in investigations and to request assistance in locating fugitives, witnesses, and missing or lost persons, including parental abduction cases and missing children. In addition, member countries use INTERPOL databases to collect additional information about a person’s identity or activities in relation to a crime or to provide information on career criminals who have committed, or are likely to commit, offenses in several countries, such as child molesters.

Finally, the databases assist member countries to identify dead bodies, and recover lost and stolen property, such as vehicles and art.

Exhibit 1-4 contains summary descriptions for each of the INTERPOL databases.

EXHIBIT 1-4
INTERPOL Databases as of February 2009

| Database | Description |
|---|---|
| Nominal data | Information about known international criminals, missing persons, and unidentified bodies; includes criminal history, photographs, and fingerprints. |
| Notices | INTERPOL uses a system of notices to alert police to fugitives, suspected terrorists, dangerous criminals, missing persons or weapons threats. |
| Stolen and Lost Travel Documents (SLTD) | The SLTD database contains information on more than 16.7 million travel documents reported lost or stolen by 145 countries and is used to determine the validity of a suspect travel document. |
| Stolen Motor Vehicles | This system contains identification details on approximately 4.7 million vehicles reported stolen around the world. |
| DNA Profiles | This system contains 83,000 DNA profiles from 48 countries, that can be used to make person-to-person, person-to-scene, or scene-to-scene matches with no previous connections, or help identify missing persons and unidentified bodies. To preserve privacy, the records do not contain nominal information such as names, and member countries control their own data. |
| Fingerprints | INTERPOL's automated fingerprint identification database contains 86,000 fingerprints and 1,800 crime scene marks. |
| Stolen Works of Art | This database includes information on more than 33,000 pieces of artwork and cultural heritage reported stolen worldwide. |
| INTERPOL Child Abuse Image Database (ICAID) | The ICAID system contains more than 550,000 child abuse images submitted by member countries. ³⁶ |
| Fusion Task Force | Created in September 2002, this database contains information about over 13,000 known or suspected terrorists from 120 countries. Approximately 120 countries contribute. |
| Stolen Administrative Documents | This database contains information on almost 190,000 official documents that identify objects, such as vehicle registration documents and clearance certificates for import or export. |
| Counterfeit Payment Cards | Implemented in 2000, this database contains images of counterfeit payment cards and corresponding data. Seized cards are categorized and form a standard reference library against which suspect cards can be checked. |

Source: INTERPOL

³⁶ The INTERPOL Child Abuse Image Database information is strictly controlled by INTERPOL and may only be accessed by law enforcement personnel once permission is granted by INTERPOL.

Overview of Notices and Diffusions³⁷

INTERPOL utilizes a system of color-coded international notices and diffusions to share critical crime-related information with the 187 member countries.³⁸ Generally, notices and diffusions provide information on individuals wanted for serious crimes, missing persons, unidentified bodies, possible threats, and criminals' modus operandi.³⁹ As of February 2009, INTERPOL had nearly 25,000 active notices, of which most were red. The color signifies the purpose of the notice, as noted below.

Red Notice – These messages provide information about and request searches for the location and arrest of subjects for whom an arrest warrant has been issued and where extradition will be requested. For example, the United States may issue a Red Notice if a case meets all of the following criteria: (1) a crime has been committed; (2) an arrest warrant has been issued; (3) there is reason to believe the subject has fled the United States; and (4) the responsible prosecutor having jurisdiction in the matter confirms that extradition will be sought.

Blue Notice – These messages seek to obtain information about, locate, or identify a person of interest in a criminal investigation.

Green Notice – These messages provide warnings about criminals who have committed, or are likely to commit, offenses in several countries, such as habitual offenders, child molesters, and pornographers.⁴⁰

³⁷ At the meeting of the INTERPOL General Assembly in October 2008, the member countries adopted a new framework for the issuance of notices, including revised criteria for the issuance of a Green, Orange, and Purple Notices. (A Purple Notice provides information on methods, objects, and hiding places used by criminals.). See Appendix VII for the new definitions and criteria.

³⁸ A diffusion is a message sent by a member country to one or more member countries without the formal review conducted by INTERPOL. Frequently, the diffusion message is sent to immediately disseminate information pending submission and approval of the more formal notice. A diffusion message contains information similar to a notice, but member countries also use diffusions to request assistance. After 1 year, one of three actions must occur on all diffusions: (1) a notice must be issued for the subject; (2) a message must be sent to INTERPOL confirming the wanted status of the subject; or (3) the diffusion must be cancelled.

³⁹ Notices are published in all of the organization's working languages: Arabic, English, French, and Spanish.

⁴⁰ According to the USNCB General Counsel, prior to the adoption of the new criteria in October 2008 many of the member countries were reluctant to issue Green Notices because of confusion over the requirements for issuance and privacy concerns.

Yellow Notice – These messages provide information to help locate missing persons, especially minors, or to help identify persons who are not able to identify themselves.

Black Notice – These messages provide information about unidentified bodies or deceased persons and request assistance in obtaining the correct identification.

Orange Notice – These messages provide information and warn police, public entities, and other international organizations of dangerous materials, criminal acts, or events that pose a potential threat to public safety.

INTERPOL-United Nations (U.N.) Security Council Special Notice – These notices are issued by INTERPOL on behalf of the United Nations Security Council to alert police of groups and individuals who are the targets of U.N. sanctions against Al Qaeda and the Taliban.

The INTERPOL General Secretariat, NCBs, and international organizations and entities with which INTERPOL have special agreements can apply for the issuance of a notice.⁴¹ For example, when U.S. officials suspect that a fugitive has fled the country, they may request that a Red Notice regarding the fugitive be issued internationally to all NCBs.

These notices contain two basic types of information – identity and judicial. Information pertaining to an individual's identity can include name, date of birth, physical description, photograph, fingerprints, occupation, languages spoken, and identity document numbers. Judicial information can include the offense with which the person is charged, references to the laws under which the charge is made or conviction was obtained, the maximum penalty that has been or can be imposed and, in the case of the Red Notice, references to the arrest warrant or sentence imposed by a court and details about the conditions under which the requesting country will request extradition from other countries.

As shown in Exhibit 1-5, the notice process generally begins with a request from a domestic or foreign law enforcement agency. The request is forwarded to the source law enforcement agency's NCB for review and submission to the INTERPOL General Secretariat in Lyon, France, for additional review and approval.

⁴¹ The General Secretariat is the entity that performs INTERPOL's administrative and operational functions. The Secretary General is the individual who directs the staff, administers the budget, and organizes and directs the permanent departments.

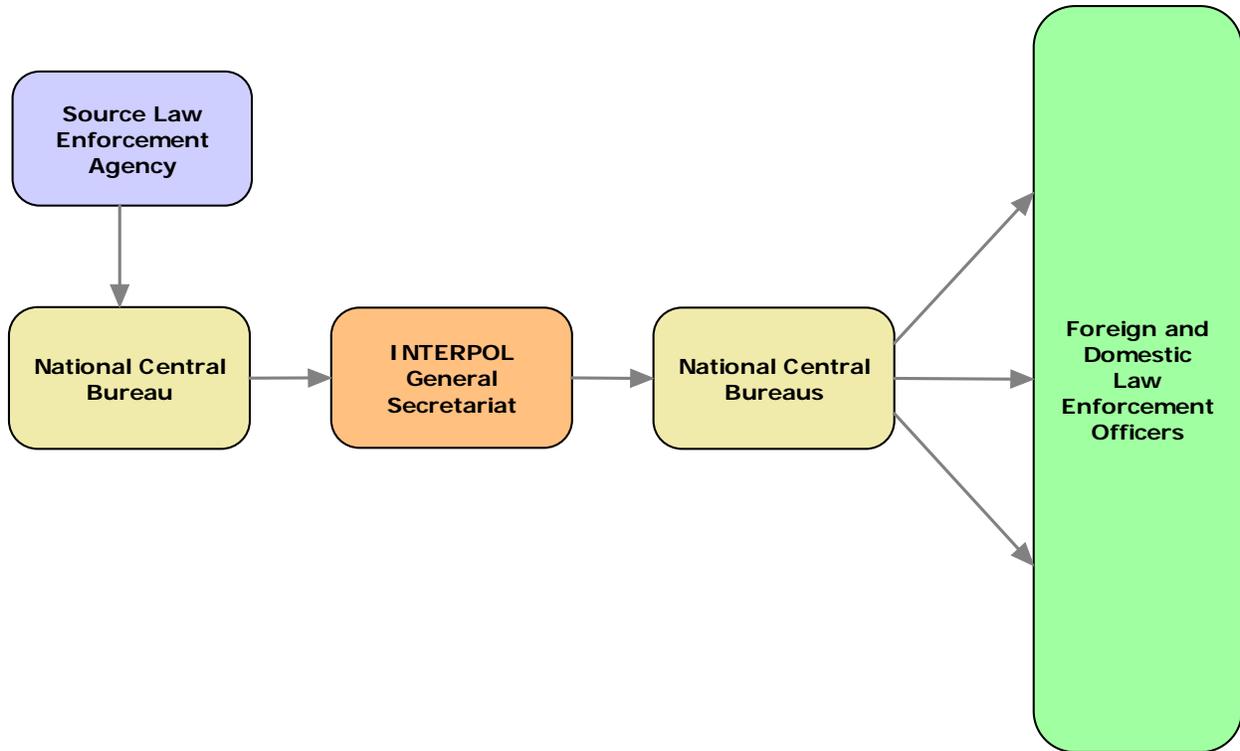
According to INTERPOL, all applications for notices should be reviewed by the originating member country for accuracy, completeness, legal sufficiency, and compliance with INTERPOL regulations. However, this review is especially important for applications for a Red Notice. All Red Notice applications also receive a quality assurance review by INTERPOL staff members to ensure that the Red Notice application is not based on a prohibited matter, including acts of a racial, military, political, or religious nature. According to the USNCB General Counsel, this review is essential because for approximately one-third of the member countries a Red Notice serves as a provisional arrest warrant.⁴²

Following the review by INTERPOL, the notices are distributed to the member country NCBs.⁴³ Upon receipt of the notices, each member country NCB can distribute the information to its law enforcement officers.

⁴² The United States does not recognize the Red Notice as an official arrest warrant. If the subject of another member country's Red Notice is located in the United States, federal officials will notify the member country of the individual's possible location. Once the foreign country provides sufficient documentation, a provisional arrest warrant is issued, the subject of the Red Notice is detained, and extradition through diplomatic channels is arranged.

⁴³ Each member country may restrict another member country's access to its information.

EXHIBIT 1-5
Overview of the INTERPOL Notice Process



Source: OIG depiction of information obtained from the USNCB

request that notices be removed for a variety of reasons, including location of the missing person, apprehension of a fugitive, identification of a body, or if a fugitive is no longer wanted. Member countries regularly receive notifications from INTERPOL that list the cancelled notices. Similarly, as additional information is obtained that enhances or modifies the notice, INTERPOL issues an addendum.

As shown in Exhibit 1-6, the United States accounts for 20 percent of all active INTERPOL notices.

⁴⁴ INTERPOL policies require that each notice be reviewed every 5 years to ensure that the notice is still accurate and, in the case of the Red Notice, that the warrant is valid and extradition will be pursued.

EXHIBIT 1-6
Active INTERPOL Notices
(as of February 28, 2009)

| Type | INTERPOL | United States | Attributable to the United States (by type) |
|-----------------------------|---------------|---------------|---|
| Red – Wanted Persons | 15,836 | 1,798 | 11% |
| Blue – Trace/locate | 2,074 | 167 | 8% |
| Green – Career Criminals | 3,389 | 2,524 | 74% |
| Yellow – Missing Persons | 2,127 | 299 | 14% |
| Black – Unidentified Bodies | 861 | 38 | 4% |
| Orange – Warning | 48 | 8 | 17% |
| U.N. Special | 333 | -- | -- |
| Total | 24,668 | 4,834 | 20% |

Source: INTERPOL and the USNCB

Prior Reviews

DOJ and the Government Accountability Office (GAO) previously reviewed various programs that relate to USNCB and INTERPOL operations.⁴⁵ In July 2006, the GAO issued a report on the border security and Visa Waiver Program.⁴⁶ The report identified INTERPOL's Stolen and Lost Travel Documents (SLTD) database as a means through which DHS was attempting to mitigate the risks of the Visa Waiver Program.⁴⁷ The GAO recommended that the DHS Secretary, along with appropriate agencies, require all visa waiver countries to provide the United States and INTERPOL with non-biographical data from lost, stolen, or blank passports. The GAO also recommended that DHS develop a plan to make INTERPOL's lost or stolen travel document database automatically accessible to border personnel at U.S. ports of entry.

⁴⁵ The USNCB was the subject of several reviews conducted by DOJ and the GAO in 1986, 1987, and 1993. However, given the length of time since these reviews were performed and the significant changes in the environment and technology over the last two decades, we considered these reviews only for historical content.

⁴⁶ U.S. Government Accountability Office, *Border Security Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program*, GAO-06-854 (July 2006).

⁴⁷ The Visa Waiver Program was created to facilitate international travel and is a substitute entry mechanism for non-immigrant, short-term, business, and tourism visas only; it does not apply to students, temporary workers, and others who require visas to enter the United States.

In August 2004, DOJ's Justice Management Division (JMD) conducted a review of the USNCB's organizational structure, role, and mission to identify potential management and operational improvements.⁴⁸ JMD recommended changes to the USNCB's organizational structure and procedures to improve its administrative capability, strengthen career advancement for its employees, maximize detailee value to the USNCB by instituting minimum tours of duty, and improve its maintenance of case files. Further, JMD recommended moving funds for INTERPOL dues into an account separate from operational funds. According to the USNCB Director, while the USNCB began implementing changes as a result of the JMD review, several of the matters raised by JMD, such as case management and the budgeting for INTERPOL dues, have not been fully addressed. We discuss these issues in our report.

OIG Audit Approach

The objectives of this audit were to: (1) evaluate the USNCB's efforts to ensure the sharing of INTERPOL information among federal, state, local, and tribal law enforcement agencies; (2) review the USNCB's processes for the exchange of INTERPOL information to ensure that requests for assistance and information were handled in an appropriate, efficient, and timely manner; (3) review the USNCB's controls over INTERPOL case information; and (4) examine the USNCB's organizational role and strategic priorities to ensure that they are in line with DOJ priorities.

To accomplish these objectives, we conducted more than 60 interviews of USNCB officials and participating agency representatives, including the Director, Deputy Director, and Assistant Directors of the USNCB. We also attended a training session presented by the USNCB for state, local, and tribal liaisons to understand its working relationships, the assistance it provides, and its communication with local offices. In addition, we interviewed officials in the Office of the Deputy Attorney General, Federal Bureau of Investigation (FBI), and Drug Enforcement Administration (DEA). We also interviewed the INTERPOL Secretary General, officials at the INTERPOL General Secretariat in Lyon, France, and law enforcement officials from the Bundeskriminalamt (BKA) located in Wiesbaden, Germany.⁴⁹

⁴⁸ U.S. Department of Justice, Justice Management Division, *Management Review of INTERPOL – USNCB August 2004 – Draft*, (2004). Although labeled as a draft report, according to an official at the Justice Management Division, this is the final report.

⁴⁹ The BKA is the German national police force. Among its other duties, it functions as the National Central Bureau for Germany.

Findings I through IV present an overview of our audit results. In Finding I, we attempted to evaluate the level of cooperation and participation between the USNCB and its partner agencies. We also checked whether information about high-profile U.S. fugitive criminals and terrorists had been shared with foreign counterparts through the red notice system. In addition, we distributed a questionnaire to all 66 state and local USNCB liaison offices to assess the level of cooperation and satisfaction among the USNCB partners.

Finding II focuses on the USNCB's efforts and ability to accurately integrate and maintain data from a variety of countries. In addition, we reviewed the USNCB's efforts to ensure that domestic law enforcement agencies have access to INTERPOL databases. We also reviewed the USNCB's efforts to ensure INTERPOL information is being made available to U.S. agencies and placed in U.S. agency databases in an accurate, current, and timely manner.

Finding III focuses on the USNCB's internal case management, including its efforts to utilize INTERPOL information to enhance U.S. investigations. In addition, we assessed the USNCB's capability to identify potential patterns and evolving trends in criminal activities, such as transnational organized crime.

Finding IV examines the USNCB's role, mission, and organizational structure. We also assessed the USNCB's ability to adequately address its strategic needs.

The audit scope and methodology are presented in Appendix I.

FINDINGS AND RECOMMENDATIONS

I. FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT COOPERATION AND PARTICIPATION

The USNCB's relationships with and the level of participation provided by U.S. law enforcement agencies are key elements to the USNCB's effectiveness in carrying out its mission. However, federal law enforcement agencies do not fully participate in INTERPOL's red notice program to apprehend fugitives. In addition, we found that poor communication between the USNCB and federal law enforcement agencies leads to incomplete information being shared with the international law enforcement community. Further, the USNCB has not adequately maintained communication channels for interacting with its state and local liaisons. As a result, there is a risk that critical law enforcement information or requests for assistance are not reaching the intended recipients.

Federal Law Enforcement Agency Participation

The United States' participation in INTERPOL depends on the USNCB's coordination with U.S. law enforcement agencies. However, some federal law enforcement agencies do not fully participate in INTERPOL's red notice program. Moreover, the USNCB is often not informed of actions taken by its federal domestic law enforcement partners on INTERPOL-related cases and as a result the USNCB is hindered in its coordination with other member countries. Further, the United States does not contribute information to INTERPOL's stolen motor vehicle database.

Red Notice Program

According to INTERPOL, as of December 31, 2008, among INTERPOL member countries the United States had the highest number of active red notices seeking the location and arrest of a wanted person with a view to extradition based on an arrest warrant or court decision. However, not every federal law enforcement agency fully participates in the red notice program.

We reviewed the public websites of the DEA, FBI, and ICE to determine if their most wanted fugitives had red notices issued through INTERPOL. As shown in Exhibit 2-1, we found that 14 of these 32 "most wanted" criminals (44 percent) did not have red notices issued. A red notice

provides wide distribution of information about wanted criminals to all INTERPOL member countries. By not using this program, U.S. law enforcement fails to take advantage of a relatively easy method of communicating this information to the widest possible audience, which can increase the opportunity to locate and apprehend the criminal or obtain related intelligence.

**EXHIBIT 2-1
DEA, FBI, and ICE Fugitives**

| Component | Number of Fugitives | Number without a Red Notice |
|--------------------------------|----------------------------|------------------------------------|
| DEA – International Fugitives | 14 | 6 |
| FBI – 10 Most Wanted Fugitives | 10 | 3 |
| ICE – International Fugitives | 8 | 5 |
| Total | 32 | 14 |

Source: As listed by each component on its public website

We discussed this issue with the USNCB Director, who is also a DHS ICE employee. He attributed ICE’s failure to pursue red notices in these instances to insufficient numbers of experienced personnel being detailed from DHS to the USNCB. The USNCB Director stated that prior to the creation of DHS, two staff with experience in customs and two other staff with experience in immigration matters were detailed to the USNCB. However, after the creation of DHS, the agency detailed just one or two employees to the USNCB to handle cases involving both customs and immigration issues. The USNCB Director stated that he believed that the workload related to immigration issues was too large for one person to effectively manage and ensure that ICE pursued red notices.

We also discussed this issue with the FBI Assistant Director (since retired) for International Operations, who is also a delegate to the INTERPOL Executive Committee. He agreed that all of the FBI’s 10 Most Wanted Fugitives should have red notices issued. He was unable to explain the FBI’s failure to pursue red notices in these cases because the FBI has directed its agents to issue INTERPOL notices for all outstanding FBI fugitives believed to be in a foreign country. Moreover, he said that the FBI special agent in charge of the case or the FBI representative at the USNCB should be responsible for publishing the notice. He also acknowledged that the FBI is not utilizing the USNCB and INTERPOL as it should and said he is trying to educate FBI agents on how to utilize USNCB and INTERPOL resources more fully.

In addition, we discussed this issue with the Assistant Director for the USNCB Drug Division, a DEA employee, who stated that she was working to improve the DEA's participation in the INTERPOL notice program. She identified the six DEA divisions that had the lowest red notice activity and said that she wants to train the divisions on the uses of INTERPOL, especially on preparing red notice requests. However, when we spoke with a DEA headquarters official about this issue, he stated that the DEA frequently does not issue INTERPOL notices because of the sensitivity of its drug cases and concerns regarding security of the information. This DEA official also stated that some countries in which the DEA has sensitive cases experience high levels of public corruption, and as a result, the DEA may not want to publish a red notice that can be used by a corrupt law enforcement official to inform criminals that the DEA is investigating them.

Both FBI and DEA officials stated that their agencies have many agents working abroad that share information about sensitive cases directly with their law enforcement counterparts within foreign governments. Consequently, the FBI and DEA agents can control the use and distribution of information rather than use INTERPOL to share information.

While we understand the FBI's and DEA's need to control the use and dissemination of highly sensitive, non-public information, the fugitives that we reviewed were listed on the FBI, DEA, and ICE public websites accessible to anyone with a computer and Internet connection. Information related to these types of cases should be shared with appropriate foreign counterparts through the INTERPOL network because it can allow U.S. law enforcement agencies to reach places where they do not have a physical presence and increase the likelihood that fugitives are captured.

Officials at both the FBI and DEA told us that they are working to improve their agency's participation in INTERPOL and provide additional training for their agents regarding the INTERPOL program. We believe it is essential that domestic law enforcement agencies receive information and training regarding the uses and benefits of the INTERPOL network and coordination with the USNCB.

We discussed the underutilization of the red notice program with USNCB officials. They believed that the USNCB's current paper-based process that domestic agencies use to apply for a notice is time-consuming, inefficient, and may have contributed to agencies' lack of participation. USNCB officials suggested that adopting an on-line process for submitting notice applications and diffusion requests could improve the use of the INTERPOL network.

The USNCB General Counsel said that the FBI had developed an internal, on-line application for its agents to use when submitting a notice application to the USNCB. However, he stated that he doubted the USNCB has sufficient current resources to develop such a capability. We agree that an electronic, on-line procedure would streamline the notice application process and make it easier for all domestic law enforcement agents to use the INTERPOL notice program, and we believe that the USNCB and the Department should make this a priority to implement.

In addition, we recommend that DOJ, the USNCB, and the USNCB Executive Committee should consider pursuing formal agreements with federal law enforcement agencies to clarify the extent and type of case information that should be shared with the USNCB and INTERPOL.

Case Resolution Information

We found that the USNCB cannot adequately coordinate the sharing of case-related information because it is often not informed of actions taken by its U.S. law enforcement partners on INTERPOL-related cases. For example, we identified a February 2005 wanted person diffusion issued by another country's NCB for an individual wanted for homicide and attempted homicide. During our review of the USNCB case file, we noted that the USNCB had identified that the subject of the notice had potentially entered the United States on numerous occasions. In January 2008 the USNCB informed the other NCB that the subject was attempting to re-enter the United States and was being detained by DHS. The other NCB responded that the foreign arrest warrant remained in force and that the subject would be extradited. The final document in the USNCB case file contained a communication from the other NCB inquiring why the subject was not detained for extradition.

Because the case file did not contain a USNCB communication indicating that it had responded to the other NCB, we asked the USNCB to review the case and provide us with an explanation. The USNCB responded that a USNCB detailee had contacted DHS and determined that the subject was permitted to enter the United States. However, the Deputy did not document in the USNCB case file his discussion with DHS.

While reviewing the case in response to our request, the USNCB also learned that another DOJ agency had previously opened a case related to this same individual and that an extradition package had been received through diplomatic channels. However, the extradition package did not meet DOJ criteria because the package did not contain a photograph of the subject. In 2007, DOJ informed the State Department that the case would

be closed. The USNCB reviewed the other agency's case file and found that the agency may have reopened its case in September 2008. In addition, the USNCB determined that the investigator had attempted to locate this subject within the United States. However, the investigator closed the investigation in December 2008.

Without our review and inquiry, the USNCB would not have known about the actions being taken by the other DOJ agency regarding the subject of the INTERPOL wanted person diffusion. Further, while the other agency's case file indicated that the foreign government's application for extradition was closed because it did not contain a photograph of the subject, we identified a photograph of the subject in the USNCB's case files. As a result of this lack of communication and coordination, an individual wanted by a foreign government for homicide and attempted homicide was allowed to evade prosecution for these crimes.

We discussed this issue with officials at other DOJ agencies, such as the FBI and DEA. Although the FBI and DEA officials said that their agency works closely with the USNCB, they also said that their agencies often bypass the USNCB and deal directly with their foreign counterparts or through diplomatic channels when they need information about a particular case with an international nexus. According to a USNCB official, this lack of communication with the USNCB significantly impacts the USNCB's ability to coordinate the exchange of information and the United States' response to inquiries from domestic and foreign law enforcement agencies. Additionally, while this flow of information directly between agencies may meet the immediate needs of the agencies involved, the information passed remains "stovepiped" within these agencies instead of being shared with other law enforcement entities that also may have a need for it. Moreover, the USNCB is not informed about the final outcome of INTERPOL investigations, and it thus cannot accurately measure the impact of its efforts, rate its performance, and compile meaningful management statistics.

We met in September 2008 with the official in the Office of the Deputy Attorney General (ODAG) who serves as the DOJ official responsible for USNCB matters. We discussed the challenges the USNCB faces in its attempts to effectively communicate and coordinate with domestic and international law enforcement agencies. The ODAG official stated that the USNCB serves as a valuable partner with domestic law enforcement agencies to share INTERPOL information on international criminals, and he acknowledged that domestic law enforcement agencies needed to increase their use of and participation in the USNCB. He also said that there is a lack of awareness among law enforcement agencies about the mission of the USNCB and that training and outreach to these agencies would be

worthwhile. The ODAG official stated that it makes sense to keep USNCB oversight with the ODAG, but that it might be worth considering having the day-to-day operations more closely aligned with the Department's Criminal Division or the OIA.

We believe that DOJ, the USNCB, and the USNCB Executive Committee should work to establish formal agreements between federal law enforcement agencies that describe the type of case information these agencies will share with foreign counterparts through the INTERPOL network.

Stolen Motor Vehicles

INTERPOL has developed a stolen motor vehicle (SMV) database to support efforts in member countries to combat international vehicle theft and trafficking. According to INTERPOL records, the SMV database contains approximately 4.6 million records of reported stolen motor vehicles. At the end of 2008, approximately 158 countries used the database regularly, 122 of which share their national stolen vehicle database records with INTERPOL. As a result of searches of the SMV database, more than 31,000 stolen motor vehicles were recovered worldwide in 2008. However, INTERPOL officials stated that as of August 2008 the United States had entered just five vehicles into the SMV database.

When we discussed these issues with USNCB officials, they were aware that the United States did not provide INTERPOL with information about motor vehicles stolen in the United States. The FBI maintains information in the National Crime Information Center's (NCIC) Vehicle File about stolen U.S. motor vehicles and determines what information will be shared and with whom in accordance with 28 U.S.C § 534.⁵⁰ According to the USNCB, rather than including the NCIC information in the INTERPOL database, the FBI provides certain countries with the ability to directly search NCIC's Vehicle File. Currently, only a limited number of INTERPOL member countries have the ability to search NCIC for information on vehicles reported stolen in the United States.

⁵⁰ The National Crime Information Center (NCIC) is a computerized index of criminal justice information such as fugitives, stolen properties, and missing persons maintained by the FBI. NCIC is available to federal, state, local, and tribal law enforcement and other criminal justice agency users and is operational 24 hours a day, 365 days a year. According to the NCIC 2000 Operating Manual for the Vehicle File, a vehicle is any motor-driven conveyance (except a boat) designed to carry its operator. In addition to conveyances meeting this definition, aircraft and trailers are also entered in the Vehicle File. Additional information about NCIC can be found in Appendix VIII.

However, the USNCB Chief Information Officer (CIO) explained that a foreign law enforcement officer attempting to identify one of those stolen vehicles would need to conduct two separate queries. In one query, the officer would search the INTERPOL SMV records of 122 countries. Then the officer would have to run a second query in NCIC to search the records of the United States. To reduce the number of searches that law enforcement officers need to perform, the USNCB stated in its August 2005 information technology strategic plan that it intended to work with the FBI to develop a link between the INTERPOL SMV database and NCIC. This link would allow foreign law enforcement officers querying the INTERPOL SMV to simultaneously query NCIC without requiring a separate search. But the USNCB CIO stated that the USNCB had not implemented the initiative because the FBI and USNCB would need to improve their information technology systems to build and maintain such a link and stolen vehicles are not considered as high a priority as other information sharing projects, including lost and stolen travel documents.

We acknowledge that improving the efficiency of sharing stolen vehicle information may not be as high a priority as other information technology initiatives related to international crime. However, we believe that the USNCB should move forward on linking the INTERPOL SMV and NCIC or explore alternative solutions to assist foreign law enforcement counterparts to investigate and solve crimes associated with stolen motor vehicles.

Fingerprints

Our audit revealed a recent USNCB initiative that we believe is a noteworthy accomplishment for enhancing international information sharing. Specifically, the USNCB has established a proactive initiative with the FBI to foster the exchange of fingerprints of the subjects of interest in the international law enforcement community.

According to the USNCB CIO, the FBI and USNCB have worked closely to ensure that the fingerprint records for the subjects of foreign INTERPOL notices were available to domestic law enforcement agencies through the FBI's Integrated Automated Fingerprint Identification System (IAFIS).⁵¹ In March 2007 the USNCB provided the FBI with a data file containing fingerprints from all active notices that contained fingerprints as of

⁵¹ Deployed in 1999, IAFIS contains digitized records of latent fingerprints (e.g., fingerprints found at crime scenes) and a Criminal Master File of more than 64 million sets of 10 rolled fingerprints. IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours per day, 365 days a year.

March 23, 2007.⁵² Of the fingerprints submitted, the FBI created new IAFIS records for 3,960 fingerprints that were not found in the database.⁵³ The FBI also matched 326 fingerprints to existing fingerprints in IAFIS. Through the review of the 326 matches the USNCB identified:

- The subject of a foreign country's red notice wanted for vehicle theft had been arrested for assault in New York in 2007. The individual was residing in the United States illegally and subsequently was deported.
- The subject of a foreign country's red notice wanted for rape and identified as a U.S. resident had been arrested in Puerto Rico in 2000 for kidnapping and attempted rape. The notice-issuing country has agreed to extradite the subject.
- The subject of a foreign country's red notice wanted for armed robbery was found to be incarcerated in New York under a different name. The USNCB informed the other NCB of the projected date of the subject's release.
- The subject of a foreign country's black notice was deported previously from the United States after serving a sentence for drug trafficking. The USNCB assisted in confirming the identity of the remains.

Following this one-time data match, the USNCB has continued to submit to IAFIS the fingerprints of subjects of INTERPOL notices and diffusions. The USNCB stated that it currently submits the fingerprints for subjects of red, green, and blue notices and diffusions.⁵⁴ As notices are updated or cancelled, the USNCB notifies the FBI so that the records can be modified or deleted.

⁵² Notices and diffusions may be published without having the subject's fingerprints.

⁵³ During the matching process, 340 fingerprint records were rejected for data quality errors.

⁵⁴ Because of potential concerns for the privacy of juveniles, the USNCB does not submit to IAFIS the fingerprints for the subjects of yellow notices and diffusions (missing or abducted children). According to the USNCB General Counsel, since October 2008 the FBI has been reviewing the possibility of allowing into IAFIS these types of fingerprints. Further, the USNCB does not submit to IAFIS fingerprints for subjects of black notices (unidentified bodies). However, for both yellow and black notices and diffusions, the USNCB conducts a search of IAFIS for potential matches.

In April 2008, the USNCB installed a stand-alone IAFIS workstation at the USNCB that gives the USNCB the ability to convert fingerprints originating in the United States to the format used by the INTERPOL database and vice versa. This allows the USNCB to take fingerprint records received from INTERPOL member countries and electronically cross-check them in IAFIS.

In addition, the USNCB can better address fingerprint searches requested by domestic law enforcement agencies because the USNCB can use the IAFIS workstation to convert the fingerprints into the format used by INTERPOL. The USNCB then uses the converted fingerprint file to cross-check the records against the INTERPOL database. According to USNCB officials, they are able to provide a response to domestic law enforcement agencies in less than 20 minutes.⁵⁵

According to the USNCB CIO, state and local law enforcement agencies currently submit their fingerprint requests via e-mail or facsimile. The USNCB manually uploads the fingerprint record using the IAFIS workstation and electronically submits the converted record to INTERPOL. However, this process is labor-intensive and time-consuming for the USNCB. As a result, the USNCB and FBI are currently working to develop a method that would allow state and local law enforcement agencies to directly query the INTERPOL fingerprint database.

State and Local Law Enforcement Coordination

As the U.S. point of contact for INTERPOL matters, the USNCB has to not only maintain close relationships with federal law enforcement agencies, but must also maintain close relationships with state and local law enforcement agencies throughout the United States and its territories. The USNCB has therefore established an INTERPOL liaison office in each state, as well as in American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, the U.S. Virgin Islands, and in 11 major cities in the United States.⁵⁶ These 66 liaison offices are typically located within a state police agency, state Attorney General's office, or the law enforcement agency of a city or county. Each office has at least one liaison officer who has been designated to serve as the point of contact for USNCB-related interaction.

⁵⁵ During our observations of the USNCB's operation of its IAFIS workstation, the processing time for fingerprint requests of INTERPOL records averaged approximately 5 minutes.

⁵⁶ The list of all 66 State and Local Liaison Offices can be found in Appendix V.

The USNCB Assistant Director of the State & Local Law Enforcement Division explained that foreign government requests that require action by a state or local law enforcement agency are forwarded from the USNCB to one or more of the 66 liaisons. The liaisons then forward the requests to the appropriate law enforcement agency in their jurisdiction for processing and response. Conversely, domestic law enforcement agencies that need criminal investigative assistance on cases with an international nexus may forward a request through the appropriate liaison or contact the USNCB directly.

Secure Electronic Connectivity

At the beginning of our audit, USNCB officials informed us that they had established a secure e-mail network that the USNCB uses to communicate directly with each of its 66 liaison offices. However, during our audit we found significant problems with the USNCB's ability to reliably communicate with its state and local liaisons.

To assess the relationships between the USNCB and the state and local liaisons, we developed a questionnaire to be completed by the liaisons. We discussed our plans with USNCB officials, who agreed to send our questionnaire to the state and local liaisons via their secure e-mail connections. The questionnaires were sent out by the USNCB on July 24, 2008, with a requested return date of August 22, 2008.

Only one-third of the liaisons responded by the deadline, a response rate significantly lower than we expected. Using telephone numbers obtained from the USNCB, we attempted to contact the liaison officers who had not replied and discovered that 25 of 66 had not received the questionnaire that was e-mailed to them by the USNCB.⁵⁷

When we discussed this issue with USNCB officials, they were surprised that so many liaisons did not receive the questionnaire via the USNCB's e-mail and the USNCB Director directed USNCB staff to resolve the problem. Subsequently, we were informed that some liaisons did not receive the questionnaire because the e-mail messages addressed to them were undeliverable or because there may have been a technical problem

⁵⁷ We re-sent the questionnaire to those liaison offices we were able to contact via an alternate e-mail address or facsimile. In total, we received 58 completed questionnaires from 57 liaison offices (one office provided two questionnaires, each completed by a different individual), which resulted in a response rate of 86 percent. Five liaison officers verbally promised to send the questionnaire but never did. The four remaining liaison officers never responded to our telephone calls and facsimiles.

with the network used to send the messages. Ultimately, we learned that the USNCB had to send some of our questionnaires via facsimile.

According to our questionnaire results, many of the state and local liaisons stated that they interacted with the USNCB on a regular basis. For example, of the 58 state and local liaisons that responded to our questionnaire, 50 (or 86 percent) indicated that they interacted with the USNCB via telephone or e-mail on at least a monthly basis. However, we believe that the problems that the USNCB experienced in sending out our questionnaire call into question the USNCB's ability to effectively communicate with its liaison officers.

We discussed with USNCB officials the problems encountered during the dissemination of our questionnaire. In response, in January 2009 the Assistant Director for the USNCB's State and Local Liaison Division provided us with documentation that indicated that the USNCB had, as of that date, four methods for electronic communication with its liaison offices. Specifically, the USNCB communicated with the 66 liaison offices via the Regional Information Sharing Systems (RISS) network (47 liaison offices), USNCB virtual private network (12 liaison offices), International Justice and Public Safety Information Sharing Network (NIlets) (6 liaison offices), and direct connection to the INTERPOL network (1 liaison office).⁵⁸ Additionally, the USNCB identified several initiatives it has undertaken to determine whether the e-mail accounts within RISS were functioning properly.

Despite these actions, the USNCB still has not adequately ensured that connections through RISS are effective. Specifically, the USNCB sent out a test e-mail message to its liaison offices with RISS e-mail accounts, but could not document that all of these e-mails had been received. Further, while the USNCB has attempted to verify its RISS communication channel, it has not conducted similar processes to ensure that its liaison offices using other electronic applications receive its messages.

Despite its attempts to ensure that it has an adequate method to communicate with its liaisons, we found that the USNCB does not have a

⁵⁸ The RISS network is a national program of regional services designed to enhance the ability of local, state, federal, and tribal criminal justice agencies to: (1) identify, target, and remove criminal conspiracies and activities spanning multijurisdictional, multistate, and sometimes international boundaries; (2) facilitate rapid exchange and sharing of information among the agencies pertaining to known suspected criminals or criminal activity; and (3) enhance coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be interjurisdictional in nature. The USNCB virtual private network is a grouping of computers that uses the Internet to connect remote sites or users together. NIlets links state, local, federal, and international law enforcement, justice, and public safety agencies for the exchange of critical data.

reliable and complete network of connectivity with its liaisons. This deficiency could result in critical law enforcement information or requests for assistance not being disseminated. For example, the USNCB could issue a diffusion to a liaison in a city police agency that a known international fugitive is traveling to that city's jurisdiction. But because of the unreliable nature of the network, the police agency does not receive the message, no action is taken on the fugitive, and the USNCB does not know that the message has not been received and no action has been taken. Therefore, it is imperative that the USNCB ensure that it maintains a secure method of communication with its state and local liaison officers.

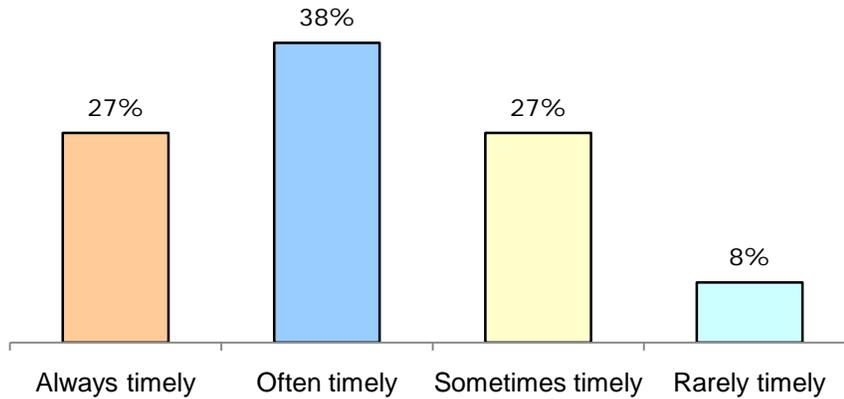
Liaison Evaluation of USNCB Services

In our questionnaire to the 66 state and local liaisons, we requested specific information on feedback they had received about the USNCB from the law enforcement officers in their jurisdictions, along with how helpful USNCB-provided information was in investigations. We also provided respondents the opportunity to comment at the end of the questionnaire.⁵⁹

According to the questionnaire results, many of the state and local liaisons believe the information they received from the USNCB was timely and complete. For example, as shown in Exhibit 2-2, of the 52 state and local liaisons that responded to questions regarding the timeliness of the USNCB, 65 percent indicated that the USNCB was often or always timely.

⁵⁹ The complete questionnaire and responses can be found in Appendix VI.

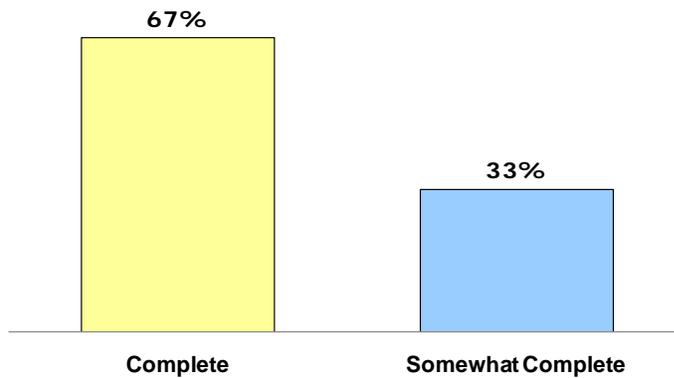
EXHIBIT 2-2
State and Local Liaison Evaluation of USNCB Timeliness



Source: OIG analysis of questionnaire data

In addition, 67 percent of the 52 state and local liaisons that responded to questions regarding the completeness of the information provided by the USNCB indicated that the information was complete. Our results are displayed in Exhibit 2-3.

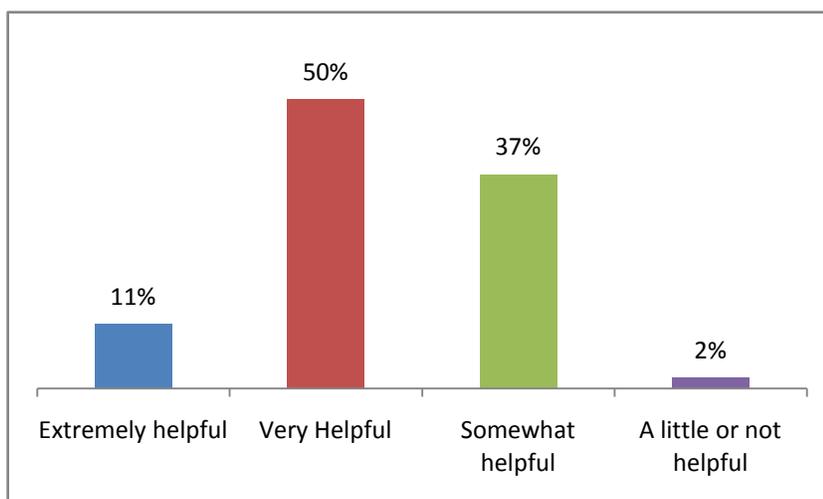
EXHIBIT 2-3
State and Local Liaison Evaluation of the Completeness of Information Provided by the USNCB



Source: OIG analysis of questionnaire data

Further, of the 54 state and local liaisons that responded to our question about the usefulness of the INTERPOL information, 98 percent indicated that the information they received from the USNCB was at least somewhat helpful when investigating cases. Our results are displayed in Exhibit 2-4.

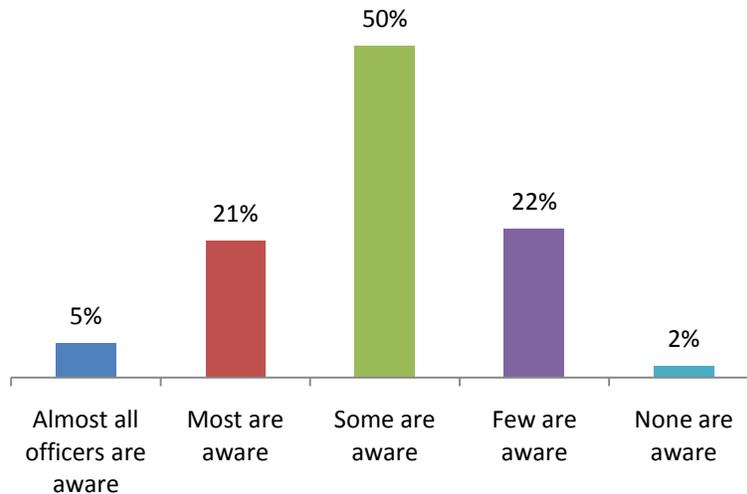
EXHIBIT 2-4
State and Local Liaison Evaluation of the Helpfulness
of Information Provided by the USNCB



Source: OIG analysis of questionnaire data

Although these responses were generally positive, many of the state and local liaisons who responded to our questionnaire indicated that a significant percentage of the law enforcement officers within their jurisdictions were unaware of the INTERPOL databases. As shown in Exhibit 2-5, of the 58 state and local liaisons that responded to our questionnaire, only 26 percent indicated that either almost all or most of the officers within their jurisdictions were aware that they could obtain access to INTERPOL databases. Moreover, only 5 percent of the law enforcement officers in their jurisdictions were more than somewhat knowledgeable about the usefulness of the INTERPOL information.

Exhibit 2-5
Percentage of Officers Aware of INTERPOL Databases



Source: OIG analysis of questionnaire data

We discussed these results with the USNCB Director and Deputy Director. They acknowledged that many law enforcement agencies were unaware of the role and mission of the USNCB and INTERPOL. The Assistant Director for the State and Local Liaison Division stated that although they do not have a formal, written outreach program, they have established a training program for state and local liaisons, which consists of classroom-style training sessions that are conducted at the USNCB twice a year for 4 days each. The training is voluntary and participants are responsible for all expenses. The Assistant Director for the State and Local Liaison Division estimated that approximately 20 participants attend each session. In April 2008, we attended one of these training sessions. However, this training reaches only a very limited audience and does little to expand the understanding of domestic law enforcement officers about how INTERPOL and the USNCB can assist in their investigations.

USNCB officials also stated that they have established booths at numerous law enforcement conferences and have recently implemented a new initiative in which an FBI representative detailed to the USNCB conducts a briefing for FBI Legal Attachés prior to their deployment overseas to inform

them about the role and mission of the USNCB and INTERPOL.⁶⁰ Further, the USNCB has developed and distributed informational pocket cards to law enforcement agencies and has recently redesigned its website.

The USNCB Deputy Director stated that the USNCB's outreach efforts have been hampered by limited resources. However, he stated that the USNCB is exploring alternative methods to provide information to domestic law enforcement. For example, USNCB officials told us that they were working with the Department to produce an informational DVD/CD for distribution to all domestic law enforcement agencies. While the project is still in the development phase, one USNCB official stated that she believed that the DVD/CD will help to reduce training costs and potentially reach a wider audience.

Our review found that the USNCB has implemented some elements of an outreach program. However, despite the USNCB's efforts, many domestic law enforcement agencies remain unaware of the USNCB role and mission, as well as the potential uses of INTERPOL information. We recommend that the USNCB develop a more formal plan that identifies and prioritizes outreach efforts to specific law enforcement organizations.

Conclusion

It is critical that U.S. law enforcement information about international criminals is appropriately disseminated to the 187 member countries of INTERPOL. By sharing this information, the USNCB plays an important role in the United States' ability to identify, locate, and apprehend criminals that have fled the U.S. and entered a foreign country. To effectively accomplish this responsibility, the USNCB needs to encourage domestic law enforcement agencies to provide information to INTERPOL through the USNCB.

We believe that the USNCB has not adequately coordinated with federal law enforcement agencies to solicit their full participation in INTERPOL. As a result, we found that foreign law enforcement counterparts have not been alerted about some of the United States' most wanted fugitives. In addition, we found that information on motor vehicles reported stolen in the United States has not been efficiently shared through the USNCB and INTERPOL with international partners. Moreover, information

⁶⁰ The FBI has stationed agents and other personnel overseas to help build relationships with law enforcement, intelligence, and services around the globe and facilitate a prompt and continuous exchange of information. These Legal Attaché offices - commonly known as LEGATS - are established through mutual agreement with the host country and are generally located in the U.S. embassy or consulate in that nation.

pertaining to the status of INTERPOL-related cases has not been fully shared with all appropriate domestic law enforcement agencies.

We attribute these deficiencies, in part, to a lack of formal agreements between domestic law enforcement agencies regarding the extent and type of case information that should be shared with the USNCB and INTERPOL. In addition, we noted a lack of awareness among federal law enforcement agents of the role of and appropriate uses for INTERPOL information.

Additionally, despite the USNCB's attempts to ensure that it has an adequate method to communicate with domestic state, local, and tribal law enforcement agencies, the USNCB has not implemented a reliable communications network with its liaisons. As a result, we believe that critical law enforcement information or requests for assistance is not effectively disseminated.

Finally, in response to our survey, many of the state and local liaisons expressed satisfaction with the services of the USNCB. However, many of the liaisons also stated that the law enforcement officers in their jurisdictions were unaware of or unfamiliar with the USNCB and INTERPOL. While the USNCB has implemented some elements of an outreach program, we believe that the USNCB should develop a formal outreach plan that identifies and prioritizes specific law enforcement organizations.

Recommendations

We recommend that the Office of the Deputy Attorney General:

1. Work with DHS, the USNCB, and the USNCB Executive Committee to establish formal agreements between federal law enforcement agencies that describe the type of case information these agencies should share with foreign counterparts through the INTERPOL network.

We recommend that the USNCB:

2. Work with its domestic law enforcement partners to ensure that the agencies issue INTERPOL notices for appropriate international fugitives, particularly those already publicly identified on the agencies' websites or elsewhere.
3. Encourage federal law enforcement agencies to provide USNCB and INTERPOL-related training to their employees.

4. Develop a method for domestic law enforcement agencies to submit a notice application electronically.
5. Implement information technology solutions to more broadly share U.S. stolen motor vehicle information with INTERPOL members.
6. Ensure that a reliable communications network is maintained with all state and local liaison offices.
7. Develop a formal outreach plan that identifies and prioritizes law enforcement organizations that would benefit from a better understanding of the USNCB and INTERPOL.

II. EXCHANGE OF INTERPOL INFORMATION

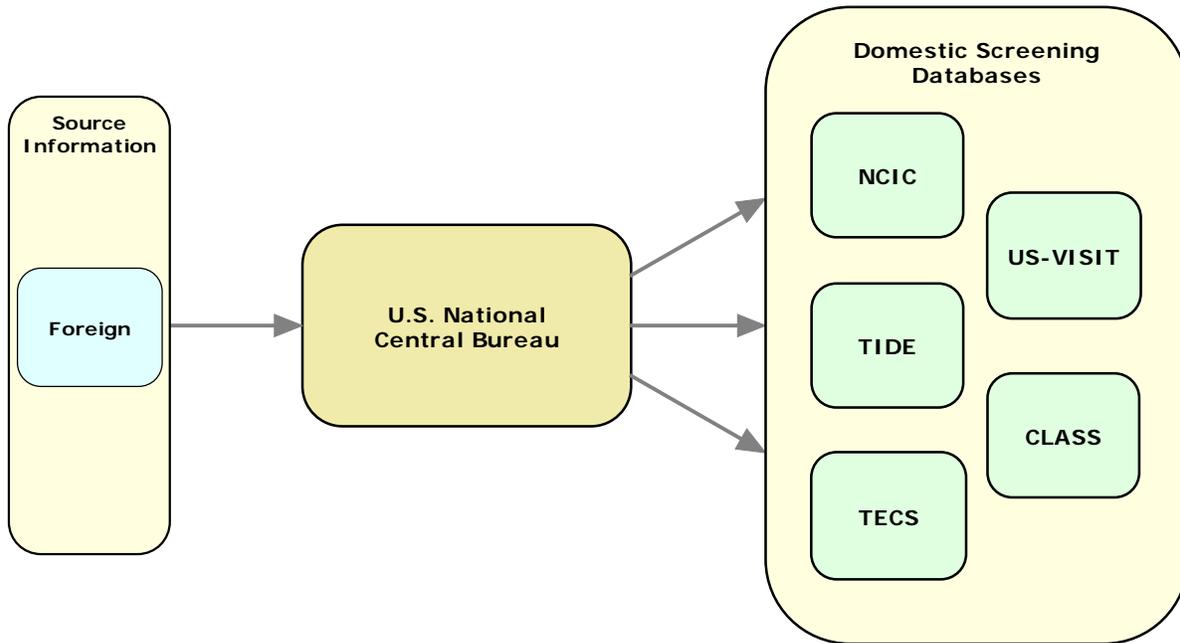
The USNCB has not made critical international criminal information available to appropriate law enforcement agencies in the United States, which increases the potential that high-risk, violent criminals may enter undetected and move about freely in the United States. The USNCB also has not implemented adequate controls or processes to ensure that the INTERPOL information it has made available to domestic law enforcement agencies is current, accurate, complete, and timely. Consequently, domestic law enforcement data systems likely contain out-of-date or incomplete data and include information on individuals for whom no law enforcement agency has a current investigative interest.

Overview of the USNCB's Information Sharing Processes

The USNCB assists domestic law enforcement agencies in obtaining direct access to criminal and terrorist-related information in INTERPOL databases. In addition, as shown in Exhibit 3-1, the USNCB enters a "lookout record" in or provides appropriate international criminal data from INTERPOL to domestic agencies or related domestic systems, such as the FBI's Foreign Fugitive File and Missing Person File within its NCIC system, DHS's Traveler Enforcement Compliance System (TECS) and United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program.⁶¹

⁶¹ A description of each of these data systems is contained in Appendix VIII.

EXHIBIT 3-1
USNCB International Criminal Information Data Flow



Source: OIG depiction of information obtained from the USNCB

The information in these data systems is used by personnel working for domestic law enforcement organizations as part of their regular duties. For example:

- DHS U.S. Customs and Border Protection (CBP) agents encounter individuals at U.S. ports-of-entry and search TECS to determine if a person should be granted access to the United States.
- State Department officials process visa applications from non-U.S. citizens wanting to visit the United States and search CLASS to determine if the individual should be granted a U.S. visa.
- Federal, state, local, and tribal law enforcement officers query NCIC for information on individuals they encounter.
- Officials at regulating agencies request criminal history information prior to issuing licenses to handle hazardous materials and financial securities. Similarly, human resource officials request criminal history information during pre-employment background investigations for various posts in the federal government.

Information Not Shared with U.S. Law Enforcement Agencies

It is critical that international criminal information is appropriately and timely disseminated to domestic law enforcement officers and to U.S. government personnel deciding on the admissibility of individuals attempting to cross a U.S. border. We determined that though the USNCB has made some INTERPOL information accessible to these domestic law enforcement agencies, it has not done so for all of the information that it receives. In the sections that follow, we discuss the deficiencies in the sharing of INTERPOL information and improvements that could be made.

Foreign Notices and Diffusions Not Included in U.S. Agency Databases

USNCB analysts manually enter information on subjects of foreign-issued notices and diffusions into TECS, which are then electronically sent to CLASS. However, the USNCB does not fully share INTERPOL information with NCIC, resulting in inadequate information sharing with domestic law enforcement agencies.

Foreign Green Notices Not Included in NCIC

We found that the USNCB does not enter a lookout record in NCIC for the subjects of foreign-issued green notices. These individuals (including habitual criminal offenders, child molesters, and child pornographers) are considered career criminals who have committed, or are likely to commit, offenses in several countries. We therefore believe that the subjects of green notices should be entered into NCIC. That way although the individuals may be allowed to enter the country, if the individuals commit criminal acts in the United States law enforcement officers investigating those acts will have more information in attempting to solve the crimes.

However, according to the USNCB Compliance Officer, the USNCB has not sought nor has the FBI authorized the USNCB to enter information into NCIC files other than the Foreign Fugitive and Missing Person Files. Because the career criminals identified in green notices are neither foreign fugitives nor missing persons, they are not entered into NCIC. USNCB officials stated that they have not sought approval from the FBI to enter information into other NCIC files, such as the Sexual Offender or the Violent Gang and Terrorist Organization File. When we asked the USNCB Director about entering the subjects of green notices into NCIC, he said that doing so would be a good idea.

We believe that the potential threat to the United States posed by individuals who are the subject of foreign-issued green notices makes it

essential that information about them be shared with domestic law enforcement agencies. We recognize, however, that because INTERPOL green notices cover a variety of criminal types, the criteria for creation of a green notice may not be identical to the criteria for entry into any specific NCIC file. Therefore, we believe that the USNCB should: (1) review foreign-issued green notices and determine if they are appropriate for inclusion in an NCIC file, and (2) work with the FBI to obtain approval to enter green notice subjects into other NCIC files and thereby increase the amount of INTERPOL information available to law enforcement personnel in the United States.⁶²

Foreign Diffusions Not Included in NCIC

The USNCB also does not enter a lookout record into NCIC for the subjects of foreign-issued diffusions. According to USNCB officials, the USNCB enters subjects of foreign diffusions into TECS and CLASS to prevent individuals from entering the country, but does not enter subjects of foreign diffusions into NCIC because, in contrast to formal notices, other member countries often do not ensure that the diffusion information remains accurate and current.⁶³

An INTERPOL official told us that notices have not always been published in a timely manner and cited the lengthy review process, the need to translate notices into the working languages used by INTERPOL, increased workload, and limited resources. As a result, many countries send a diffusion to immediately disseminate information pending submission and approval of the more formal notice. For example, a member country may send a diffusion that an inmate has escaped prison and there is reason to believe the criminal may flee to the United States. In addition, a diffusion may be sent when a child has been abducted. Diffusions can be issued directly by INTERPOL member countries and do not undergo the extensive review process that notices do.

While INTERPOL has undertaken several initiatives to improve its timeliness for notice publication, from June to December 2007 INTERPOL took an average of 26 days from the date it received the notice application

⁶² As of February 28, 2009, there were 865 non-U.S. issued active green notices.

⁶³ INTERPOL requires member countries to validate notices every 5 years and publish updates and cancellations, but it does not require a similar formal review of diffusions.

to the date the notice was published.⁶⁴ In addition during our review of a judgmental sample of 42 foreign diffusion messages, we noted that the foreign country eventually obtained a formal notice in about one-third of the cases. Moreover, the subjects of the wanted person diffusions were often wanted for committing a violent crime and posed a threat to public safety if they entered the United States.

Not entering potentially dangerous criminals into NCIC reduces the chance they will be detected should they try to enter the United States illegally. Further, excluding crime victims (such as abducted children) from NCIC reduces the likelihood that they will be located and returned safely.

While we believe that entering such diffusion information only into border screening systems is useful before a subject enters the country, it does not help for subjects who may have already entered the country before a diffusion could be issued or before the USNCB enters the information into TECS and CLASS.

We recognize that some member countries do not ensure that the information contained in its diffusions remains accurate and current. However, USNCB officials said they tell domestic law enforcement agencies to immediately contact the USNCB before taking any law enforcement action based upon INTERPOL information. Following this contact, the USNCB verifies with the originating law enforcement agency that the information is accurate and reliable. Given the risk inherent with allowing dangerous criminals to enter or remain in the country, we believe that the USNCB should ensure that appropriate data from diffusions are included in NCIC. In doing so, the USNCB could consider entering the subjects of diffusions into NCIC on a term basis and then removing the diffusion subject if a notice was not forthcoming in a set amount of time.

Domestic Notices and Diffusions Not Included in U.S. Agency Databases

When the USNCB becomes involved in a domestic case requiring an INTERPOL notice or diffusion, USNCB analysts do not enter a lookout record

⁶⁴ In January 2008, INTERPOL reported that it had reduced its average time to process a notice to 10 days from the date they receive the notice application to the date the notice is published.

into NCIC. According to the USNCB Compliance Officer, domestic agencies are responsible for entering their own lookout records into NCIC.⁶⁵

The USNCB also does not create a lookout record in TECS or CLASS.⁶⁶ According to the USNCB Compliance Officer, the USNCB determined that it did not need to enter a record into TECS because NCIC and TECS are interconnected and when border control personnel submit a query in TECS, that system automatically queries NCIC and should return a hit against the record entered by the originating agency.

When we asked a USNCB official how INTERPOL information was made available to the State Department for use when reviewing visa and passport applications, the USNCB official said that INTERPOL information was exported from TECS to CLASS once a day. Further, the official said that if the information was not in TECS, it was not in CLASS, and therefore, not available to the State Department for visa and passport checks.⁶⁷ Subsequent to our exit conference, the USNCB official stated that the USNCB had been unaware that its information was provided to the State Department through NCIC.

We recommend that the USNCB re-evaluate its policies and procedures to ensure that information on subjects of domestic notices and diffusions are made available to all domestic law enforcement and border screening agencies.

Inadequate Access to Stolen and Lost Travel Document Information

In July 2002 INTERPOL launched the Stolen and Lost Travel Documents (SLTD) database to collect information on travel documents

⁶⁵ In general, the FBI requires that the law enforcement agency enter records immediately into NCIC when the conditions for entry are met. Records regarding federal fugitives should be entered immediately (e.g., within 24 hours) into NCIC upon receipt of information by the law enforcement agency after the decision to arrest or authorize to arrest has been made.

⁶⁶ Because identity records entered by the USNCB into TECS are electronically disseminated to CLASS once a day, USNCB records that are not entered into TECS are not included in CLASS.

⁶⁷ The FBI told us that NCIC is available for visa and passport checks. According to the FBI, the State Department conducts IAFIS fingerprint searches for all visa applicants. These searches generate NCIC queries and INTERPOL would be notified of any matches to its NCIC records. For passports, CJIS provides the State Department an extract of NCIC records that contain offense codes specified by the State Department, including INTERPOL records associated with those offenses.

reported lost or stolen in member countries.⁶⁸ In a July 2006 report, the GAO stated that passports from Visa Waiver Program countries had been used illegally by travelers attempting to enter the United States. The GAO recommended that DHS, along with appropriate agencies, require all visa waiver countries to provide the United States and INTERPOL with non-biographical data from lost, stolen, or blank passports. The GAO also recommended that DHS develop a plan to make INTERPOL's SLTD database automatically accessible to law enforcement personnel at U.S. ports of entry.

DHS has begun implementing the GAO's recommendation. Utilizing the pre-existing interface between TECS and the Advance Passenger Information System (APIS), DHS, the State Department, the USNCB, and INTERPOL implemented real-time, automated pre-screening of arriving travelers against the SLTD.⁶⁹ When a passenger's travel document information potentially matches information in the SLTD system, a lookout record is created in the TECS system. DHS then coordinates with the USNCB to verify the validity of the document with the foreign country.

In October 2007 DHS implemented a 30-day pilot program at John F. Kennedy International Airport in New York City whereby inbound international air passengers were pre-screened against the SLTD. During the pilot period, the airport reported 129 instances in which a passenger's travel document information potentially matched information in the SLTD. Of the 129 instances, 2 individuals were refused entry. In June 2008 the USNCB reported that passengers aboard all inbound international flights were being pre-screened against the SLTD.⁷⁰

According to a State Department official detailed to the USNCB, the USNCB is currently working with the State Department's Bureau of Consular Affairs to establish a direct interface between State Department components and DOJ for access to the SLTD. This direct connection will provide State Department personnel with critical information about lost and stolen travel

⁶⁸ Information entered by the State Department into the SLTD about U.S. travel documents reported lost or stolen is electronically updated three times per day.

⁶⁹ APIS is the electronic data interchange system approved by DHS's Customs and Border Protection (CBP) agency for air and sea carrier transmissions to CBP for electronic passenger, crew member, and non-crew member manifest data. APIS data includes information that is routinely found on a passport, visa, or airline boarding pass, such as an individual's name, birth date, country of residence, country of origin, and final destination.

⁷⁰ The USNCB is coordinating with DHS to test the feasibility of expanded access to the SLTD. The USNCB reported that the current plan is to initiate a pilot project at several border points. However, various technical and resource issues have not been fully addressed.

documents and will be used in determining eligibility for a U.S. passport or visa. However, the State Department official told us that this project is not considered a high priority by the State Department, and he was unaware of any specific plans to implement the initiative.

State, local, and tribal law enforcement agencies do not have direct access to INTERPOL's stolen and lost travel document information. As a result, these domestic law enforcement agencies may unknowingly encounter a criminal who is fraudulently using a stolen or lost travel document.

According to the detailed State Department official, the USNCB has not pursued including SLTD information directly into NCIC, thereby making the information available to state and local law enforcement agencies. He explained that INTERPOL rules do not allow for the downloading of SLTD data into national databases because this would impede INTERPOL member countries' ability to automatically update the data and receive automatically generated notifications when their records are viewed.

We were also told by USNCB and INTERPOL officials that although INTERPOL requires that member countries verify the accuracy of INTERPOL information prior to taking any law enforcement action, some countries are slow to respond to these verification efforts. Because of concerns over the accuracy of the SLTD information and the unnecessary delay or potentially adverse impact to an individual during an encounter with law enforcement officers, the detailed State Department official said that the USNCB is reluctant to include SLTD information in NCIC.⁷¹

We understand the need for SLTD information to be as current and accurate as possible to avoid unnecessarily or adversely impacting innocent individuals. However, as noted in the July 2006 GAO report, DHS officials acknowledged that inadmissible aliens may enter the United States using a stolen or lost passport from a visa waiver country. As a result, we believe that the USNCB should develop an acceptable method to provide domestic law enforcement agencies with access to the information in the SLTD. While acknowledging the benefit of providing such access, USNCB officials said it is essential that the information be updated in near-real time. Therefore, we believe that the USNCB should explore options that provide a technological solution to this issue, such as a direct connection between the INTERPOL databases and NCIC. Using this configuration, when a law enforcement

⁷¹ The State Department official also informed us that some countries re-use and re-issue passport numbers that have been reported as lost or stolen, and frequently the originating foreign country does not update the SLTD to reflect that the passport number has been re-issued.

officer submitted a query to the NCIC database, the system would automatically submit the query to the INTERPOL databases.

Identifying and Sharing New Information

As a central access point for information from many law enforcement sources, the USNCB is in a position to receive additional identifying information on subjects of domestic notices and diffusions. For example, the USNCB may have access to information provided by a foreign law enforcement agency indicating that the subject of a domestic notice is using additional aliases or fraudulent travel documents. This additional information could augment the domestic agency's records. For example, we identified a U.S.-issued wanted person diffusion for an individual that is wanted in New York for forcible rape. The wanted person diffusion indicated that the subject had a foreign passport and provided the passport number. The diffusion also reported that U.S. officials believed that the individual had fled to the Middle East via an African nation. Another NCB responded to the USNCB that the passport identified in the diffusion had expired and the NCB provided the new passport number. However, the USNCB did not forward the new passport number to the U.S. agency that submitted the diffusion and did not update its electronic case file to include the new passport number.

Subsequently, two additional NCBs responded to the wanted person diffusion that the subject had traveled through their countries. However, because these responses referenced the fugitive's new passport number and the USNCB had not updated its records, the USNCB failed to respond to the new information. As a result, opportunities for apprehending this criminal may have been missed.

Further, USNCB officials told us that when processing a domestic law enforcement agency's application for issuance of a notice or diffusion, they verify that the domestic agency has appropriately entered a record into NCIC for the subject. However, during our review of 101 domestic notices and diffusions, we identified 7 instances in which the NCIC record contained additional information about the subject that was not included on the domestic-issued notice or diffusion. Although the domestic law enforcement agencies did not always include the additional information in their applications for issuance of the notice or diffusion, the USNCB should have identified the information during its review of the NCIC record. As a result of the USNCB's failure, the information was not distributed to foreign law enforcement.

We found that the USNCB has not developed processes for ensuring that it identifies and shares additional information on subjects of domestic notices and diffusions. As a result, additional information that could be used to identify or apprehend criminals has not been shared with relevant law enforcement agencies. Moreover, much of the information we identified during our review of USNCB case files was easily obtained by the USNCB through notice applications and searches of other law enforcement databases.

We recognize that identifying all such additional information currently in the USNCB's possession would be a time-consuming and labor-intensive process for the USNCB. However, we believe that the USNCB must address this issue to ensure that additional information it obtains that augments the domestic law enforcement agency data should be made available to all relevant agencies.

INTERPOL Database Direct Accessibility

At the beginning of our audit, USNCB officials including the Director, Deputy Director, and Assistant Director for the State and Local Liaison Division informed us that the USNCB had made significant progress in providing all domestic law enforcement officers with the ability to independently query the INTERPOL databases through Nlets. Specifically, the Assistant Director for the State and Local Liaison Division stated that a majority of the 50 State Terminal Control agencies had signed Memoranda of Understanding (MOU) that are required by the USNCB for organizations to gain access to the INTERPOL databases.⁷²

When we discussed this issue with the USNCB CIO, he clarified that the USNCB had established an Internet connection between INTERPOL and each state through Nlets. However, he said that each state must first modify its local system before it can access the INTERPOL databases using the Nlets connection. The USNCB Assistant Director for the State and Local Liaison Division told us that some states were reluctant to make the necessary modifications because of budget and other resource constraints. In April 2008, the USNCB CIO stated that all 50 states were still in the process of evaluating the initiative, modifying their systems, or testing the connections, and therefore none of the states was able to directly access and query the INTERPOL databases via Nlets. When we spoke to the Assistant Director for the State and Local Liaison Division about this issue in

⁷² Nlets State Terminal Control agencies are law enforcement agencies in each state that are assigned the responsibility for managing access to the Nlets network and ensuring that Nlets's system security and operational policies and procedures are carried out within the state.

June 2008, he stated that he believed that some states had implemented the required system modification. However, he was unable to provide us with a list of the states that had fully implemented the necessary system modifications. After several attempts to confirm this information, the same USNCB official stated in September 2008 that the USNCB had determined that a limited number of states had fully implemented the system modifications to permit law enforcement officers within these states to query INTERPOL databases. Moreover, he stated that the Nlets connection required state or local law enforcement officers to generate a separate query for the INTERPOL databases in addition to a standard NCIC query.⁷³ The FBI informed us that the Nlets configuration can provide access for tribal law enforcement agencies that have been assigned an NCIC Originating Agency Identifier (ORI).⁷⁴

During the course of these meetings, we discussed an alternative method for providing federal, state, local, and tribal law enforcement agencies with access to INTERPOL information. Specifically, we asked if USNCB officials had considered the feasibility of developing a direct connection between the INTERPOL databases and NCIC. Using this configuration, when a law enforcement officer submitted a query to the NCIC database the system would automatically submit the query to the INTERPOL databases. The USNCB CIO said that he believed that this would require only relatively minor modifications to USNCB and NCIC systems and would provide access to most law enforcement agencies that currently have the ability to query NCIC, including many tribal law enforcement agencies.

When we discussed these issues with officials at the FBI's Criminal Justice Information Services (CJIS), they initially expressed concern regarding the logistics and potentially prohibitive cost of developing such an interface.⁷⁵ However, the USNCB Director requested the FBI to coordinate with the USNCB and establish a joint USNCB-FBI working group to evaluate

⁷³ In April 2009, the USNCB reported that the Metropolitan Police Department of the District of Columbia had provided its law enforcement officers with the ability to directly query the INTERPOL databases. In addition, two states had modified their systems to allow law enforcement officers to submit just one query to search NCIC and INTERPOL databases.

⁷⁴ The USNCB reported that it has joined a DOJ working group on tribal issues to evaluate the need and feasibility of providing tribal law enforcement agencies with access to INTERPOL information. An NCIC ORI is a nine-character identifier assigned by the FBI NCIC to an agency that has met the established qualifying criteria for an ORI assignment to identify the agency in NCIC and Nlets transactions. An ORI identifies an agency by state and location within a state.

⁷⁵ Established in February 1992, the FBI's Criminal Justice Information Services (CJIS) manages NCIC.

the feasibility of utilizing NCIC as a means to expand access to the INTERPOL databases. In October 2008, the USNCB and CJIS agreed to conduct a study to determine if NCIC provides a viable and useful environment for delivering increased access to INTERPOL data, including notice, stolen motor vehicle, and lost and stolen travel document information.

In April 2009, the USNCB reported that it was in the final stages of testing the requisite infrastructure upgrades for the study and had requested sample data from CJIS to begin testing the process. The USNCB said it anticipated that it would begin the initial testing in May 2009, which would consist of simulating 1 day's worth of NCIC queries against the INTERPOL databases. With an estimated 7 million NCIC transactions per day, the USNCB, FBI, and INTERPOL General Secretariat will be evaluating performance response times to ensure the process conforms to NCIC criteria. In addition, the working group will measure the query-to-hit ratios to evaluate the value or benefit of providing INTERPOL information to NCIC users. Depending on the success of the initial data match exercise, additional comparisons may be conducted to obtain a better statistical baseline to justify full implementation.

Standard queries made by law enforcement officers to NCIC return information contained in NCIC's files, such as its wanted person and gang files. After law enforcement officers run an NCIC query, unless they have additional information or a reason to believe that an individual may be a person of interest to another country, there is no way for them to know that they should perform an additional query of INTERPOL's databases to potentially obtain additional information. We believe that requiring officers to perform multiple queries increases the risk that information on these subjects will not reach frontline law enforcement officers. As a result, we believe that the USNCB should either ensure that all INTERPOL information is contained within NCIC or develop a method, such as a direct connectivity through NCIC, to ensure that all domestic law enforcement have access to the INTERPOL databases using one query. Therefore, while the USNCB works with the FBI to assess the feasibility of a direct connection with INTERPOL through NCIC, the USNCB should ensure that INTERPOL information is entered into NCIC in a complete, timely, and accurate manner.

USNCB Processing of INTERPOL Information

We reviewed a judgmental sample of 216 cases consisting of 115 foreign and 101 domestic notices and diffusions that were active from

October 1, 2005, to May 29, 2008.⁷⁶ We examined the notices and diffusions to ensure that the USNCB entered the INTERPOL information into the appropriate U.S. agency databases in a timely manner. Further, we reviewed the cases to determine if basic information (name, date of birth, passport number and country of issuance, other identification numbers such as driver's license number, warrant information, and physical characteristics) was consistent in all of the affected databases.⁷⁷

We found that, in general, the USNCB's processing of domestic-issued notices and diffusions ensured the accuracy of the data, and we identified virtually no errors in the 101 domestic cases we tested.⁷⁸ However, our examination of the USNCB's processing of foreign notices and diffusions revealed that the agency has not implemented adequate controls or processes to ensure that the INTERPOL information it makes available to domestic agencies is accurate, current, and timely. Consequently, the U.S. agency systems likely contain out-of-date or incomplete data, include information on individuals for whom no law enforcement agency has a current investigative interest, and may violate INTERPOL's guidelines for handling information. Our results are discussed in detail below.

INTERPOL Information Not Shared

The USNCB has established guidelines for the inclusion of foreign-issued notice and diffusion information into TECS and NCIC.

We examined whether the USNCB adequately entered the foreign-issued notice and diffusion information into U.S. agency databases. We assessed the USNCB's processing of 92 foreign-issued notices and diffusions that met the USNCB's guidelines for entering a lookout record into DHS's TECS.⁷⁹ As shown in Exhibit 3-2, our analysis revealed that 21 of the 92 cases, or approximately 23 percent, did not have a corresponding lookout record in TECS.

⁷⁶ Our sample consisted of 42 domestic notices, 59 domestic diffusions, 62 foreign notices, and 53 foreign diffusions.

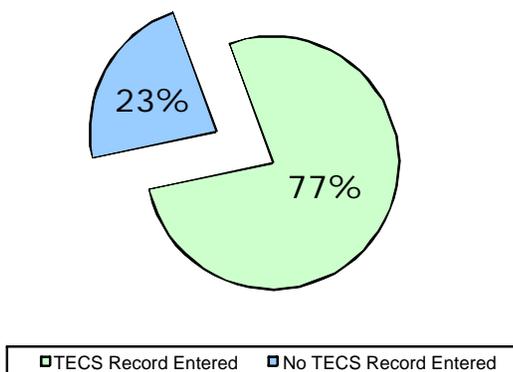
⁷⁷ For more a detailed description of our methodology, see Appendix I.

⁷⁸ Because the USNCB does not enter the subjects of domestic notices into any U.S. agency systems, our review of the USNCB's processing of domestic notices and diffusions was limited to entries into its internal case management system.

⁷⁹ We originally selected 115 foreign-issued notices and diffusions, but 23 did not meet the USNCB's guidelines for entry into TECS. According to the USNCB, some specific notices and diffusions contain information that may not be suitable for entry in screening databases. For additional information on our methodology, see Appendix I.

EXHIBIT 3-2
USNCB Inclusion of
Foreign Notices and Diffusions in TECS

Number of Records Eligible for Entry in TECS = 92



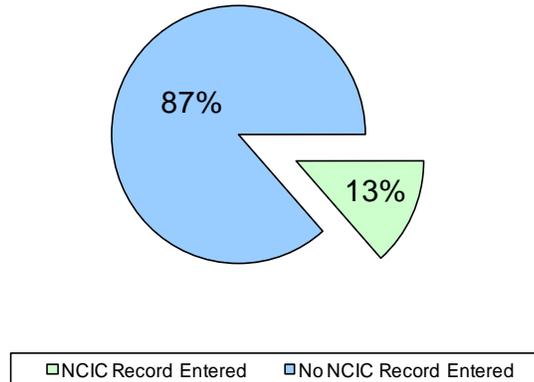
Source: OIG analysis of USNCB data and TECS records

As shown in Exhibit 3-3, we examined the USNCB's processing of 52 foreign-issued notices and diffusions that met the USNCB's current guidelines for entering a lookout record into the FBI's NCIC.⁸⁰ We found that 45 of the 52 cases, or approximately 87 percent, did not have a corresponding lookout record in NCIC.

⁸⁰ We originally selected 115 foreign-issued notices and diffusions, but 63 did not meet the USNCB's criteria for entry into NCIC. According to the USNCB, some specific notices and diffusions contain information that may not be suitable for entry in screening databases. For additional information on our methodology, see Appendix I.

EXHIBIT 3-3
USNCB Inclusion of
Foreign Notices and Diffusions in NCIC

Number of Records Eligible for Entry in NCIC = 52



Source: OIG analysis of USNCB data and NCIC records

We also found that the USNCB had not entered a lookout record into NCIC for 22 of the 24 foreign red notices in our sample of 115 cases. As a result, in the cases we reviewed the USNCB had not entered lookout records into NCIC for approximately 92 percent of the fugitives for whom extradition was sought from a foreign country.

We discussed these issues with USNCB officials, and they agreed with our findings but were unable to provide an explanation for the 21 records missing from TECS. However, for the 45 records missing from NCIC, the officials said the USNCB was erroneously applying a too restrictive set of criteria for including the records in NCIC. As a result, many records were not entered into NCIC because the USNCB believed that the INTERPOL records did not contain the necessary data. Specifically, the USNCB erroneously believed that the subject's height, weight, and hair color were required for entry. In fact, the FBI does not require the USNCB to populate these fields if either the subject's photograph or fingerprints are available instead.

As a result of our discussions with USNCB officials, the USNCB made changes to its computer systems to ensure that all appropriate subjects would be entered into NCIC in the future. In addition, the USNCB worked to identify the subjects of foreign notices in its existing cases that had been omitted from TECS and NCIC and made the necessary entries. The USNCB reported that its initial review identified 2,650 files that required additional review for possible entry of a record into TECS and NCIC. In August 2008, the USNCB assigned staff to review the subjects and make the appropriate

entries. According to the USNCB Director, the USNCB completed its review in October 2008 and identified and corrected 688 and 481 records that required entry in TECS and NCIC, respectively.

Untimely Entry of Information into U.S. Agency Databases

According to USNCB internal policies, if a foreign notice or diffusion contains sufficient information and meets the criteria for entry in TECS and NCIC, USNCB analysts are required to enter a lookout record immediately upon receipt of the foreign communication. To assess the USNCB’s efforts at making these entries in a timely manner, we calculated the length of time from the date that the notice or diffusion was first published or received by the USNCB to the date the USNCB entered a lookout record into TECS or NCIC. Based on our review of TECS and NCIC records concerning subjects of foreign notices or diffusions, we found that the USNCB frequently entered these records in an untimely manner.

As shown in Exhibit 3-4, of the 71 lookout records entered in TECS by the USNCB, 31 percent were entered within 1 day, while more than 40 percent were entered more than 30 days after initial receipt. In addition, of the seven lookout records that the USNCB entered into NCIC, none were entered within 1 day. In fact, the majority were entered over 30 days after the USNCB first received the notice or diffusion.

EXHIBIT 3-4
USNCB Inclusion of Foreign Notices and Diffusions from Domestic Systems

| | TECS | | NCIC | |
|---------------------------|-----------|------------|----------|------------|
| | Records | Percentage | Records | Percentage |
| 1 day or less | 22 | 31 | 0 | 0 |
| 2-5 days | 6 | 8 | 0 | 0 |
| 6-10 days | 4 | 6 | 0 | 0 |
| 11-30 days | 8 | 11 | 2 | 28 |
| 31-90 days | 18 | 25 | 3 | 43 |
| Over 90 days | 13 | 18 | 2 | 28 |
| Total⁸¹ | 71 | 99 | 7 | 99 |

Source: OIG analysis of USNCB, TECS, and NCIC records

We discussed this issue with USNCB officials, who agreed with our findings and attributed these delays to the USNCB’s increasing workload, limited resources, and the need to translate notices and diffusions into English. According to the USNCB Assistant Director for the INTERPOL

⁸¹ The percentages did not total 100 percent due to rounding differences.

Operations and Command Center (IOCC), the number of notices processed each month increased from an average of 230 per month in fiscal year (FY) 2007 to an average of 309 per month in FY 2008 or 34 percent. However, the USNCB did not receive additional permanent staff during this time, which, according to the USNCB Assistant Director, caused delays in its processing of notices and diffusions.

According to a USNCB official, as of June 2008 the USNCB had a backlog of 119 new foreign notices that required initial review for inclusion in domestic systems. When we brought this situation to the attention of the USNCB Director, he stated that he had been unaware of the backlog in processing notices and diffusions. As a result, he said he would adjust staff assignments, reassign staff from other sections, and hire two contractors.

Removal of Foreign Notice and Diffusion Information from U.S. Databases

According to its internal policies, when the USNCB receives notification of the cancellation of a notice or diffusion, a USNCB analyst is required to immediately delete the corresponding lookout records in NCIC and TECS. Using our sample of foreign notices and diffusions for which the USNCB entered a lookout record in TECS or NCIC, we assessed the USNCB's efforts at ensuring the timely removal of INTERPOL information from the U.S. systems. We reviewed the length of time from the date that the notice or diffusion was cancelled to the date the USNCB removed the domestic lookout records.

We found that the USNCB frequently failed to remove records in a timely manner regarding subjects of foreign notices or diffusions from these systems, as detailed in Exhibit 3-5.⁸² For 25 of the 71 cases the USNCB entered into TECS, the originating government requested cancellation of the initial notice or diffusion. Of these, the USNCB removed just five records (20 percent) within 1 day. Further, it took the USNCB more than 5 days to remove the majority, or approximately 44 percent, of the lookout records. Of the seven lookout records that the USNCB entered into NCIC, two of the originating notices or diffusions had been cancelled by the originating government. The USNCB removed these two NCIC lookout records within 1 week.

⁸² Because the USNCB requires that its analysts remove a lookout record from U.S. agency databases immediately upon receipt of the communication, we considered them to be timely if the record was removed within 1 day.

EXHIBIT 3-5
USNCB Removal of Foreign Notices and Diffusions from
U.S. Agency Systems

| | TECS | | NCIC | |
|---------------|-----------|------------|----------|------------|
| | Records | Percentage | Records | Percentage |
| 1 day or less | 5 | 20 | 0 | 0 |
| 2-5 days | 9 | 36 | 2 | 100 |
| 6-10 days | 7 | 28 | 0 | 0 |
| 11-30 days | 2 | 8 | 0 | 0 |
| 31-90 days | 1 | 4 | 0 | 0 |
| Over 90 days | 1 | 4 | 0 | 0 |
| Total | 25 | 100 | 2 | 100 |

Source: OIG analysis of USNCB, TECS, and NCIC records

We discussed this issue with USNCB officials who agreed with our findings and again attributed the delays in removing the records to a lack of sufficient resources and increasing workload.

However, it is essential that the USNCB ensure that the information it provides to law enforcement agencies remains current. If the USNCB fails to do this, domestic systems will contain out-of-date or incomplete data and may include information on individuals for whom no law enforcement agency has a current investigative interest. Retaining incomplete or out-of-date data also increases the probability that the information may violate INTERPOL's guidelines for handling information. INTERPOL has established record-purging requirements to help ensure that data is not improperly retained or utilized. In addition, according to USNCB officials, INTERPOL's Rules for Processing Information (RPI) take into consideration member countries' privacy laws.

Inconsistent or Inaccurate Records

Using our sample of 92 foreign-issued notices and diffusions that met the criteria for entry in TECS or NCIC, we examined U.S. domestic system records to determine if basic information, including name, date of birth, gender, passport number and country, warrant information, additional identification numbers, and physical characteristics, was shown consistently in all of the affected databases. We compared the information contained in the notice or diffusion to that entered in TECS, NCIC, or ENVOY records. As shown in Exhibit 3-6, within the 92 records we reviewed we identified 53 inconsistencies in the information contained in the domestic system records.⁸³

⁸³ Not all of the 92 records we reviewed contained inconsistencies. Some records contained multiple inconsistencies.

EXHIBIT 3-6
Foreign Notice and Diffusion
Sample Record Inconsistencies

| Record Field | Record Inconsistencies⁸⁴ |
|-----------------------------------|--|
| Name | 0 |
| Date of Birth | 3 |
| Gender | 2 |
| Passport Number and Country | 5 |
| Warrant Information | 22 |
| Additional Identification Numbers | 7 |
| Physical Characteristics | 14 |
| Total | 53 |

Source: OIG analysis of USNCB data

We discussed these inconsistencies with USNCB officials, who agreed with our findings but were unable to provide an explanation for the errors. USNCB internal case management policies require that a supervisor review both the NCIC and TECS entries within 48 hours of the entry in the respective systems. Further, upon completion of the review the supervisor is required to document their review in the USNCB case file. During our review of the USNCB case files, we noted that most of the case files did not have the required documentation indicating a supervisory review. Moreover, during our interviews of USNCB analysts and supervisors, some stated that supervisory review was lacking.

Errors and inconsistencies in database records that should contain identical information can hamper investigations or delay law enforcement agents in their efforts to determine if individuals they encounter are a positive match for the subject of a notice or diffusion. In addition, errors and inconsistencies can contribute to the misidentification and delay of an innocent person or the inappropriate release or admittance of a dangerous individual. Therefore, we recommend that the USNCB ensure that all of its employees, including detailees, are properly trained on the supervisory review process. In addition, the USNCB should ensure that necessary supervisory reviews are conducted and documented.

⁸⁴ Each entry in this column represents a notice or diffusion for which we determined that the information contained within the notice or diffusion was not in agreement with NCIC, TECS, or ENVOY. It is possible for one record to have more than one error. The overall total is the number of field errors.

INTERPOL Rules for Processing Information

INTERPOL and its member countries have established rules for the maintenance, retention, and deletion of INTERPOL information in INTERPOL and domestic databases. INTERPOL permits the inclusion of INTERPOL data in domestic data systems, such as DHS's TECS and FBI's NCIC. However, INTERPOL requires the NCBs to control the use of data and ensure that any shared data is accurate, current, and timely.⁸⁵ Moreover, INTERPOL has established record-purging requirements to comply with its RPI and to help ensure that obsolete data is not retained or improperly utilized. INTERPOL requires that the NCBs review the systems to which they provide information to verify compliance with the INTERPOL RPI.

According to the INTERPOL RPI, NCBs are required to ensure that each organization they designate to access or receive INTERPOL information is aware of and able to comply with the INTERPOL rules, such as ensuring that data is accurate, current, and timely. In addition, the NCBs are required to verify, to the extent possible, compliance with the rules. The USNCB General Counsel told us that the USNCB requires each organization that accesses or receives INTERPOL data to sign an MOU in which they agree to abide by the INTERPOL RPI. However, he stated that the USNCB does not review these systems to verify that the information has been appropriately maintained or deleted. As a result, the USNCB is unable to verify whether the domestic organizations who have access to INTERPOL data comply with the terms of the RPI.

In one instance, USNCB officials told us that the USNCB had allowed DHS to include biographical data and fingerprints from INTERPOL notices in its Automated Biometric Identification System (IDENT). USNCB and DHS officials discussed the conditions under which DHS may include INTERPOL information in the IDENT system, as well as the requirements for the information's maintenance and retention. The USNCB and DHS documented their agreement in an e-mail. According to the agreement, the USNCB permitted DHS to retain the INTERPOL fingerprints and biographical information if the information already matched an existing IDENT record even if the notice was cancelled.⁸⁶ However, the agreement stipulated that INTERPOL information for which there was no match in IDENT should be deleted following the closure or cancellation of a notice.

⁸⁵ According to INTERPOL's rules, the NCBs must update information that has been incorporated into other systems at least weekly.

⁸⁶ When a notice is canceled, DHS annotates the IDENT record to document that the individual is no longer wanted, but that the individual may have a criminal history in a foreign country.

During our review, USNCB and DHS officials stated that regardless of the existence of a pre-existing record, DHS was retaining all information on all notices that indicated that the subject was violent. When we asked USNCB officials if this practice complied with their agreement with DHS, they were uncertain, although they said the practice did not appear to comport with their electronic agreement with DHS or the RPI.

According to USNCB officials, as a result of our findings they worked with DHS to identify and update or remove those records that were not consistent with the written agreement and INTERPOL's rules. The USNCB and DHS identified 265 records that had been retained in the IDENT system, the majority of which should be removed. DHS has agreed to delete these records and provide the USNCB with written confirmation of the deletion.

USNCB officials also reported that they met with DHS and FBI officials and recently designated the FBI's IAFIS as the primary domestic database for all INTERPOL fingerprints. To ensure that DHS retains access to INTERPOL fingerprint information, the USNCB intends to use the pre-existing interface between IAFIS and IDENT to facilitate the exchange of INTERPOL fingerprints. Further, the USNCB indicated that it has expanded the number and types of fingerprints that will be shared and will allow DHS to access INTERPOL criminal history data. The USNCB anticipates that this information will be used by law enforcement agents at U.S. borders to determine admissibility of individuals.

During our review of the USNCB's case files, we also noted that the USNCB requested that the FBI remove the USNCB-provided fingerprints from IAFIS when a notice or diffusion was cancelled. However, there is no policy that requires the FBI to provide the USNCB with written confirmation of record removals, and the USNCB is not receiving this information. As a result, the USNCB is unable to verify that the INTERPOL information it provided for entry into IAFIS remains current and accurate. When we discussed this with the USNCB Compliance Officer, she acknowledged this weakness and stated that the USNCB had not established a formal process to confirm that fingerprint records have been removed from IAFIS. However, the USNCB agreed to work with the FBI to establish a formal process to add and remove fingerprints from IAFIS that included a written confirmation of removal.

INTERPOL Enhancements to Information Exchange Efforts

As noted above, during our discussions with USNCB officials regarding the deficiencies in USNCB management and control of INTERPOL data, these

officials attributed many of the problems and delays to the need to translate documents, increasing workloads, and limited resources, including personnel and funding. However, during our review of the USNCB's procedures we found that its manual data entry processes were overly labor-intensive, time-consuming, and prone to errors and that these issues contributed to the USNCB's deficiencies.

According to USNCB officials, the notices and diffusions that it receives are often electronic messages with documents attached. To share the information electronically with domestic law enforcement agencies, USNCB analysts must copy or enter the data from the message or document – field-by-field –into the appropriate databases. When the USNCB needs to send a notice or diffusion to INTERPOL or any member countries, it must extract the data from its databases and convert the information into an electronic message or document.

When we discussed this issue with INTERPOL officials in Lyon, France, they acknowledged that this process was inefficient and prone to errors. INTERPOL officials said that they had problems similar to those experienced at the USNCB, including issues related to notice and diffusion translation, workload, and limited resources. As a result, INTERPOL has experienced delays and has a significant backlog in publishing notices and disseminating information. According to INTERPOL data, as of August 2008 the time required for publishing a notice in at least one of the official INTERPOL languages was approximately 2 weeks. The delay to publish the notice in the other official languages was 60 days. INTERPOL officials also stated that from 2001 to 2007 there was more than a 200-percent increase in the number of message requests that contributed to the backlog and overwhelmed INTERPOL resources.

According to INTERPOL General Secretariat officials, redundant data entry processes have been necessary because there is no accepted standard within the international law enforcement community for the structure and transmission of electronic police information. INTERPOL officials stated that they worked with member countries and in 2008 defined such a standard for INTERPOL. In addition, INTERPOL has designed a new messaging system for member countries based on the new standard.⁸⁷ When implemented, this new system, I-Link, will replace INTERPOL's current system, the INTERPOL Criminal Information System. According to INTERPOL officials, because all member country transmissions will use the new standard, the

⁸⁷ Once the new system is implemented by each member country, they will be required to use the new standard for all communication concerning INTERPOL information.

I-Link system will automate the notice and diffusion process. As a result, I-Link should eliminate the manual entry and manipulation of data by both INTERPOL and USNCB analysts.

Further, INTERPOL officials anticipate that the I-Link system should improve data quality because the new system will use a computer program to analyze incoming information against a set of business rules.⁸⁸ INTERPOL officials believe the business rules will help to ensure data integrity for information regarding the subject of the notice, including physical characteristics, name, and date of birth. For example, if a field should contain only numeric data, the system will reject a record that contains letters or any symbol other than numerals. Moreover, to reduce the need for human translation services, INTERPOL anticipates incorporating software technology to facilitate the conversion of various non-INTERPOL languages into one of the four languages used by INTERPOL.

INTERPOL officials also stated that the new I-Link system will provide member countries with the ability to obtain a master list of the notices that are current and available for them to view. In contrast, the current data system does not provide member countries with a comprehensive and current list of all active notices and diffusions to which they have been granted access.⁸⁹ As a result, the USNCB is unable to ensure that it has shared with law enforcement agencies all information to which it has been granted access by member countries.

INTERPOL officials anticipate that each of these improvements should dramatically reduce the time it takes for INTERPOL and member countries to process and share law enforcement information. As a result, they expect to reduce the need to translate documents, thereby saving personnel and other resources. Moreover, INTERPOL officials reported that once the I-Link system is implemented, they anticipate that staff currently performing manual data entry may be reassigned to perform more critical, higher-level analysis such as criminal trend analysis.

According to the USNCB, I-Link was launched on January 19, 2009, and underwent a 2-month trial during which the USNCB tested the red notice form application. Although a few of the NCBs are using I-Link, the USNCB stated that most of the NCBs were still testing the I-Link system.

⁸⁸ A business rule is an automated information technology function in which the record is analyzed for specific deficiencies and compliance with established criteria.

⁸⁹ Each member country may designate which countries may access the law enforcement information it shares with INTERPOL. As a result, none of the member countries have identical access to INTERPOL information.

However, during the USNCB's testing period, the USNCB found that the program was not easy to use and it identified several legal issues related to the wording of the notices. In addition, the USNCB identified significant problems with data integrity and accuracy. The USNCB stated that it has reported these issues to the INTERPOL I-Link project manager. The USNCB continues to attend the I-Link advisory group meetings and is working with INTERPOL to resolve the issues. However, the USNCB did not provide an estimated date that it would implement the I-Link system.

USNCB Quality Assurance Efforts

Beginning in 1994, INTERPOL implemented a program to review the operations of each member country's National Central Bureau. These "Good Practices" reviews are conducted by a team of representatives from other NCBs, the INTERPOL General Secretariat, and the relevant sub-regional bureau. During each review, the subject NCB is evaluated against 24 agreed-upon service standards.⁹⁰

The USNCB was last evaluated in January 2006. During this review, the INTERPOL review team made eight recommendations, including recommendations related to the quality of USNCB messages sent to other INTERPOL members and the USNCB's internal monitoring of the progress of ongoing cases.

For example, the INTERPOL review team recommended that USNCB supervisors conduct regular reviews of a sample of outgoing messages regarding notices and diffusions to ensure that the messages are correctly classified and worded, and provide all the pertinent information. The USNCB senior management team agreed with the findings and implemented an updated internal quality control process in February 2008. According to the USNCB Compliance Officer, the USNCB had not conducted an internal quality assurance review during the prior 3 to 4 years because of a lack of resources.

Under the USNCB's quality assurance program implemented as a result of the INTERPOL review, each USNCB division is responsible for preparing and submitting a self-evaluation package once a year. The self-evaluation package consists of a questionnaire completed by senior management and a Quality Assurance Review checklist completed by each caseworker in the

⁹⁰ These service standards are designed to evaluate each member country's NCB ability to perform the functions as a representative of INTERPOL, including adequate governmental support for operations, translation capability, and sufficient staffing levels. In addition, the service standards address INTERPOL notice and diffusion messaging requirements, including timeliness, accuracy, and responsiveness.

division. In addition, the evaluation includes a review of the opened cases assigned to the division in the previous 12 months. The USNCB's process reviews 1 percent or, at a minimum, two to three cases from each caseworker.⁹¹ The supervisor reviews each selected case to ensure compliance with USNCB guidelines and to ensure that standard case management practices are being followed. If any inaccuracies or errors are identified during the file review, the supervisor must ensure that the errors are corrected. The USNCB believes that through this review it will be able to recognize and correct errors and inaccuracies and identify potential employee training needs.

According to the USNCB, following the first cycle of quality assurance reviews, which occurred during the last half of FY 2008, the USNCB identified several weaknesses in its processing of INTERPOL information and made modifications to its procedures, including requiring supervisory approval prior to the closure of a case. In addition, in February 2009, the USNCB implemented an additional monthly review of its caseworkers.

According to the NCIC operating manual, the USNCB is required to be audited at least once every 3 years by the FBI to verify compliance with FBI policies and regulations. The USNCB was last audited in August 2008 by the FBI and was found to be out of compliance in three areas, including the untimely entry of NCIC records and a lack of a required user agreement with one of its liaison offices.

We believe that the USNCB's implementation of a new quality assurance program is an important step to enhancing the accuracy of its information. The new processes require a more thorough review of cases and more documentation of the reviews completed. They also require more involvement in the review process by division supervisors and assistant directors. The inaccuracies that we identified in USNCB's case files underscore the need for these additional actions to ensure that the information provided by the USNCB is reliable. Therefore, we recommend that the USNCB to continue to conduct the monthly and annual reviews of its caseworkers. In addition, we recommend that the USNCB continue to require ongoing supervisory review of its caseworkers' work products, including supervisory approval of NCIC and TECS records.

⁹¹ The USNCB reported that it opened 24,345 new cases in FY 2008. Therefore, it anticipates that approximately 243 cases will be reviewed during the FY 2009 quality assurance review process.

Conclusion

It is essential that the USNCB make international law enforcement information available in a timely and accurate way to law enforcement personnel and to officials who make decisions about the admissibility of individuals into the United States. We found that the USNCB has not made critical international criminal information available to all appropriate law enforcement agencies, thereby increasing the risk of international criminals entering the United States.

The USNCB relies on manual data entry processes to add, modify, or delete information from each of the U.S. agency databases. This manual data entry process creates delays in entry of information and is susceptible to transposition errors, missed data, and data inaccuracies. During our review, we found that the USNCB has not instituted controls or processes to ensure that the information it has made available to domestic agencies is accurate, complete, or current. Consequently, these systems often contain out-of-date or incomplete data, include information on individuals for whom no law enforcement agency has a current investigative interest, and may violate the other member countries' privacy laws.

While USNCB officials attribute many of the problems and delays in processing INTERPOL information to the need to translate documents, increasing workload, and limited resources, the manual data entry processes they use are overly labor intensive, time-consuming, and prone to errors. The USNCB implemented the manual processes because of the format of the information it receives from INTERPOL and other member countries. To address this weakness, INTERPOL officials in Lyon, France, are working to implement a new standard for the transmission of international law enforcement information. In addition, INTERPOL is in the process of developing a new messaging system for member countries' use that it anticipates will dramatically enhance INTERPOL's and member countries' ability to process and share law enforcement information.

Because the USNCB currently relies on manual data entry processes, the USNCB should ensure that international criminal information, including notices and diffusions, are entered in a timely and accurate manner into appropriate domestic systems such as TECS, NCIC, and CLASS. Additionally, the USNCB should continue to work with the FBI to assess the feasibility of providing all domestic law enforcement officers with access to INTERPOL information through a direct connection with INTERPOL through NCIC using one query.

In addition, to reduce its dependence on manual data entry processes, the USNCB should continue to work with INTERPOL to develop and implement an effective information technology system such as I-Link that will allow the USNCB to electronically add, modify, and delete INTERPOL information from domestic data systems. Pending the results of the feasibility assessment of a direct connection between INTERPOL and NCIC using a single query, the USNCB should assess the feasibility of developing the capability for electronically adding, modifying, and deleting INTERPOL information from domestic systems, including TECS, NCIC, and CLASS.

Recommendations

We recommend that the USNCB:

8. Review current and incoming green notices and determine if they are appropriate for inclusion in NCIC.
9. Modify its policies and procedures regarding notice and diffusion information to ensure that the appropriate data is shared with U.S. agency databases and is made available to domestic law enforcement personnel in a timely manner.
10. Develop procedures to ensure that any additional information the USNCB obtains that augments previously provided domestic law enforcement agency data is made available to all relevant agencies.
11. Provide domestic law enforcement agencies with access to INTERPOL information on stolen and lost travel documents.
12. Work with the FBI to assess the feasibility of developing and implementing a direct connection between the INTERPOL databases and NCIC.
13. Review existing USNCB-generated lookout records to ensure that the notice and diffusion information is accurate and consistent, including those identified by the OIG in this review as being inaccurate or inconsistent.

14. Ensure that the notice and diffusion information retained in DHS's IDENT system and the FBI's IAFIS is compliant with the INTERPOL Rules for Processing Information. The USNCB should also coordinate with DHS and the FBI to implement an agreement regarding the inclusion of fingerprints and photographs in their internal databases. This agreement should describe the type of information to be shared, appropriate uses, retention period, removal requirements, and written confirmation of removal.
15. Develop and implement automated processes to transmit INTERPOL information to U.S. agency systems.
16. Eliminate the backlog of notices and diffusions and develop procedures to regularly monitor the timeliness of workflow processes.

III. CONTROLS OVER USNCB CASE INFORMATION

The USNCB has not developed processes to ensure that subjects of foreign notices or diffusions have not entered the United States subsequent to the receipt of the notice or diffusion. Additionally, the USNCB has not fully developed the capability to identify patterns and evolving trends in criminal activities, such as transnational organized crime. As a result, the USNCB does not use INTERPOL information to its fullest extent. We also identified weaknesses with ENVOY, the USNCB's internal case management system, such as poor record retention and disposal, inappropriate case mergers, inadequate management reporting and statistics, and a lack of audit trails.

USNCB Internal Case Management

As previously discussed, when the USNCB receives domestic and foreign law enforcement agency requests, USNCB analysts are responsible for ensuring that the request is entered into ENVOY, the USNCB's case management system; the necessary entries are made into the other domestic lookout systems; and the case is assigned to the appropriate USNCB division or section. Case workers conduct additional, more extensive queries of domestic databases to provide the analysts with additional information, including:

- immigration status information, such as information on lawful permanent residents, naturalized citizens, violators of immigration laws, and deportees; and
- criminal history, such as prior arrests and convictions.

In addition, if the foreign request or notice relates to drug trafficking or drug seizures, the USNCB analyst may request that a DEA agent detailed to the USNCB query the DEA's Narcotics and Dangerous Drugs Information System (NADDIS).⁹² The analyst also has access to commercial databases to review additional information, including employment history and financial records. If these additional database searches reveal information on the subject that might assist in the investigation or generate a "lead," the case

⁹² The Narcotics and Dangerous Drugs Information System (NADDIS) is a centralized automated file of summaries of reports on 5.9 million subjects of interest to the DEA, including individuals, businesses, vessels, aircraft and selected airfields identified through the DEA investigative reporting system, and related investigative records.

is assigned to an agent within the appropriate USNCB division who will coordinate with the appropriate law enforcement agency for investigation.

According to the USNCB's internal guidance, analysts are required to conduct these additional searches on most foreign-issued notices and diffusions, including red, green, blue, yellow, black, and the U.N. Special notice.⁹³ During our review of a judgmental sample of 115 foreign notices and diffusions active from October 1, 2005, through May 29, 2008, we identified 106 that required additional searches of the databases. Of these 106, we noted that 55 did not have evidence of all of the required queries. In addition, we were told by the supervisor of the Notice Section that as of June 4, 2008, the USNCB had a backlog of more than 2,600 foreign notices and diffusions that required additional searches. We brought these backlogs to the attention of the USNCB Director, who stated that he had been unaware of the backlogs. In response to our inquiry, he adjusted staff assignments, reassigned staff from other sections, and hired two contractors.

USNCB officials also told us that they do not have a process by which they continue to conduct searches of the databases to ensure that the subjects of the foreign notices or diffusions have not entered the United States subsequent to the receipt of the notice or diffusion. The USNCB Director agreed that continuing to attempt to locate these individuals through ongoing investigation was important, but that the USNCB did not have sufficient resources to address this issue.

We believe that these additional queries and searches could provide valuable information for U.S. law enforcement agencies and potentially assist them in identifying, locating, and apprehending these criminals. For example, the subject of a red notice issued by a foreign country could be using a stolen travel document, enter the United States undetected, and establish permanent residency. If the USNCB continued to conduct searches of the databases, the subject might be located once the travel document is reported as stolen.

We agree that conducting individual queries and searches is a time-consuming and labor-intensive endeavor. However, we believe that the USNCB should explore alternative methods that incorporate technology such

⁹³ USNCB analysts do not perform additional queries and searches for orange notices. If a black notice or diffusion contains names, fingerprints, or numbers, such as a passport, which might be used to identify human remains, the USNCB analysts are required to perform additional searches of databases.

as batch queries to ensure these additional queries and searches are performed.⁹⁴

Domestic Case Enhancement

Part of the USNCB's mission is to coordinate and integrate information for investigations of an international nature and attempt to identify international criminal patterns and trends to be more prepared for emergent illegal activities. However, during interviews with USNCB officials, they stated that while the identification of criminal patterns and trends is part of the USNCB's mission, the organization currently does not have sufficient resources to address it. We believe that these are essential functions of the USNCB, and that by not conducting these analyses, significant opportunities are being missed to enhance the usefulness of INTERPOL information.

During our review, we discussed with USNCB officials the potential benefits associated with attempting to determine if the subject of a foreign notice or diffusion is also a person of interest in another domestic law enforcement agency's investigation. For example, the subject of a foreign red notice who is wanted for drug trafficking may also be a person of interest in a money laundering investigation being conducted by the FBI.

USNCB officials agreed that it would be beneficial to query other agency databases (such as the FBI's or DEA's case systems) to determine if other U.S. law enforcement agencies had an interest in the subject of a notice or diffusion. However, they stated that with just 4 analysts assigned to the Notice Section, and with each analyst managing approximately 7,000 notices and diffusions, the USNCB did not have sufficient resources to perform such queries. Moreover, the USNCB Deputy Director stated that the USNCB would need increased access to other agency databases, including those operated by the FBI and DEA.⁹⁵

In addition, USNCB officials stated that they believed that analyzing INTERPOL information for potential patterns and trends in criminal activities could provide valuable insight into evolving patterns of transnational organized crime. In turn, this information could be shared with law enforcement agencies in the United States to better prepare them to address emerging trends in transnational crime, including gang activity and human trafficking. However, the USNCB officials told us that they have not

⁹⁴ A batch query is a method by which electronic records are searched automatically.

⁹⁵ Currently, access to each agency's database is restricted to employees of the agency. For example, only FBI employees stationed at the USNCB may access the FBI's case management system.

attempted to develop the capability to accomplish this portion of the USNCB mission because they lack sufficient resources.

We discussed these issues with the Office of the Deputy Attorney General (ODAG) official responsible for overseeing USNCB matters. He agreed with our assessment and acknowledged the potential value of determining if other U.S. law enforcement agencies have an interest in the subject of a notice or diffusion. The ODAG official stated that he believed that the USNCB should have access to other agency systems, including FBI and DEA systems, to determine whether individuals who are the subject of a foreign notice or diffusion also are identified in a U.S. case. Moreover, this official stated that he believed that the USNCB should work to develop the capability to use the INTERPOL information to identify international criminal activity trends and that it made sense to “connect the dots.” However, he said he was uncertain as to whether the Department had any plans to develop such a capability.

Combining Case Information

USNCB analysts told us that they close cases in ENVOY when a notice or diffusion is cancelled. If a new notice or diffusion is issued that appears to match the subject of a closed case (name, date of birth, and country of origin), the analysts re-open the original case and append the new information to the re-opened case. However, the new information could potentially pertain to an unrelated individual who possesses similar identifying information, such as the name, date of birth, and country of origin. As a result, the analyst could unknowingly associate the criminal information from one individual with a completely unrelated person. Further, a USNCB official told us that once the documentation is combined into one case file it is extremely difficult to separate.

When we discussed with the USNCB Deputy Director the USNCB analysts’ practice of re-opening closed cases, he acknowledged that the practice is a significant weakness. He expressed concern that this practice could result in a domestic law enforcement agent attempting to support a warrant request based on a conviction associated with another individual.

The USNCB Compliance Officer told us that they have the ability to create multiple cases on the same individual in ENVOY and link them together, but they do not do so because they believe that matching the name, date of birth, and country of origin is sufficient to ensure that it is the same individual. We believe that these three pieces of information provide the basis for determining that the cases might *potentially* be related. However, we believe that additional information such as fingerprints and

photographs should be used to make a definitive determination. Therefore, we believe that the USNCB should only add information to an existing case if additional information confirming the identity of the subject, such as fingerprints and photographs, is available. In the absence of this additional information, we believe the USNCB should open a new case on the subject and establish a link to the original case.

Records Management

The USNCB uses ENVOY, a computer database, to maintain and organize documents related to requests from law enforcement agencies for assistance or information from the international community, including notices and diffusions. ENVOY is intended to provide the USNCB with records management, workflow management, automated workflow processes, and records search and reporting capabilities.

ENVOY was initially implemented in 1999 to replace the USNCB's previous case management system - the INTERPOL Case Tracking System. According to the USNCB CIO, the initial deployment of ENVOY did not provide the full functionality required by the USNCB. As a result, the USNCB experienced significant operational issues with the initial version of ENVOY, including system instability, a lack of software documentation, and limited reporting capability. In addition, because of the lack of reporting capability, USNCB officials said they have experienced significant problems tracking basic workload statistics, including the number of active notices and diffusions. When the USNCB sought to correct these issues, the original developer was no longer in business, so the USNCB hired a second contractor.

According to the USNCB CIO, the second developer prepared system documentation that conformed to industry standards, as well as identified and addressed some system weaknesses, including instability and reporting. However, the USNCB CIO stated that the USNCB has not been able to address all of the ENVOY issues at one time because of limited funding. He said that as a result, the USNCB has adopted a phased approach and has made incremental improvements to ENVOY. In addition, because of the lack of funding available to create a more enhanced automated reporting capability, the USNCB CIO stated that he has developed several management reports. However, he stated that he has been unable to develop all of the required reports because of limited IT staff resources.

During our review, we observed the operation of ENVOY and examined a sample of 216 cases selected from notices and diffusions active from

October 1, 2005, through May 29, 2008.⁹⁶ In general, we noted the USNCB case files in ENVOY were disorganized and inconsistently assembled, and we identified a transposition error, missing data, and duplicate entries. We also found documents that were filed in the wrong case file. We identified three instances in which information pertaining to two unrelated individuals appeared to have been erroneously combined into a single case file. We also identified instances in which cases were improperly classified within ENVOY. Most importantly, we identified poor record retention and disposal, inappropriate case mergers, inadequate management reporting and statistics, a lack of audit trails, and inadequate standardized correspondence, as discussed below.

Record Retention and Disposal

In compliance with the Privacy Act of 1974, the USNCB has published a Systems of Records Notices (SORN) in the *Federal Register*.⁹⁷ The SORN outlines the USNCB's policy for the types of individuals reflected in its records, data collected, reason for data collection and safeguards of the data, rules and purposes for which the data may be shared, and guidelines for data retention and disposal.⁹⁸ The USNCB's SORN for its internal case information states that it will retain on-site paper and electronic records of case files for 2 years after closing the case.⁹⁹ After 2 years, the SORN states that records will be archived and stored at an off-site facility. The documents can be destroyed if there has been no case activity 5 years after the transfer, for a total retention period of 7 years following closure of a case. The SORN also states that any automated information will be identified as an archived case and maintained on the USNCB local area network (LAN) server for an indefinite period.

The USNCB Compliance Officer said that some USNCB files have been archived and stored off site. However, she could not recall the last time the USNCB sent paper records to the off-site facility. Further, the Compliance Officer stated that there were numerous boxes of paper case files currently located in the USNCB hallways. In addition, she could not recall the date

⁹⁶ For a detailed description of our methodology, see Appendix I.

⁹⁷ Privacy Act of 1974 (5 U.S.C. § 552a).

⁹⁸ According to its Privacy Threshold Assessment, the USNCB's systems were not subject to the requirement under the E-Government Act of 2002 (Act) to conduct a Privacy Impact Assessment because its systems were developed prior to the Act's effective date and its systems had not undergone significant changes since then.

⁹⁹ The USNCB's SORN provides retention and disposal guidelines for cases closed on or after April 5, 1982.

that a USNCB case was last destroyed at the off-site facility and stated that the USNCB had not archived any of the electronic information contained within ENVOY. As a result, ENVOY contains information from all USNCB cases dating back to when the USNCB first automated its case files in 1979.

The USNCB needs to manage its case-related information to ensure that the information is easily and readily available throughout the USNCB. Leaving boxes of paper records lying unattended in uncontrolled hallways leaves the records vulnerable to loss, damage, and review by unauthorized personnel. These paper records should be adequately maintained, controlled, and disposed of when appropriate.

We believe it is also important that electronic records are protected from loss and unauthorized review. However, the USNCB CIO told us that all authorized users of ENVOY have unrestricted access to all case files.

We discussed the USNCB record retention and disposal issues with a USNCB official, who stated that they have not archived paper records in recent years because of a lack of personnel. According to the USNCB Director, as the United States' obligation for INTERPOL dues increased, the USNCB was forced to reduce the number of administrative personnel. The USNCB Director stated that the USNCB had hired a new administrative officer in August 2007 to assist with records management and other administration functions.

According to the USNCB CIO, the USNCB has not archived its electronic records because the current version of ENVOY is not designed to perform case archiving. The USNCB CIO stated that the USNCB recognizes that its case management system should facilitate the ability to archive its outdated or obsolete electronic case information. He said that he anticipates that the USNCB will incorporate this functionality into future versions of its case management system.

We recommend that the USNCB develop a case management system that ensures that its case-related information is easily and readily accessible to authorized personnel throughout the USNCB. In doing so, the USNCB should implement procedures to control access to the information to prevent loss, as well as to preserve the privacy of individuals on whom the information is maintained. Further, the USNCB should develop policies for the routine archiving and destruction of its cases as outlined in its SORN. In addition, it should review its paper case files and electronic cases in ENVOY to determine whether they need to be archived, stored, or destroyed.

Management Reporting and Statistics

According to the USNCB CIO, when a new case is opened in ENVOY the software application assigns a sequential case number, as well as the date and time the case was opened. During our review of a judgmental sample of notices and diffusions active from October 1, 2005, through May 29, 2008, we identified several anomalies related to the system dates recorded for key events of the cases, including the date the case was opened. Specifically, of the 216 cases we examined, 6 cases appeared to have been opened before the USNCB received the notice or diffusion leading to it opening a case. For example, we noted that the date that the USNCB received and processed one notice was December 9, 2007. The date that the system recorded that particular notice was 2 days earlier – December 7, 2007. Although the difference of 2 days in this example may seem insignificant, the fact that this can occur in the USNCB's primary recordkeeping system may indicate that there are other cases with significantly longer gaps of the same nature. We discussed this issue with the USNCB Compliance Officer and CIO who stated that they believed these anomalies occurred because of the USNCB's practice of reusing case numbers.

The reuse of case numbers also affects the USNCB's ability to track the number of new cases opened and closed each year. According to the CIO, ENVOY has limited reporting capabilities and the system cannot generate accurate information on the number of new cases opened and closed by the USNCB each year. As a result, the USNCB developed an alternative process by which it counted the number of new cases by utilizing the sequential system case number.

However, to ensure effective management the USNCB needs a case management system that allows it to compile basic workload statistics, such as the number of cases opened. In addition, the system should track the time elapsed between key events in its case processing, such as when the USNCB receives a notice or diffusion, when the case is opened, and when lookout records are entered.

We believe that the USNCB would benefit from regularly tracking and monitoring the time elapsed between these key events to ensure that it is processing information in a timely manner. Further, by tracking and analyzing these statistics, the USNCB would be able to measure its progress against pre-determined performance objectives and identify potential process weaknesses. Therefore, we recommend that the USNCB design and implement a case management system that is capable of providing reliable workload statistics.

Audit Trails

ENVOY does not provide for tracking and retaining historical transactions within its database. As a result, the USNCB is unable to determine which actions were performed by which analyst or supervisor. We believe that these audit trails, including historical data and detailed transactions by users, could help ensure that the information is properly used in conformance with INTERPOL and USNCB policies.

Standardized Correspondence

To ensure that the information it provides to foreign and domestic law enforcement agencies is consistent with the statutes of the INTERPOL Constitution, U.S. laws, and the provisions of the Freedom of Information and Privacy Acts, the USNCB has provided guidance to its personnel on what information may be released and under what circumstances. In addition, the USNCB has designed standardized templates for its analysts to use when preparing routine correspondence. According to the USNCB Compliance Officer and the CIO, USNCB analysts can automatically generate this standardized correspondence. In addition, the electronic process saves a copy of the correspondence to the case file.

During our review of the 216 USNCB notices and diffusions, we noted that frequently the case file contained multiple copies of the same USNCB-prepared correspondence. We identified numerous instances in which the case files contained three similar versions of a USNCB-prepared diffusion. When we discussed this issue with the USNCB Compliance Officer, she stated that the USNCB was aware that the electronic process generated and saved three similar, but not identical, versions of the diffusion correspondence to the case file.

Saving multiple copies of the same or similar documents to the case file can be confusing to USNCB investigators and analysts and may result in delays during investigations. For example, investigations may be delayed while analysts attempt to determine which version of the document contains the most accurate and current information. The USNCB Compliance Officer stated that the process also hampers her ability to obtain accurate management statistics regarding the total number of diffusions processed in a given period.¹⁰⁰

¹⁰⁰ Because the electronic process generates three versions of a diffusion, it overstates the total number of diffusions processed in a given period. To compensate for the overstatement of diffusion correspondence, the USNCB Compliance Officer stated that she divides by three the total number of diffusions processed in a given period.

Further, USNCB officials said that the analysts are not required to use the standardized templates. Several analysts stated that they do not use the electronic processes and have developed their own templates for routine correspondence. As a result, the diffusions generated by the USNCB analysts are not in a consistent and standardized format and therefore may not contain the information necessary to conduct an investigation or to comply with statutes of the INTERPOL Constitution, U.S. laws, and the provisions of the Freedom of Information and Privacy Acts.

New Electronic Case Management System

In FY 2007 the USNCB began to explore alternative software applications to manage its case information, and in 2008 selected a commercial off-the-shelf application. The USNCB CIO said that the new application will be relatively easy for USNCB employees to learn because it uses the same operating system and programming as the one currently used for other functions. The USNCB CIO wanted also to minimize the USNCB's cost for initial software, upgrades, and software maintenance by utilizing an existing DOJ contract with the vendor.

In May 2008 the USNCB received an initial planning document for the implementation of the new case management software. This document contained the USNCB's general vision for and scope of the project, but it did not contain specific details regarding the software features, cost, and delivery schedule. The document stated that it was not a legally binding contract and that future revisions to the document would provide the specific details of the project.

At that time, the USNCB reported that it expected that the new case management system would be deployed by December 2008. In November 2008 we asked the USNCB to provide us with its formal planning documents, including a description of the project, timelines, milestones, and costs. On November 12, 2008, the USNCB CIO stated that the initial planning document was the most current and accurate information he possessed. In January 2009, the USNCB CIO informed us that deployment of the new case management system had been delayed because of other IT priorities. As a result, the USNCB reported that it anticipated its new system to deploy by the end of February 2009. In April 2009, the USNCB stated that it had resolved several technical difficulties that were encountered during development, and after hiring an additional developer to help expedite the delivery schedule, officials said they anticipate that the upgrade will be completed by mid to late August 2009.

The USNCB needs to develop a case management system that provides it with the ability to easily manage the information in its possession and generate reliable workload statistics. The system should include processes and procedures to monitor access to its information to prevent loss and unnecessary access. The case management system should also provide the USNCB with the ability to examine the international information to assist with investigations and identify trends and patterns in crime.

Since the initial deployment of ENVOY in 1999, the USNCB has struggled to adequately plan and implement a case management system that provides it with such full functionality. As a result, the USNCB has been hampered in its ability to protect information, provide management statistics, and provide its domestic and international law enforcement partners with accurate, reliable, and consistent investigative case information. We have significant concerns with implementation of the new system, such as the USNCB's continued lack of formal planning documents containing a description of the project, timelines, milestones, and costs. We believe that the USNCB should consider obtaining an independent evaluation of the new system and whether it will meet the USNCB's needs. We also believe the problems experienced with this implementation underscore the USNCB's need for a comprehensive plan for determining the agency's future IT investment needs.

Conclusion

The USNCB has not conducted searches of domestic databases to ensure that subjects of foreign notices or diffusions have not entered the United States. In addition, the USNCB has not developed a process for the ongoing review of domestic databases to locate subjects of foreign notices or diffusions subsequent to the receipt of the notice or diffusion. Further, the USNCB has not developed processes to help domestic law enforcement agencies determine if the subject of a foreign notice or diffusion is also a person of interest in the domestic law enforcement agencies' case files. As a result, individuals that are wanted in another country may enter the United States and evade prosecution. Moreover, we believe that these deficiencies result in missed opportunities to investigate and solve crimes committed in the United States by subjects of foreign notices and diffusions.

We identified significant weaknesses with the USNCB's processes and controls related to its case management. These deficiencies have diminished the USNCB's ability to dispose of documents according to its records schedule, generate management statistics, audit individual user activity, and ensure that its communication with other law enforcement agencies is consistent, accurate, and complete.

Recommendations

We recommend that the USNCB:

17. Review all active notices and diffusions to ensure that appropriate database searches have been conducted.
18. Develop and implement policies and procedures, including technological solutions, to determine if subjects of INTERPOL notices and diffusions have entered the United States subsequent to the receipt of the notice or diffusion.
19. Develop a formalized process to ensure that searches of federal law enforcement agency databases have been conducted on subjects of foreign notices or diffusions to determine if they are persons of interest to these agencies.
20. Develop the capability to use INTERPOL information to identify trends and patterns in international criminal activities, such as transnational organized crime.
21. Develop procedures to ensure that information is added to an existing case only if additional information is available to confirm the identity of the subject, such as fingerprints and photographs. In the absence of this additional information, a new case on the subject should be opened and linked to the original case.
22. Ensure that its case management system provides the ability to:
 - (a) adequately maintain, control, and dispose of case-related information, including access restrictions by user and audit trails;
 - (b) compile management statistics; and
 - (c) generate standardized correspondence.

IV. USNCB MISSION AND PRIORITIES

The Department has not provided adequate supervision and oversight of the USNCB. The USNCB Executive Committee, composed of senior DOJ officials, has not met in more than 5 years and therefore has not evaluated or updated the USNCB's strategic plan to ensure that it is consistent with current DOJ priorities; that its IT investments are appropriate; or that the USNCB is adequately staffed. Additionally, DOJ has not undertaken any evaluation of the USNCB to ensure that its executive positions are at the appropriate pay level and that these positions are attracting the most qualified candidates.

Strategic Needs of the USNCB

As discussed earlier, we determined that the USNCB has missed opportunities for sharing INTERPOL information or taking advantage of evolving technology to improve its operations. We attribute these weaknesses, in part, to DOJ's and DHS's inadequate oversight of the USNCB and lack of assistance in developing a meaningful vision for the role and mission of the USNCB. We identified several areas that require attention to ensure that the organization fulfills its important mission, including department-level support and oversight, USNCB executive leadership, strategic planning, information technology, and resources (particularly staffing and funding).

Department-level Support and Oversight

In May 2003 DOJ and DHS signed an MOU establishing the USNCB as a separate component of DOJ under the supervision of the Deputy Attorney General. The MOU established an Executive Committee consisting of the Deputy Attorney General, Deputy Secretary of DHS, and the USNCB Director, which would meet semi-annually and make policy and personnel decisions, except those delegated to the Director, relating to the USNCB. However, according to the ODAG official responsible for USNCB matters, the Executive Committee has not met for at least 5 years.

The ODAG official we interviewed acknowledged that the USNCB has not received sufficient guidance and support from the USNCB Executive Committee. He attributed many of the deficiencies we identified in this review, in part, to this general lack of support and supervision. This official also stated that he believed that DOJ had failed to maintain its oversight of the USNCB because of significant levels of turnover in the ODAG. He told us that DOJ is working to arrange a meeting of the Executive Committee to

begin addressing these issues. The ODAG official stated that he believed that the “full support of the ODAG” should be sufficient to address the weaknesses that we had identified during this audit.

While we believe that the Executive Committee’s oversight of the USNCB can help to improve USNCB functions, we also have concerns related to the current USNCB leadership structure that we discuss below.

USNCB Executive Leadership

Since the USNCB’s inception, advances in technology have provided criminals with the ability to operate unconstrained over national borders. Since the terrorist attacks of September 11, 2001, these advances in technology also have provided significant opportunities for the international law enforcement community to enhance border security by electronically sharing terrorism and other criminal information. As a result, the role and function of the USNCB has become more complex.

Further complicating the USNCB’s mission is its need to comply with the INTERPOL RPI. INTERPOL requires that NCBs ensure that international criminal and terrorist-related information is used in compliance with its RPI, which USNCB officials explained takes into consideration member countries’ privacy laws. For example, INTERPOL officials in Lyon, France, told us that Germany severely limits the length of time that records on its citizens may be retained. As a result, the USNCB should ensure that it retains and disseminates information provided by German law enforcement in accordance with the RPI. Moreover, INTERPOL requires that the NCBs review any databases with which INTERPOL data is shared to verify compliance with INTERPOL’s RPI. As a result, the USNCB must ensure that the information it disseminates to other law enforcement agencies is accurate, complete, and complies with the INTERPOL RPI. With 187 INTERPOL member countries and over 18,000 domestic law enforcement agencies, the USNCB experiences unique challenges in sharing international criminal and terrorism-related information across all levels of government and with foreign countries.

However, we believe that the current framework for identifying, selecting, and hiring the Deputy and Director positions may hamper the USNCB’s ability to attract the most qualified individuals to meet its evolving mission. Specifically, the USNCB senior management positions rotate between DOJ and DHS every 3 years, and the USNCB Director must be from a different department than his or her predecessor and the Deputy

Director.¹⁰¹ When the Director's term concludes, the Deputy Director assumes the Director position.

We were told by a senior FBI official that the current 6-year rotational structure presented two issues regarding compensation and career advancement that reduced the attractiveness of the USNCB position to well-qualified, experienced FBI employees. Under the present format, the USNCB Director position is a term appointment at the Senior Executive Service (SES) level, while candidates for the Deputy Director position must be "SES-eligible."¹⁰² As a result, an agent in the USNCB Deputy Director position would spend at least 3 years at the GS-15 level before achieving a term-SES appointment. Therefore, well-qualified agents at the FBI, as well as those from other federal law enforcement agencies, may be unwilling to commit to being the USNCB Deputy and then USNCB Director – for a total of 6 years – because they would then revert back to a GS-15 position at their home agency after 6 years.

In addition, the disparity in rank between the USNCB Director and Deputy Director and other DOJ and agency executives with whom they interact contributes to the perception that the role and function of the USNCB is less important than those of other agencies. The rotational nature of the Director and Deputy Director positions also contributes to a lack of continuity in historical knowledge, planning, and budget formulation.

We discussed these issues with the Secretary General of INTERPOL, who is a former high-ranking U.S. law enforcement official. He agreed with our assessment and stated that, in his opinion, the Director of the USNCB should be a presidential appointee.

When we discussed this issue with the ODAG official, he stated that the "full support of the ODAG" should be sufficient to address any of the weaknesses that we identified in the perceived disparity in rank for the USNCB Director and other DOJ and agency executives. The ODAG official noted that not all agency Directors are presidential appointees and some, such as the Director of the Executive Office for United States Attorneys (EOUSA), still have significant influence.

¹⁰¹ The current Director is a Supervisory Special Agent with DHS's U.S. Immigration and Customs Enforcement and the Deputy Director is a Chief Inspector with DOJ's U.S. Marshals Service.

¹⁰² The SES is a corps of public servants who administer programs at the top levels of federal government. SES Positions are primarily managerial and supervisory. The USNCB does not have a separate SES allocation from either DOJ or DHS. Directors must bring an SES allocation from their home agency.

Nevertheless, we believe that the position of USNCB Director should be of high enough rank to attract high quality candidates and provide the Director with the ability to make effective changes in the USNCB. Moreover, we do not believe that the current term-SES arrangement and rotational structure provides either the necessary enticement or the needed seniority to achieve these ends. We recommend that DOJ, in conjunction with DHS, evaluate options to enhance the executive management structure of the USNCB.

Strategic Planning

The USNCB current strategic plan covers FYs 2005 through 2010. Senior USNCB officials told us that they struggled to perform adequate planning because they lacked sufficient resources to manage USNCB's day-to-day operations. As a result, the officials stated that they did not approach the strategic planning process as seriously as they would have liked.

We found that the USNCB strategic plan includes some of the essential components of a strategic plan, such as strategic objectives, but lacks a comprehensive vision or a strategic direction for the USNCB, and it is difficult to assess the suitability of each of the stated objectives.

The USNCB's present functions most closely align with DOJ's Strategic Goal II to "prevent crime, enforce the federal laws, and represent the rights and interests of the American people." However, because transnational crime has been linked increasingly with terrorism and INTERPOL has expanded its role in sharing terrorism-related information, we believe the USNCB strategic plan should also address the relevant aspects of DOJ's Strategic Goal I to "prevent terrorism and promote the nation's security."

In our opinion the USNCB strategic plan also does not adequately address the USNCB's role in sharing international criminal and terrorism-related information across all levels of government, the private sector, and the international arena in a timely, accurate, and complete manner. As discussed above, the role and function of the USNCB have become more complex due to improvements in technology, the need to comply with the INTERPOL RPI, and the government's increased emphasis on border screening. We believe that more rigorous strategic planning efforts will assist the USNCB in achieving its mission and identifying which improvements are most critical.

We recognize that the USNCB, as currently constituted, may not be capable of initiating these planning efforts, and we attribute many of the

deficiencies with the USNCB's strategic planning to the lack of Department-level oversight and support. We believe it essential that the Executive Committee meet at least semi-annually, as prescribed in the MOU, and that it take the lead in developing a new strategic plan that recognizes the USNCB as the primary U.S. agency responsible for information-sharing with foreign criminal justice agencies.

The USNCB strategic plan should be a formal written document that addresses all aspects of organizational and resource planning, management, and performance measurement and does so in consideration of DOJ's strategic goals and the USNCB's contributions to the achievement of those goals. It should also provide specific strategies and timelines for accomplishing the USNCB's overall mission and specific methods for measuring achievement and performance.

Information Technology

The USNCB's management of its information technology (IT), a critical part of its ability to achieve its mission, has been deficient. Because the USNCB has not had a clear vision for its current operations or how it intends to operate in the future, its planning for IT functions has been unstructured and performed on an ad-hoc basis.

The USNCB CIO stated that he has struggled to adequately plan for IT development because the USNCB's funding for IT initiatives has been inconsistent. According to JMD's 2004 report, the USNCB budget requests for IT initiatives during FYs 2000 through 2004 failed to "make the case for how its IT enhancement request supported its own or DOJ's program goals."¹⁰³ JMD acknowledged that the USNCB's FY 2005 budget request had improved. However, the USNCB's most recent IT strategic plan is dated August 12, 2005, and outlines initiatives that were to be accomplished in FY 2005. With an IT strategic plan that we believe is outdated and a history of poorly prepared budget submissions, it is hard for the USNCB to develop and support an adequate budget request that sufficiently addresses needed IT improvements. Moreover, considering the pace of technological development and the USNCB's need to incorporate additional technology in its process, the USNCB must anticipate its future IT needs and plan accordingly.

We believe that the USNCB would benefit from establishing a formal written document that systematically addresses IT organizational and resource planning, management, and performance measurements. In

¹⁰³ JMD, *Management Review of INTERPOL - USNCB*, 12.

conjunction with the USNCB's strategic plan, the IT strategic plan should evaluate current operations and uses of data and account for the various ways in which INTERPOL information might potentially be used and accessed by other agencies. In addition, the USNCB should more often review the data in its possession and determine how different pieces of data can be combined to provide more useful information.

This plan should also combine in one document the USNCB's plans regarding its current and future IT needs. The plan should address systems interconnectivity and controls to ensure data integrity systems engineering and architecture planning, application development, project management, and resource planning (such as budget, staffing, and facilities).

Staffing Needs

The USNCB has an authorized staffing level of 65 permanent, full-time equivalent positions, and throughout its existence the USNCB has been heavily dependent upon additional staff detailed from participating agencies. Officials at the USNCB stated that having detailees who can apply their investigative skills to assist law enforcement agents is important to the mission of the USNCB. Further, the detailees serve as their home agencies' liaisons and provide invaluable agency-specific expertise.

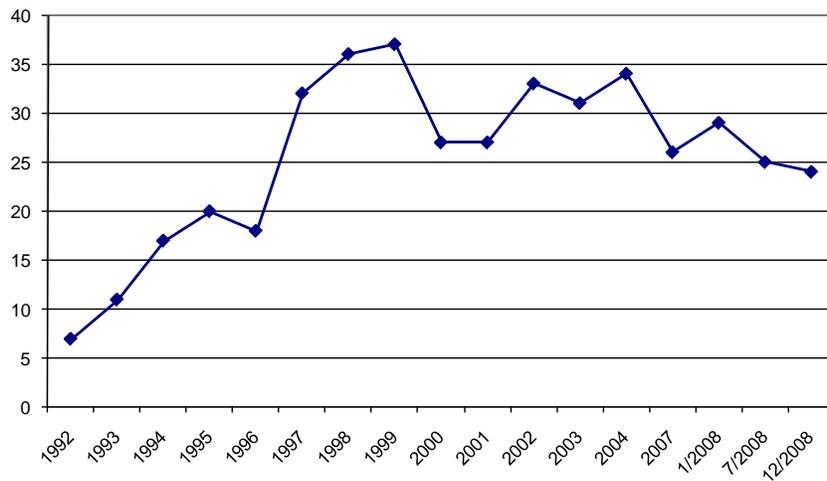
Historically, the USNCB had agreements with law enforcement agencies regarding the number of detailees that each agency would provide, and staff was assigned to the USNCB from these agencies for terms of 1 to 2 years. However, the USNCB Director said that law enforcement agencies have opted to discontinue the formal agreements, citing budget constraints and a desire to have greater control over their detailees. The USNCB Director also said that the law enforcement agencies have not been assigning as many staff to the USNCB as they had in prior years, and consequently the USNCB is understaffed.

Before the creation of DHS, the former Immigration and Naturalization Service detailed two staff with immigration expertise to the USNCB. In addition, the former U.S. Customs Service also detailed two staff with customs and border protection experience. However, as of July 2008 only one person was detailed to the USNCB from CBP.¹⁰⁴ Further, according to the USNCB Director, the FBI historically has maintained four staff at the USNCB. However, as of July 30, 2008, the FBI had just one agent detailed

¹⁰⁴ In July 2008, CBP assigned two additional staff on a temporary basis to assist with the increased workload.

to the USNCB.¹⁰⁵ The USNCB Director expressed frustration that despite frequent requests the agreed-upon personnel have not been detailed to the USNCB. As shown in Exhibit 4-1, the number of detailees assigned to the USNCB has fluctuated from a high of 37 in 1999 to the current low of 24 staff, which is lower than the number of detailees just prior to September 11, 2001.¹⁰⁶

EXHIBIT 4-1
Number of Staff Detailed to the USNCB
1992 Through 2008¹⁰⁷



Source: USNCB

The rotating nature of much of the USNCB's staff and its inability to rely on longer-term staffing projections has had a significant impact on the USNCB's performance and continuity of operations. The frequent rotation of staff reduces the USNCB historical knowledge of its own organization and initiatives. For example, we identified an instance where a USNCB staff member with whom we spoke was unable to provide us with the requested background information regarding a prior initiative that had been supervised by a former agency detailee. In addition, short temporary duty assignment periods force the USNCB to continually train and orient new personnel.

¹⁰⁵ In December 2008, one additional FBI personnel was detailed to the USNCB and two FBI personnel are currently assigned to the USNCB.

¹⁰⁶ In addition to assigning detailees to the USNCB, as of August 28, 2008, the United States had eight individuals, separate from the USNCB, assigned to INTERPOL. These detailees are located at the INTERPOL General Secretariat in Lyon, France, as well as the INTERPOL office located at the United Nations.

¹⁰⁷ The USNCB was unable to provide data for 2005 and 2006.

We discussed this issue with the ODAG official, who agreed with our assessment. The ODAG official stated that the USNCB, with the assistance and support of the ODAG, would work to establish formal agreements regarding staffing commitments and length-of-duty assignments from the various agencies.

In September 2008, the USNCB Director told us that he had recently met with the USMS Director, who agreed to increase the USMS's USNCB staffing commitment to four. In addition, the USNCB has approached CBP regarding implementing an MOU. According to the USNCB, in August 2008 the DHS Citizenship and Immigration Services (CIS) assigned one person to the USNCB and another to the INTERPOL General Secretariat in Lyon, France.

Funding the USNCB

As shown in Exhibit 4-2, in FY 2009 the USNCB's overall budget was approximately \$24.5 million, of which \$8.2 million went to pay the United States' membership dues to INTERPOL. In addition, we found that several other factors have impacted the USNCB's operational budget and the USNCB's ability to perform critical functions.

**EXHIBIT 4-2
USNCB Funding for Operations and INTERPOL Dues**



Source: USNCB and INTERPOL

Specifically, as a result of a change in the formula used by INTERPOL to calculate each member country's dues, the U.S. commitment for INTERPOL dues (as a percentage of its overall budget) increased by

10 percent, from \$1.7 million in FY 2001 to \$8.2 million in FY 2009.¹⁰⁸ In addition, INTERPOL requires that member countries pay their dues in euros. Since 2002, the dollar has generally declined in value relative to the euro, resulting in an effective increase in the United States' contribution to INTERPOL. As a result of the INTERPOL dues increases, the conversion from dollars to euros, and the decline in value between the dollar and euro, the USNCB's budget for operations, as a percentage of its total budget, has declined from 77 percent in FY 2001 to 67 percent in FY 2009.

In its 2004 report, JMD noted that inclusion of the United States' commitment for INTERPOL membership dues within the USNCB's appropriations had an adverse impact on the USNCB's operations.¹⁰⁹ JMD recommended that DOJ request approval from the Office of Management and Budget (OMB) and Congress to move the dues appropriations into a budget account separate from the USNCB appropriations.

According to the USNCB Director, the decline in its operating budget has affected the organization's ability to address several critical functions, including strategic planning and information technology development. The USNCB Director stated that he lacked sufficient staff to accomplish adequate planning in addition to the day-to-day operational tasks. Moreover, at the same time the number of employees detailed from other agencies has decreased, the reduced operating budget has increased the USNCB's dependence on these detailees.

A USNCB official said the USNCB continues to work with the JMD budget staff and OMB to develop the best method to pay for the United States' membership dues to INTERPOL. However, despite the adverse impact on its ability to perform its operation, a USNCB official stated that the USNCB does not anticipate a solution until at least FY 2011.

¹⁰⁸ INTERPOL's operations are primarily financed by member-country annual statutory contributions. To assess each member country's dues contribution, INTERPOL uses a formula based on each country's economic well being. This formula was renegotiated in the late 1990s and incorporated a gradual increase in the percentage share paid by the wealthiest nations. The U.S. share of the annual INTERPOL budget increased from 5 percent to 13.26 percent over 4 years, reaching the full negotiated dues contribution rate of 13.26 percent in FY 2006. In June 2009 the USNCB informed us that an increase in INTERPOL dues is expected to be passed in October 2009 at the annual General Assembly. If passed, the United States' contribution will be gradually increased from 13.26 percent in 2009 to 17.385 percent in 2014.

¹⁰⁹ JMD, *Management Review of INTERPOL - USNCB*, 10.

Conclusion

After the terrorist attacks of September 11, 2001, the United States enhanced its screening practices to attempt to prevent terrorists and other criminals from obtaining visas or entering the United States illegally and identify and apprehended criminals within the country. Despite its important role in these efforts, we found that the USNCB has not received adequate supervision or oversight from either DOJ or DHS. The executive committee that was created to provide guidance to the USNCB has not met in more than 5 years, and no evaluation of the USNCB's management structure has been performed to ensure that these positions are attracting the appropriate candidates. Additionally, because of the USNCB's rotational management structure, its executive officials have struggled to perform essential strategic and IT planning while managing day-to-day operations. Further, increasing INTERPOL membership dues and the USNCB's inability to rely on staffing projections has had a significant impact on the amount of resources available to the USNCB.

Recommendations

We recommend that the Office of the Deputy Attorney General:

23. Ensure that the Executive Committee meets as prescribed in the MOU and takes the lead in developing a new strategic plan for the USNCB.
24. Evaluate options to enhance the USNCB's executive management structure to help ensure identification of the most qualified candidates for its senior executive positions. Potential enhancements might include adopting a higher-ranking level for the Director and Deputy Director positions, eliminating the practice of the Deputy Director succeeding the outgoing Director at the end of the 3-year term, and revising the term length.
25. Determine the best method to budget and pay for the United States' membership dues to INTERPOL to help minimize the operational impact on the USNCB.

We recommend that the USNCB:

26. Develop a formal IT plan that systematically evaluates current operations and uses of data and accounts for the various ways in which INTERPOL information might potentially be used and accessed by other agencies. This plan should address: (a) IT

staffing needs, (b) controls to ensure data integrity, and (c) future improvements in the areas of database inter-connectivity.

27. Work to develop formal agreements with domestic federal law enforcement agencies regarding staffing commitments and length-of-duty assignments.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Objectives

Our objectives for this audit were to: (1) evaluate the USNCB's efforts to ensure participation and the sharing of INTERPOL information among federal, state, local, and tribal law enforcement agencies; (2) review the USNCB's processes for the exchange of INTERPOL information to ensure that requests for assistance and information were handled in an appropriate, efficient, and timely manner; (3) review the USNCB's controls over INTERPOL case information; and (4) examine the USNCB's organizational role and strategic priorities to ensure that they are in line with DOJ priorities.

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 objectives.

In general, our audit covered but was not limited to the period of fiscal years (FYs) 2006 through 2008. Our testing included selecting judgmental samples of various records. Our sample selection methodologies were designed to give us broad exposure to different types of notices, diffusions, and other activities, but were not designed with the intent of projecting our results to the populations from which the samples were selected.

To accomplish our objectives, we conducted work primarily at the USNCB of INTERPOL located in Washington, D.C. We interviewed USNCB employees, as well as contractors and representatives from various participating agencies working within the USNCB. We met with the representative from the Office of the Deputy Attorney General, who was the DOJ official responsible for USNCB matters, at DOJ headquarters, also in Washington, D.C., to obtain the Department's perspective on the USNCB. Additionally, we interviewed representatives from other federal law enforcement agencies, such as the FBI and DEA, to gain their perspective on the role and mission of the USNCB. We interviewed representatives from two USNCB state and local liaison offices, including the New York State Police Department and the Chicago Police Department. We also interviewed the Secretary General of INTERPOL, as well as other officials at the INTERPOL General Secretariat located in Lyon, France. We visited the

German NCB in Wiesbaden, Germany, and met with the German federal law enforcement officials who were responsible for INTERPOL-related activities.

Additionally, we analyzed data and conducted testing to assess the USNCB's efforts to ensure domestic cooperation and participation, control over the exchange of INTERPOL information, processes to coordinate information to assist with case investigations, and ability to successfully achieve its mission. To obtain an overall understanding of the USNCB's role and responsibilities, we reviewed legislative material, as well as manuals, policies and procedures, memoranda, correspondence, and electronic communications related to INTERPOL. We also reviewed and collected various records and documents as needed, including financial documents, strategic planning documents, workload data, prior audit reports, and reports to Congress.

Cooperation and Participation

To evaluate the level of cooperation, participation, and information sharing between the USNCB and its partner agencies, we reviewed the USNCB's efforts to ensure domestic law enforcement agency access to INTERPOL databases. In addition, we distributed a questionnaire to all 66 state and local USNCB liaison offices to assess the level of cooperation and satisfaction among the USNCB partners.

To assess the USNCB's efforts to ensure domestic participation in the INTERPOL notice program, we reviewed domestic law enforcement agency websites and selected a sample of 32 known international, high-profile U.S. criminal fugitives. The sample consisted of 10 names from the FBI's most wanted fugitives website, 14 names from the DEA's most wanted fugitives website, and 8 names from ICE's most wanted fugitives website. We then reviewed the INTERPOL website and USNCB records to determine whether a corresponding red notice had been issued by the domestic agency for these 32 fugitives.

Exchange of INTERPOL Information

To evaluate the USNCB's processes and controls over the exchange and integration of information, we reviewed the USNCB's policies and procedures for maintaining data within its case management system, ENVOY. In addition, we performed various tests on a limited number of domestic and foreign law enforcement agency notices and diffusions.

The USNCB maintains information pertaining to INTERPOL notices and diffusions in ENVOY. We requested from the USNCB a universe of case

records from ENVOY that included all domestic and foreign notices and diffusions that were active during the period October 1, 2005, through April 30, 2008. On May 29, 2008, the USNCB provided two spreadsheets that contained the data pertaining to all domestic and foreign notices and diffusions that were active during the period October 1, 2005, through May 29, 2008. As shown in the following table, our initial testing methodology included selecting a sample of 65 each of domestic and foreign notices and diffusions for review and analysis.

| Distribution of Sample Selection for Foreign and Domestic Notices and Diffusions | | | | |
|---|------------------|-----------------|---------------------|--------------------|
| Type | Sample Plan | | Sample Plan | |
| | Domestic Notices | Foreign Notices | Domestic Diffusions | Foreign Diffusions |
| Red | 15 | 15 | 15 | 15 |
| Blue | 10 | 10 | 10 | 10 |
| Yellow | 10 | 10 | 10 | 10 |
| Green | 10 | 10 | 10 | 10 |
| Black | 10 | 10 | 10 | 10 |
| Orange | 10 | 10 | 10 | 10 |
| Totals | 65 | 65 | 65 | 65 |

In some instances, the universe of notices and diffusions provided by the USNCB did not contain sufficient numbers of records from which to select according to the sample plan. For example, while the OIG testing plan called for a sample size of 10 each for black and orange domestic and foreign notices, there were only 7 black foreign notices, 2 orange foreign notices, and 1 domestic orange notice. As a result, in these instances we selected the entire universe of notice and diffusion records for review.

In addition, we identified several types of notices and diffusions of which we were unaware prior to the USNCB's provision of the universe of notices and diffusions, including white, purple, and grey.¹¹⁰ As a result, we judgmentally selected some white, grey, and purple notices for review.

During our analysis of the sample data, we identified several instances in which it appeared that the classification of a notice or diffusion in ENVOY

¹¹⁰ We subsequently learned that white notices pertain to stolen art and were discontinued by INTERPOL when it implemented the stolen works of art database, and purple notices pertain to methods and procedures and were also discontinued by INTERPOL. We discussed the grey notice with the USNCB Compliance Officer, but she could not recall its purpose.

was incorrect. For example, from the universe of notices identified as domestic-issued notices provided by the USNCB, we selected a specific case classified as a domestic red notice. During our review of the related documents, we noted that the red notice had been issued by a foreign law enforcement agency and, therefore should have been classified as a foreign-issued red notice. We discussed this issue with the USNCB CIO, who explained that this anomaly is related to the file structure of the ENVOY system as well as the method the USNCB used to extract the necessary data for our analysis.

While we identified several instances in which this type of anomaly occurred within our data extract, we performed limited testing of the data within ENVOY to verify that the data was properly classified. However, because of limitations within the ENVOY system, the USNCB was unable to provide a data file that did not contain these types of anomalies, as well as met our testing specifications. Despite the data limitations within the sample data provided by the USNCB, when these data are viewed in context with other available evidence, we believe the opinions, conclusions, and recommendations in this report are valid. Because each anomaly was slightly different, we determined, on a case-by-case basis, how we would categorize the notice or diffusion for analysis. We verified the results of our analysis with USNCB officials. Our analysis and subsequent re-categorization is discussed in greater detail in the following sections.

Domestic Notice and Diffusion Testing

As of May 29, 2008, the universe of domestic notice and diffusion records provided by the USNCB included 9,028 and 315 records, respectively. As shown in the following table, from the notices and diffusions classified as issued by a domestic law enforcement agency by the USNCB, we initially selected a total of 103 for analysis. We excluded one domestic red notice from our analysis because the notice was included twice in the data sample provided by the USNCB, and we inadvertently selected it twice. In addition, we excluded one domestic yellow notice from our analysis because the yellow notice had been issued by a foreign law enforcement agency. We included this yellow notice in our analysis of foreign-issued notices and diffusions. As a result of our analysis and reclassification, we reviewed 101 domestic-issued notices and diffusions, as shown in the following table.

| Distribution of Sample Selection for Domestic Notices and Diffusions | | |
|---|--|-----------------------------|
| Total Number of Records Reviewed by Color and Type | As Classified in Sample Selection | As Determined by OIG |
| Red Notice | 16 | 15 |
| Blue Notice | 10 | 9 |
| Yellow Notice | 9 | 9 |
| Green Notice | 10 | 9 |
| Orange Notice | 1 | 0 |
| FOPAC Bulletin/Grey Notice | 1 | 0 |
| U.N. Special Notice | 1 | 0 |
| Total Domestic Notices | 48 | 42 |
| | | |
| Total Number of Records Reviewed by Color and Type | As Classified in Sample Selection | As Determined by OIG |
| Wanted Person (Red) Diffusion | 15 | 13 |
| Trace and Locate (Blue) Diffusion | 11 | 11 |
| Missing Person (Yellow) Diffusion | 6 | 5 |
| Criminal Activity (Green) Diffusion | 10 | 10 |
| General Diffusion | 7 | 15 |
| Humanitarian Diffusion | 6 | 5 |
| Total Domestic Diffusions | 55 | 59 |
| Total Domestic Notices and Diffusions | 103 | 101 |
| Source: OIG analysis of USNCB data | | |

Using this sample of ENVOY case records pertaining to domestic notices and diffusions, we performed various tests to ensure that the information from each notice and diffusion was entered into ENVOY in an accurate and consistent manner. Further, we reviewed case-related information pertaining to the notices and diffusions to ensure that the requests for assistance and information were handled in an appropriate, efficient, and timely manner.

The USNCB does not enter the subjects of domestic notices into any of the U.S. agency systems, including NCIC and TECS. However, we reviewed related records from the pertinent automated domestic data systems used to store such things as criminal information, by DHS, the FBI, and USNCB. From that review, we assessed the USNCB's efforts to share all appropriate information in its possession with its domestic law enforcement counterparts.

Foreign Notice and Diffusion Testing

As of May 29, 2008, the universe of foreign notice and diffusion records provided by the USNCB included 40,663 and 134,589 records, respectively. As shown in the following table, from the notices and diffusions classified as issued by a foreign law enforcement agency by the USNCB, we initially selected a total of 116 for analysis. As discussed in the domestic notice and diffusion testing section, we identified one yellow notice classified by the USNCB as a domestic-issued notice. However, the yellow notice had been issued by a foreign law enforcement agency. As a result, we included this yellow notice in our analysis of foreign-issued notices and diffusions. During our review of the notices and diffusions classified as foreign-issued, we identified a purple notice and a criminal activity (green) diffusion that appeared misclassified. We discussed these two instances with the USNCB Compliance Officer who stated that the purple notice and criminal activity (green) diffusion were misclassified in ENVOY and should not have been included in the original sample data provided by the USNCB. As a result, we excluded these two cases from our analysis. Following our analysis and re-classification, we reviewed 115 foreign-issued notices and diffusions, as shown in the following table.

| Distribution of Sample Selection for Foreign Notices and Diffusions | | |
|--|--|-----------------------------|
| Total Number of Records Reviewed by Color and Type | As Classified in Sample Selection | As Determined by OIG |
| Red Notice | 17 | 18 |
| Blue Notice | 10 | 11 |
| Yellow Notice | 10 | 11 |
| Green Notice | 10 | 10 |
| Black Notice | 7 | 7 |
| Orange Notice | 2 | 2 |
| Stolen Art Notice | 3 | 3 |
| Purple Notice | 1 | 0 |
| Total Foreign Notices | 60 | 62 |
| | | |
| Total Number of Records Reviewed by Color and Type | As Classified in Sample Selection | As Determined by OIG |
| Wanted Person (Red) Diffusion | 21 | 20 |
| Trace and Locate (Blue) Diffusion | 10 | 9 |
| Missing Person (Yellow) Diffusion | 10 | 11 |
| Criminal Activity (Green) Diffusion | 4 | 2 |
| Dead Body (Black) Diffusion | 7 | 7 |
| Humanitarian Diffusion | 3 | 3 |
| Stolen Art Diffusion | 1 | 1 |
| Total Foreign Diffusions | 56 | 53 |
| Total Foreign Notices and Diffusions | 116 | 115 |

Using this sample of ENVOY case records pertaining to foreign notices and diffusions, we performed various tests to ensure that the information from each notice and diffusion was entered into ENVOY in an accurate and timely manner. Further, we reviewed case-related information pertaining to the notices and diffusions to ensure that the requests for assistance and information were handled in an appropriate, efficient, and timely manner.

We performed supplementary testing for the records associated with the foreign notices and diffusions that are eligible for entry into domestic law enforcement databases, including TECS and NCIC. Of the 115 records in our sample, 23 pertain to foreign notices and diffusions, including black, orange, white, and humanitarian. Because some of this information may not be suitable for use in the majority of screening processes involving domestic databases, we excluded it from this analysis. As a result, we tested 92 records that pertain to red, blue, yellow, and green foreign notices and diffusions.

We reviewed related records from the pertinent automated domestic data systems used to store, among other things, criminal information by DHS, the FBI, and USNCB, to determine if the individuals were included in the databases in a timely manner and the information was accurate, complete, and consistent. The automated data systems were the USNCB's ENVOY, DHS's TECS, and the FBI's NCIC. Specifically, we attempted to determine whether basic identifying information (e.g., name, gender, place of birth, date of birth, passport number, passport country of issuance, any additional identification information) as well as physical characteristics (e.g., hair and eye color, height, weight) listed on the notice or diffusion were accurately entered into the domestic databases in a timely manner.

Controls over INTERPOL Case Information

To assess the USNCB's controls over INTERPOL case-related information, we reviewed the USNCB's internal case management policy manual and observed USNCB analysts' management of cases. We performed various tests to ensure that the requests for assistance and information were well coordinated. We also reviewed documentation pertaining to the USNCB's electronic case management system, ENVOY, and assessed the USNCB's processes for safeguarding the information contained within ENVOY, including records retention and disposal.

USNCB Mission and Priorities

To assess the USNCB's organizational roles and strategic priorities, we examined the USNCB's mission, organizational structure, and operational environment. We also reviewed documentation and interviewed various officials to ensure that the USNCB's efforts are in line with DOJ priorities and reflect the USNCB's role in the post-September 11, 2001, world.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards*, we tested, as appropriate given our audit scope and objectives, selected records, procedures, and practices, to obtain reasonable assurance that the United States National Central Bureau's (USNCB) management complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. USNCB management is responsible for ensuring compliance with federal laws and regulations applicable to the USNCB. In planning our audit, we identified the following laws, regulations, and requirements that concerned the operations of the auditee and that were significant within the context of the audit objectives:

- The Freedom of Information Act 1.5 U.S.C. § 552 (2000 & Supp. III 2003)
- The Privacy Act (28 C.F.R § 16.103) (2008)
- ICPO-INTERPOL Constitution and General Regulations
- Memorandum of Understanding between the Department of Homeland Security and the U.S. Department of Justice pertaining to U.S. membership in the international criminal police organization (INTERPOL), and related matters (2003)

Our audit included examining, on a test basis, the USNCB's compliance with the aforementioned laws, regulations, and requirements that could have a material effect on the USNCB's operations, through interviews of USNCB personnel, the analysis of procedures and practices, and case file examination.

As noted in the body of this report, we found that the USNCB did not comply with elements of the Privacy Act because it has not archived case-related information as outlined in its System of Records Notice (SORN). As part of the agreement of participating in INTERPOL, member countries agree to abide by the established rules for the maintenance, retention, and deletion of information. Contrary to these rules, the USNCB has not ensured that the information it provides to other organizations is accurate, complete, and current. Further, the USNCB has not ensured that INTERPOL information is appropriately controlled and safeguarded.

STATEMENT ON INTERNAL CONTROLS

As required by the *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of the United States National Central Bureau's (USNCB) internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. USNCB management is responsible for the establishment and maintenance of internal controls.

As noted in the body of this report, we identified deficiencies in the USNCB's internal controls that are significant within the context of the audit objectives. Based upon the audit work performed, we believe these deficiencies adversely affect the USNCB's ability to properly perform its core mission. We identified four main weaknesses in our report: (1) The USNCB has not made critical international criminal information available to U.S. law enforcement agencies, which has increased the potential that high-risk, violent criminals could enter the United States undetected; (2) The USNCB has not implemented adequate controls or processes to ensure that the INTERPOL information it has made available to domestic agencies is accurate, current, and timely. This has resulted in domestic law enforcement systems that likely contain out-of-date or incomplete data, includes information on individuals for whom no law enforcement agency has a current investigative interest, and may violate other member countries' privacy laws; (3) The USNCB's internal case management information system, ENVOY, contains deficiencies that prevent the USNCB from adequately maintaining, controlling, and disposing of case-related information; compiling management statistics; and generating standardized correspondence; and (4) The USNCB has not adequately maintained the communication channels established for interacting with its domestic law enforcement partners. As a result, critical law enforcement information or requests for assistance may not be reaching the intended recipients. These issues are discussed within the body of this report.

Because we are not expressing an opinion on the USNCB's internal control structure as a whole, this statement is intended solely for the information and use of the auditee. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

INTERPOL MEMBER COUNTRIES

| | |
|-----------------------------|---------------------------------------|
| Afghanistan | Costa Rica |
| Albania | Côte d'Ivoire |
| Algeria | Croatia |
| Andorra | Cuba |
| Angola | Cyprus |
| Antigua and Barbuda | Czech Republic |
| Argentina | Denmark |
| Armenia | Djibouti |
| Aruba | Dominica |
| Australia | Dominican Republic |
| Austria | Ecuador |
| Azerbaijan | Egypt |
| Bahamas | El Salvador |
| Bahrain | Equatorial Guinea |
| Bangladesh | Eritrea |
| Barbados | Estonia |
| Belarus | Ethiopia |
| Belgium | Fiji |
| Belize | Finland |
| Benin | Former Yugoslav Republic of Macedonia |
| Bhutan | France |
| Bolivia | Gabon |
| Bosnia and Herzegovina | Gambia |
| Botswana | Georgia |
| Brazil | Germany |
| Brunei Darussalam | Ghana |
| Bulgaria | Greece |
| Burkina Faso | Grenada |
| Burundi | Guatemala |
| Cambodia | Guinea |
| Cameroon | Guinea-Bissau |
| Canada | Guyana |
| Cape Verde | Haiti |
| Central African Republic | Honduras |
| Chad | Hungary |
| Chile | Iceland |
| China | India |
| Colombia | Indonesia |
| Comoros | Iran |
| Congo | Iraq |
| Congo (Democratic Republic) | Ireland |

Israel
Italy
Jamaica
Japan
Jordan
Kazakhstan
Kenya
Korea (Republic of)
Kuwait
Kyrgyzstan
Laos
Latvia
Lebanon
Lesotho
Liberia
Libya
Liechtenstein
Lithuania
Luxembourg
Madagascar
Malawi
Malaysia
Maldives
Mali
Malta
Marshall Islands
Mauritania
Mauritius
Mexico
Moldova
Monaco
Mongolia
Montenegro
Morocco
Mozambique
Myanmar
Namibia
Nauru
Nepal
Netherlands
Netherlands Antilles
New Zealand
Nicaragua
Niger
Nigeria
Norway
Oman
Pakistan
Panama
Papua New Guinea
Paraguay
Peru
Philippines
Poland
Portugal
Qatar
Romania
Russia
Rwanda
Saint Kitts and Nevis
Saint Lucia
Saint Vincent and the Grenadines
San Marino (Republic of)
Sao Tome and Principe
Saudi Arabia
Senegal
Serbia and Montenegro
Seychelles
Sierra Leone
Singapore
Slovakia
Slovenia
Somalia
South Africa
Spain
Sri Lanka
Sudan
Surinam
Swaziland
Sweden
Switzerland
Syria
Tajikistan
Tanzania
Thailand
Timor-Leste
Togo
Tonga

Trinidad and Tobago
Tunisia
Turkey
Turkmenistan
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States of America
Uruguay
Uzbekistan
Vatican City State
Venezuela
Vietnam
Yemen
Zambia
Zimbabwe

USNCB STATE & LOCAL LIAISONS

| | |
|-----------------------------|---|
| Alabama | Alabama Bureau of Investigation |
| Alaska | Alaska State Troopers |
| Arizona | Arizona Department of Public Safety |
| Arkansas | Arkansas State Police |
| California | California Department of Justice |
| | Los Angeles Police Department |
| | Los Angeles County Sheriff's Department |
| | San Diego Criminal Intelligence Unit |
| | San Francisco Police Department |
| Colorado | Colorado Bureau of Investigation |
| Connecticut | Connecticut State Police |
| Delaware | Delaware State Police |
| District of Columbia | Washington Metropolitan Police Department |
| Florida | Florida Department of Law Enforcement |
| | Miami-Dade Police Department |
| Georgia | Georgia Bureau of Investigation |
| Hawaii | Department of the Attorney General |
| Idaho | Criminal Investigation Bureau |
| Illinois | Illinois State Police |
| | Chicago Police Department |
| Indiana | Indiana State Police |
| Iowa | Iowa Department of Public Safety |
| Kansas | Kansas Bureau of Investigation |
| Kentucky | Kentucky State Police |
| Louisiana | Louisiana State Police |
| Maine | Maine State Police |
| Maryland | Maryland State Police |
| Massachusetts | Massachusetts State Police |
| | Boston Police Department |
| Michigan | Michigan State Police |
| Minnesota | Bureau of Criminal Apprehension |
| Mississippi | Mississippi Department of Public Safety |
| Missouri | Missouri State Highway Patrol |
| Montana | Montana All Threat Intel Center |
| Nebraska | Nebraska State Patrol |
| Nevada | Nevada Division of Investigation |
| New Hampshire | New Hampshire State Police |
| New Jersey | New Jersey State Police |
| New Mexico | New Mexico State Police |

| | |
|--|--|
| New York | New York State Police |
| | New York New Jersey HIDTA |
| North Carolina | North Carolina State Bureau of Investigation |
| North Dakota | Bureau of Criminal Investigation |
| Ohio | Criminal Intelligence Unit |
| Oklahoma | Oklahoma State Bureau of Investigation |
| Oregon | Oregon State Police |
| Pennsylvania | Pennsylvania Office of the Attorney General |
| Rhode Island | Rhode Island State Police Headquarters |
| South Carolina | South Carolina Law Enforcement Division |
| South Dakota | Division of Criminal Investigation |
| Tennessee | Tennessee Bureau of Investigation |
| Texas | Texas Criminal Investigations Division |
| | Houston Police Department |
| Utah | Utah Criminal Intelligence Center |
| Vermont | Vermont Fusion Center |
| Virginia | Virginia State Police |
| Washington | Washington State Patrol |
| | Seattle Police Intelligence Section |
| West Virginia | West Virginia State Police |
| Wisconsin | Wisconsin Department of Justice |
| Wyoming | Wyoming Division of Criminal Investigation |
| U.S. American Samoa | American Samoa Government |
| Puerto Rico | Puerto Rico Department of Justice |
| U.S. Virgin Islands | Virgin Islands Police Department |
| Guam | Guam Police Department |
| U.S. Commonwealth of the Northern Mariana Islands | Department of Public Safety |

USNCB QUESTIONNAIRE AND RESPONSES

*****Please Respond by August 22, 2008*****

The United States National Central Bureau (USNCB) for Interpol is the U.S. contact for the Interpol database. Our records indicate you are a State or Local Liaison to the USNCB. The Department of Justice, Office of the Inspector General is conducting a performance audit of the USNCB. Please take a few moments to answer the questions that apply to your organization.

Please submit your response via e-mail to a secure mailbox to which the USNCB has no access at OIGSurvey@US.IGCS.INT or via facsimile to the Department of Justice, Office of the Inspector General at (312) 886-0513.

Organization Name: _____

1. In your opinion, how many officers in your jurisdiction are aware of the Interpol database? (Check (√) one that applies) **[58 respondents]**

- | | | |
|--------------------------|-------------------------------------|-----|
| <input type="checkbox"/> | Almost all officers are aware | 5% |
| <input type="checkbox"/> | Most are aware | 21% |
| <input type="checkbox"/> | Some are aware | 50% |
| <input type="checkbox"/> | Few are aware | 22% |
| <input type="checkbox"/> | None are aware (please explain why) | 2% |
-

The OIG received the following comments:

- One city has sent internal documents to all officers;
 - Another city has not publicized the Interpol database throughout the entire department, but relies on word of mouth; and
 - One state has described Interpol resources in statewide intelligence bulletins.
-

2. In your opinion, of those officers aware of the database, how knowledgeable are they about the usefulness of the information in the Interpol database? (Check (√) one that applies) **[57 respondents]**

- | | | |
|--------------------------|--|-----|
| <input type="checkbox"/> | Extremely knowledgeable | |
| <input type="checkbox"/> | Very knowledgeable | 5% |
| <input type="checkbox"/> | Somewhat knowledgeable | 81% |
| <input type="checkbox"/> | Not knowledgeable (please explain why) | 14% |
-

The OIG received the following comments:

Most of the respondents stated that the officers are not aware, haven't had training, or that training would be helpful.

3. Do you access the Interpol database directly? (Check (√) one that applies) **[57 respondents]**

- Yes (51%) No (49%)
↓

If yes, was the Interpol database easy to use? **[30 respondents]**

- Yes (73%) No (27%)
↓

If no, please explain why.

The OIG received the following comments:

- One state said that they have had trouble doing the practice session, and
 - One city said that no training has ever been done on a local basis.
-

4. If you access the Interpol database directly, how frequently do you access it? (Check (√) one that applies) **[35 respondents]**

- | | | |
|--------------------------|---------|-----|
| <input type="checkbox"/> | Daily | 9% |
| <input type="checkbox"/> | Weekly | 31% |
| <input type="checkbox"/> | Monthly | 37% |
| <input type="checkbox"/> | Yearly | 3% |
| <input type="checkbox"/> | Never | 20% |

↓

If never, please explain why.

The OIG received no comments for this question.

5. How frequently do you interact with the USNCB via telephone or e-mail? (Check (√) one that applies) **[58 respondents]**

- | | | |
|--------------------------|---------|-----|
| <input type="checkbox"/> | Daily | 5% |
| <input type="checkbox"/> | Weekly | 45% |
| <input type="checkbox"/> | Monthly | 36% |
| <input type="checkbox"/> | Yearly | 7% |
| <input type="checkbox"/> | Never | 7% |
-

The OIG received no comments for this question.

6. If you have been a liaison to the USNCB for 2 or more years, has there been a change in the frequency of your communication with the USNCB in the past 2 years? (Check (√) one that applies) **[56 respondents]**

Yes (39%) No (32%) Not applicable (29%)
↓

If 'Yes', how did the frequency of communication change?
(Check (√) one that applies) **[22 respondents]**

Increased (100%) Decreased

Please describe any reasons for the change.

The OIG received the following comments:

- Better/secure communication through RISS.net;
 - Attendance at USNCB Liaison training improved understanding of responsibilities;
 - World's getting smaller;
 - Police Departments are getting more pro-active in requesting information from other countries;
 - More comfort in contacting USNCB with inquiries; and
 - More personnel becoming aware of the capabilities.
-

7. In your opinion, how helpful was the USNCB information when investigating cases? (Check (√) one that applies) **[54 respondents]**

| | |
|--|-----|
| <input type="checkbox"/> Extremely helpful | 11% |
| <input type="checkbox"/> Very Helpful | 50% |
| <input type="checkbox"/> Somewhat helpful | 37% |
| <input type="checkbox"/> A little or not helpful | 2% |

The OIG received no comments for this question.

8. In general, how timely has the USNCB responded to your requests?
(Check (√) one that applies) **[52 respondents]**

- | | | |
|--------------------------|------------------|-----|
| <input type="checkbox"/> | Always timely | 27% |
| <input type="checkbox"/> | Often timely | 38% |
| <input type="checkbox"/> | Sometimes timely | 27% |
| <input type="checkbox"/> | Rarely timely | 8% |
-

The OIG received no comments for this question.

9. In general, how complete was the information provided to you by the USNCB in response to your requests? (Check (√) one that applies)
[52 respondents]

- | | | |
|--------------------------|-------------------|-----|
| <input type="checkbox"/> | Complete | 67% |
| <input type="checkbox"/> | Somewhat complete | 33% |
| <input type="checkbox"/> | Not complete | 0% |
-

The OIG received no comments for this question.

10. On an average, how often do the law enforcement agencies in your jurisdiction request Interpol information? (Check (√) one that applies)
[56 respondents]

- | | | |
|--------------------------|---------|-----|
| <input type="checkbox"/> | Daily | 2% |
| <input type="checkbox"/> | Weekly | 9% |
| <input type="checkbox"/> | Monthly | 46% |
| <input type="checkbox"/> | Yearly | 38% |
| <input type="checkbox"/> | Never | 5% |

↓

If never, please explain why.

From the 5% that answered never, the explanations were:

- No publicity about the database existence, and
- Unsure what type of information can be obtained.

11. If you have been a liaison to the USNCB for 2 or more years, has the number of requests from the law enforcement agencies in your jurisdiction (about international-related cases) changed during the past 2 years? **[55 respondents]**

Yes (25%) No (44%) Not applicable (31%)

↓

If 'Yes', how did the frequency of communication change?
(Check (√) one that applies) **[15 respondents]**

Increased (100%) Decreased

Please describe any reasons for the change.

Comments received regarding any reasons for the change:

- More residents from other countries living here illegally;
 - Local law enforcement either seems more open to request information and/or there has been an increase in these types of cases within the rural areas; and
 - USNCB staff assisted in training unit personnel.
-

12. Have the law enforcement agencies in your jurisdiction ever provided feedback regarding USNCB information and assistance?
[54 respondents]

Yes (please explain about the feedback) (17%) No (83%)

The OIG received the following comments:

- Two "thank-yous" for the assistance/information;
 - Frustration at the slowness;
 - Not understanding guidelines for issuing notices;
 - The other countries are slower to respond or not respond at all;
 - Usually positive although timeliness is always a concern;
 - Disappointed that the requesting country didn't have as much information on the subject they were investigating; and
 - Information received was useful but it takes too long to get response back.
-

13. Are there any comments or concerns regarding the USNCB services? Please describe below.
-

The OIG received the following overall comments:

- The Special Agents that I have the pleasure working with from INTERPOL have been extremely helpful. They have provided insight to other aspects that I may have over looked in a case and are always up front in advising if specific information is attainable from other member countries. They have been very good about keeping in touch with me on pending requests. And the response time in acknowledgement of a new request is outstanding. It's a pleasure working with the USNCB individuals and I appreciate all the assistance they have provided me.
- The USNCB is a valuable resource for this Unit and the state.
- Some of the other countries take too long to respond and process is labor intensive. I receive a request from my state, I send a request to D.C., they send a request to the country, the country responds to D.C., and D.C. sends a response to me and I send a response to the requester. There are some situations that are more appropriate for the officer here to e-mail and phone directly. This could occur after the Interpol number is assigned. Response would be much quicker.
- Every contact with USNCB has been positive. The patience of USNCB representatives during our transition period has been most appreciated.
- We provide a great deal more information than we request. The volume of requests from USNCB has increased steadily. In our experience, a significant percentage of the requests from USNCB could be handled by USNCB or other federal agencies.
- More training for new state liaisons.
- It is not a case where we do not use this data base. It is a matter of having too many databases to check. In the case of Interpol it is usually reserved for international inquiries.
- My experience with the USNCB has always been positive. They are professional courteous and bend over backwards to help!

- The only critique is the method of communication; the Rissnet secure e-mail system is slow, cumbersome and often frustrating to use. Because of that, I rarely use it and only when required to correspond with USNCB. That may be the nature of secure e-mail systems.
- We greatly enjoy the spool of USNCB intelligence and open source information. The information is received daily and in a timely manner.
- I have not received timely responses and this is very frustrating. It also does not encourage use when the information is not received for months at a time.
- I'm very happy with the services USNCB provides. It's difficult to get some out of country request that flows through the USNCB answered quickly but that appears to me to be the fault of the country receiving the request.
- Sending and receiving all requests, replies, and messages via e-mail works much better for me. The information sent via teletype sometimes gets lost, and I never see it. Fortunately, the majority of my communications is now being conducted via e-mail.
- We are unable to access the database. It is the fault of our organization as far as I know! The Assistant Director of Interpol has tried!
- (1) Acknowledgment of receipt of electronic communications (not just a "read receipt").
- (2) Allow liaisons to electronically track or check the case status.
- (3) Love the new database I-24/7. It's easy to use, results return quickly, and data is presented in a way that is easy to understand.
- USNCB should do an automatic resending (second request) of a message to a foreign country, if that country fails to respond in thirty (30) days. The requesting agency should be notified and

provided documentation that the original request and/or additional re-sent request are forwarded to a foreign country.

- The main concern is when receiving a request for assistance from INTERPOL minimal information is provided. It would be helpful for INTERPOL to provide as much information as possible when sending a request to us. Usually, the information needed is an identifier or is very basic and may be information that INTERPOL already has or could easily find out. This would save valuable time being that by the time we receive the initial request, it is usually several months late.
- I have had problems with getting confirmation that they have received reports I have sent to them using the RISS e-mail system.
- We are looking forward to using the database and feel we will be able to obtain information that will assist in our investigations. While I have only been the liaison for approximately 1 year all of my dealings with the USNCB have been very informative and helpful.
- We would like to obtain a simple manual or guide on the use of the I-24/7 in order to efficiently use the Interpol system.
- There is no way of knowing if USNCB has received any e-mail response that may have been sent to them. Often receive a message stating e-mail deleted without being read. Very little communication from USNCB other than e-mail. E-mail often cumbersome to use with required headers and footers no matter how short the message. E-mail requests often lacking needed information for a case, with no phone contact information available. Training needed for outlying areas away from D.C.
- Like the connectivity of Interpol liaison using the Riss.net system. I get notified by MOCIC when the USNCB has sent me a specific e-mail that requires response & that works well.
- In this age of computers, it would be useful to have access via computer - possibly VPN connection to all personnel designated access users.
- Superb response - extremely efficient & always helpful!

- There have been some recent issues with INTERPOL communications and requests coming from the USNCB Watch Center that are not being directed to the appropriate INTERPOL liaisons with jurisdiction over the matter. This issue has manifested itself in two ways, primarily:
 1. Often, no distinction is made between the INTERPOL liaisons that represent the New York Police Department and the INTERPOL liaisons that represent the remaining law enforcement jurisdictions outside of the five boroughs of New York City. Sometimes the IP-USNCB sends the request to both entities in New York State, but often the request is sent to only one of them, and it is the incorrect agency. This leads to numerous requests made of the USNCB to re-direct the request to the appropriate entity, or in an exigent circumstance, losing valuable response time while the request gets sent directly between the two liaison offices so the appropriate agency can respond.
 2. Cases involving federal issues are not being directed to the appropriate federal law enforcement agency with jurisdiction over the matter. Instead, they are being sent to state-level IP liaisons that lack jurisdiction to intervene. In recent months, there have been several examples of this concern, where cases involving the location of possible international war criminals, child/human trafficking, and international Internet fraud were directed to the state liaisons instead of the appropriate federal law enforcement agency. The concern has also operated in reverse, where an urgent DNA databank search request relating to a homicide investigation was misdirected to the FBI-NY instead of the NYS INTERPOL liaisons, resulting in much confusion and delay about what entity was supposed to respond to the request. It was only after extensive file checks and communication with USNCB that it was revealed where the original request was sent to, and what happened subsequently.
- We are looking forward to utilizing Interpol for requests.
- It is a great law enforcement tool. Everyone should have access.
- What types of information can be obtained. How will it help us?

- Recently assigned liaison.
 - There seems to certain countries that send out numerous requests, and all of their requests are answered in a timely fashion. From experience, those same countries don't honor the same timeframe when my agency puts out the request.
 - I would like to request training and direct access to the INTERPOL database.
-

Thank you for taking the time to complete the questionnaire. Your participation is greatly appreciated and will help us in our audit of the USNCB.

INTERPOL NOTICES

INTERPOL utilizes a system of color-coded international notices and diffusions to share critical crime-related information with each of the 187 member countries. The information concerns individuals wanted for serious crimes, missing persons, unidentified bodies, possible threats, and criminals' modus operandi. At the meeting of the INTERPOL General Assembly in October 2008, the member countries adopted a new framework for the issuance of notices. According to INTERPOL guidelines, the following is the definition and purpose for each notice, as well as the criteria for issuing them:

Red Notices

Red notices are published in order to seek the location and arrest of a person with a view to his or her extradition. Before a National Central Bureau or an authorized international entity requests publication and circulation of a red notice, it shall ensure that:

- the person sought is the subject of criminal proceedings or has been convicted of a crime and references to an enforceable arrest warrant, court decision, or other judicial documents are provided;
- assurances have been given that extradition will be sought upon arrest of the person, in conformity with national laws or the applicable bilateral and multilateral treaties; and
- sufficient information is provided to allow for the cooperation requested to be effective.

Blue Notices

Blue notices are published in order to obtain information about, locate, or identify a person of interest in a criminal investigation. Before a National Central Bureau, a national authorized institution, or an authorized international entity requests publication and circulation of a blue notice, it shall ensure that:

- the person is someone of interest in a criminal investigation, such as a criminal, a suspect, an accomplice, an associate or a witness;
-

- additional information on the possible criminal history, status, location, or identity of the person or any other information relevant to the criminal investigation is sought; and
- sufficient information is provided to allow for the cooperation requested to be effective.

Green Notices

Green notices are published to warn about a person's criminal activities. Before a National Central Bureau, a national authorized institution, or an authorized international entity requests publication and circulation of a green notice, it shall ensure that:

- the person is considered to be a possible threat to public safety or someone likely to commit a criminal offense;
- the conclusion is based on an assessment by a national law enforcement authority or an authorized international entity;
- the assessment is based on the person's previous criminal conviction or other reasonable grounds; and
- sufficient information is provided to allow for the warning to be relevant.

Yellow Notices

Yellow notices are published to locate a missing person or to identify a person unable to identify himself or herself. Before a National Central Bureau, a national authorized institution, or an authorized international entity requests publication and circulation of a yellow notice, it shall ensure that:

- if the notice is published to locate a missing person, the person has been reported missing to police, his or her whereabouts are unknown and the person's anonymity or privacy is not protected by the applicable national laws.
- if the notice is published to identify a person unable to identify himself or herself, the request is being made because a person has been found and he or she is unable to identify himself or herself; and
- sufficient information is provided to allow for identification.

Black Notices

Black notices are published to identify dead bodies. Before a National Central Bureau, a national authorized institution, or an authorized international entity requests publication and circulation of a black notice, it shall ensure that:

- the request is being made because a body has been found and it has not been identified; and
- sufficient information is provided to allow for identification.

Stolen Works of Art

Stolen works of art notices are published to locate works of art or items of cultural value that have been stolen, or to identify such objects discovered in suspicious circumstances. Before a National Central Bureau, a national authorized institution, or an authorized international entity requests publication and circulation of a stolen work of art notice, it shall ensure that:

- the work of art or item of cultural value is of interest in a criminal investigation;
- it has some unique characteristic or is of considerable value; and
- sufficient information is provided to allow identification.

Purple Notices

Purple notices are published to provide information on methods, procedures, objects, devices and hiding places used by criminals. Before a National Central Bureau, a national authorized institution, or an authorized international entity requests publication and circulation of a purple notice, it shall ensure that the circulation of the information in the form of a notice is of specific international interest to the police and is in the interests of public safety.

Special Notices

Special notices are published on the basis of an agreement with another international organization concluded pursuant to Article 41 of the INTERPOL Constitution. Before an international authorized entity requests publication and circulation of a special notice, it shall ensure that:

- the information satisfies the conditions for publishing such notices, as defined in the said agreement; and
- sufficient information is provided to allow for the cooperation requested to be effective.

Orange Notices

Orange notices are published to warn about a person, an object, an event, or a modus operandi representing an imminent threat to public safety and likely to cause serious damage to property or injury to persons. Before a National Central Bureau, a national authorized institution, or an authorized international entity requests publication and circulation of an orange notice, it shall ensure that:

- in the case of a person, he or she is considered to be an imminent threat to public safety or someone likely to commit a criminal offense; this conclusion is based on an assessment by a national law enforcement authority;
- this assessment is based on the person's previous criminal conviction or other reasonable grounds;
- in the case of an object, modus operandi, or event, it is considered an imminent threat to public safety; this conclusion is based on an assessment by a national law enforcement authority; and
- sufficient information is provided to allow for the warning to be relevant.

Orange Notices constitute alerts and it is up to each country to take appropriate measures, in conformity with its national laws.

DATABASES USED IN DOMESTIC INTERNATIONAL CRIMINAL INFORMATION SHARING

To ensure that domestic law enforcement personnel have access to criminal and terrorist-related information on international criminals, the USNCB assists domestic law enforcement agencies with obtaining direct access to the INTERPOL databases. In addition, the USNCB exports or sends international criminal data to other domestic systems. Following are descriptions of the U.S. databases that receive INTERPOL information.

CLASS

The Consular Lookout and Support System (CLASS) is maintained by the Department of State (State Department). CLASS, divided into CLASS/Visa and CLASS/Passport, is used by State Department representatives when processing visa and passport applications, respectively.

NCIC

The National Crime Information Center (NCIC) is maintained by the FBI and is a nationwide information system dedicated to serving and supporting criminal justice agencies – federal, state, local, and tribal – in their mission to uphold the law and protect the public. NCIC serves criminal justice agencies in all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, American Samoa, Guam, and Canada, as well as federal agencies with law enforcement missions. NCIC can be accessed at the lowest level by an officer on the street.

TECS

The Department of Homeland Security's (DHS) TECS is an overarching law enforcement information collection, analysis, and sharing environment. This environment is comprised of several modules designed to collect, maintain, and screen data; conduct analysis, and share information.

TIDE

The Terrorist Identities Datamart Environment (TIDE) is the U.S. government's central repository of information on international terrorist identities. TIDE supports the U.S. government's various terrorist screening systems, or "watchlists," and the U.S. intelligence community's overall counterterrorism mission. The TIDE database includes, to the extent permitted by law, all information the U.S. government possesses related to

the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of purely domestic terrorism information.

US-VISIT

Overseen by DHS, US-VISIT is the automated system that records travelers' entry and exit to and from the United States at over 300 ports of entry around the country, verifies their identity, and determines their compliance with the terms of their admission and stay. The system also collects, maintains, and shares information, including biometric identifiers, to determine whether travelers should be prohibited from entering the United States or if they have overstayed their visas.

UNITED STATES NATIONAL CENTRAL BUREAU RESPONSE



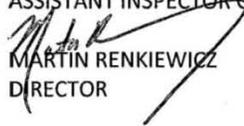
U.S. Department of Justice

INTERPOL - U.S. National Central Bureau

Washington, D.C. 20530

August 3, 2009

MEMORANDUM FOR MR. RAYMOND J. BEAUDET
 ASSISTANT INSPECTOR GENERAL

FROM: 
 MARTIN RENKIEWICZ
 DIRECTOR

SUBJECT: "DRAFT AUDIT REPORT – THE UNITED STATES NATIONAL CENTRAL
 BUREAU OF INTERPOL"

We have reviewed your Draft Audit Report dated July 13, 2009, and appreciate the opportunity to comment on the recommendations laid out in the report.

I am pleased to inform you that, since the audit began in March 2008, the INTERPOL-U.S. National Central Bureau (USNCB) has taken a number of actions in response to your findings. We are also evaluating how best to implement several of the recommendations in light of ongoing USNCB information sharing initiatives. I am confident that your report will serve to strengthen the effectiveness of our operations and enhance the value of our contribution to the Department's mission.

Recommendations 1 and 23 to 25 were directed to the Office of the Deputy Attorney General, which will respond separately to those recommendations. I have attached the USNCB's responses to recommendations 2-22, 26 and 27 with supporting documentation.

We have submitted our sensitivity review to Ms. Carol S. Taraszka, Regional Audit Manager, as instructed by your cover memorandum dated July 13, 2009. Should you have any questions regarding our response, please contact me on (202) 616-9700 or Warren Lewis, Executive Officer, on (202) 616-8810.

Attachments

cc: Deputy Attorney General
 Deputy Secretary, Department of Homeland Security
 Richard P. Theis, Assistant Director, Audit Liaison Group
 Justice Management Division

[The USNCB's response included two attachments. We have not included these attachments in our report due to their technical nature.]

Recommendation 2. Work with domestic law enforcement partners to ensure that the agencies issue INTERPOL notices for appropriate international fugitives, particularly those already publicly identified on the agencies' websites or elsewhere.

USNCB Response: Agree. The USNCB has implemented policy and procedures to regularly monitor U.S. 'Most Wanted' programs to identify subjects for inclusion in INTERPOL's notice program. In order to facilitate this goal, the USNCB will contact the appropriate United States Law Enforcement Agencies (USLEAs) to ensure that they are advised of INTERPOL's Notice Program, and provide assistance with the issuance of INTERPOL Notices for those fugitives where international leads have or may be identified. Assistant Directors (ADs) for USNCB investigative divisions will report the publication of INTERPOL notices for subjects who are also publicized on agency 'Most Wanted' lists, websites, or other media, in USNCB monthly significant activity reports. The USNCB will document those cases where an agency has declined to pursue the publication of an INTERPOL notice on the basis of agency investigative considerations. The USNCB will verify adherence to this policy through its Compliance Review Program.

Recommendation 3. Encourage federal law enforcement agencies to provide USNCB and INTERPOL-related training to their employees.

USNCB Response: Agree. The USNCB is in the process of formalizing a training outreach plan for this purpose. Earlier this year, the USNCB Director met with the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, to formalize the development of an INTERPOL-USNCB training course for all FLETC law enforcement personnel and analytical trainees. (The FLETC serves as an interagency law enforcement training organization for more than 80 Federal agencies.) The USNCB has provided FLETC with informational materials for the 2009-2010 classes, and is exploring a process to provide FLETC staff with instructional media and scheduled updates as needed. Once established, the USNCB will consider use of the media program for annual "in-service" training mandates, as well as training given to the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) students at their academies in Quantico, Virginia.

To date, the USNCB has initiated specialized INTERPOL database training (to include general information about the structure, mission, and activities of the INTERPOL organization) for various components of the Departments of Justice and Homeland Security. Important targets for this type of training are existing law enforcement fusion centers, task forces, call centers, and information sharing networks. The USNCB has also provided refresher training to the DHS Law Enforcement Support Center (LESC) on use of the INTERPOL database access already enabled at the LESC.

The USNCB will continue to work with its law enforcement partners and the INTERPOL General Secretariat in Lyon, France, to enhance INTERPOL training opportunities for the U.S. law enforcement community.

Recommendation 4. Develop a method for domestic law enforcement agencies to submit a notice application electronically.

USNCB Response: Agree. With the assistance of a contractor, the USNCB will develop a plan to implement a web portal that will allow domestic law enforcement agencies to submit electronically notice applications in a format compatible with the USNCB case management system development. Once deployed, the web portal (“IPOLNET”) will encourage greater use of INTERPOL’s notices by USLEAs, and increase efficiencies in the USNCB’s notice processing. The system will not, however, alleviate the need for the USNCB to carefully review incoming notice applications from U.S. agencies for sufficiency, legal compliance, and to supplement the information received from USLEAs with other relevant data available to the USNCB before final publication by INTERPOL. The USNCB anticipates completion of IPOLNET by end of FY2010. The USNCB will develop training methods to accompany the electronic notice application form. The USNCB will also evaluate the impact resulting from the electronic submission of notices on the USNCB’s workload, in anticipation of additional human resource needs. In the future, IPOLNET will provide a common architecture for the delivery of INTERPOL-USNCB services, including notice submissions. In the interim, the USNCB will continue to facilitate the submission of notice applications by domestic law enforcement agencies via existing infrastructure (e.g., secure email, Regional Information Sharing System, and Law Enforcement Online).

Recommendation 5. Implement information technology solutions to more broadly share U.S. stolen motor vehicle information with INTERPOL members.

USNCB Response: Agree. Currently the Federal Bureau of Investigation’s Criminal Justice Information System (FBI/CJIS) allows limited foreign country access to US stolen motor vehicle data through a USNCB-CJIS interface. To date, the FBI has not supported the uploading of US data into the INTERPOL database in Lyon, France, due to the volume of these data transactions. CJIS has also reported that it does not possess the required approval from the National Crime Information Center (NCIC) Advisory Policy Board (APB), which provides policy oversight for access to NCIC files, to authorize broad-scale INTERPOL access through the interface. The USNCB will re-engage FBI/CJIS and INTERPOL’s General Secretariat in Lyon, France, to explore whether these agencies will support making the necessary legal and policy changes (and subsequent technical and procedural changes) to both US and INTERPOL systems, to allow more INTERPOL countries access to these files through a proposed NCIC-INTERPOL interface.

Recommendation 6. Ensure that a reliable communications network is maintained with all state and local liaison offices.

USNCB Response: Agree. Presently, the USNCB communicates with its State Liaison Offices (SLOs) using existing secure networks, and the Regional Information Sharing System Networks (RISS) as a backbone. The USNCB will improve monitoring of these extranet email connections by polling each State Liaison email server every two hours. Alerts will be generated to the USNCB when email delivery notifications are not received for these messages or round-trip email communication is not validated. This step will allow the USNCB to proactively identify

any email connectivity issues with our SLOs. The USNCB State and Local Liaison Division (SLLD) will undertake a monthly poll of individual offices for any personnel changes in the user directory to avoid communication errors. In the future, the USNCB's planned "IPOLNET" web portal will support expanded networking capability for its SLOs.

Recommendation 7. Develop a formal outreach plan that identifies and prioritizes law enforcement organizations that would benefit from a better understanding of the USNCB and INTERPOL.

USNCB Response: Agree. The USNCB will formalize a comprehensive outreach plan and continue to explore areas to enhance INTERPOL training and raise awareness within the U.S. law enforcement community. The plan will address communication, information sharing, and training. The USNCB will improve its statistical reporting capability to better identify and prioritize those law enforcement agencies that would most benefit from USNCB outreach programs.

Recommendation 8. Review current and incoming green notices and determine if they are appropriate for inclusion in NCIC.

USNCB Response: Agree. The USNCB has received approval from FBI/CJIS to enter foreign-issued INTERPOL green notices on gang-related offenders into the Violent Gang and Terrorist Offender File (VGTOF). The USNCB will begin making these entries once USNCB and CJIS have implemented coding modifications to account for the specific purpose of these green notices. However, the entry of INTERPOL foreign-issued green notice information on sexual offenders into the NCIC Sexual Offender File requires the approval of the Advisory Policy Board (APB). The USNCB submitted a topic request to the NCIC APB Federal Working Group representative to propose the inclusion of this item at the NCIC APB's spring 2010 meeting, and we are awaiting confirmation. In the meantime, the USNCB will identify all active foreign green notice cases to determine those eligible for inclusion into the appropriate NCIC files; update the offense codes in the USNCB ENVOY database; and issue revised handling procedures to ensure that newly published green notices are appropriately reviewed for inclusion into the NCIC VGTOF or Sexual Offender Files.

Recommendation 9. Modify its policies and procedures regarding notice and diffusion information to ensure that the appropriate data is shared with U.S. agency databases and is made available to domestic law enforcement personnel in a timely manner.

USNCB Response: Agree. The USNCB is responsible for sharing information about domestic fugitives and subjects of interest with police in its 186 counterpart INTERPOL member countries; as well as informing domestic law enforcement about subjects of interest to foreign counterparts. Although the recommendation does not make the distinction, we note that the USNCB's procedures for handling notice and diffusion information must differentiate between foreign and domestic-issued notices and diffusions because USLEAs are responsible for placing entries on their fugitives and subjects of interest into national lookout systems. The USNCB is

responsible for placing entries on subjects of INTERPOL notifications into U.S. lookout systems. USNCB presently enters subjects of foreign notices and diffusions into TECS, and notice subjects into NCIC when criteria for that system are met. We agree there is great value in also making information on subjects of *foreign* diffusions available to state and local law enforcement via NCIC entries. To that end, beginning on 01 August 2009, USNCB staff began making NCIC entries on subjects of foreign diffusions, when NCIC criteria are met. In addition, the USNCB will make entries on foreign-issued notices and diffusions in either NCIC or TECS, but not both. TECS queries are federated with NCIC, enabling TECS users access to USNCB entries in NCIC.

We note that the USNCB is not responsible for entering subjects of domestic notices and diffusions (i.e., subjects wanted by U.S. law enforcement agencies) into NCIC and/or TECS as appropriate. For the USNCB to place entries in domestic indices for fugitives or persons of interest to domestic agencies would be duplicative, an infringement on the role and authority of the primary investigating agencies, and a burden on USNCB resources. The USNCB is working with the Department of State to enhance the exchange of INTERPOL data for purposes of passport and visa adjudication. We have determined that the State Department Consular Lookout and Support System (CLASS) receives wanted person records in a daily push from NCIC to include USNCB entries on wanted persons.

As for timeliness, this is a high priority for the USNCB and we have made several changes to improve efficiency in this area. In August 2008, following the USNCB's NCIC Audit, we implemented a procedural change requiring the USNCB Command Center to make the NCIC entries on notices received during weekend hours. This ensures that the USNCB meets the NCIC's 24-hour entry requirement for federal agencies. More recently, the USNCB began entering into IAFIS fingerprints associated with foreign diffusions. Finally, as stated above, the USNCB will modify its policy to allow for the entry of foreign diffusions into NCIC so that this information will be available to the domestic law enforcement community.

Long-term, the USNCB is exploring the establishment of a 24/7 Notice Section that will allow for the uninterrupted processing of incoming foreign notices, and will improve the timeliness of related entries into U.S. lookout systems. We will continue to streamline and improve our processes in this area.

Recommendation 10. Develop procedures to ensure that any additional information the USNCB obtains that augments previously provided domestic law enforcement agency data is made available to all relevant agencies.

USNCB response: Agree. The USNCB has issued a policy directive and new case management procedures instructing caseworkers to query relevant databases to obtain additional data, such as identification and lead information, which may add value to the notices requested or diffusions sent by the USNCB on behalf of domestic agencies. In addition, this policy directs caseworkers to review all subsequent information obtained by the USNCB from other countries or other agencies that relates to an existing case, and ensure that it is provided to the domestic agency initiating the request on the subject and included in the USNCB's case file. Finally, the

directive requires that when any subsequent information relating to the subject of a notice is received, the USNCB will ensure the information is submitted to the INTERPOL General Secretariat (IPSG) as a request for addenda or corrigenda to the original notice, and to foreign counterparts and requestors as appropriate. The USNCB will include this policy in its new employee and refresher training programs. **We consider this recommendation closed.** (See Attachment A).

Recommendation 11. Provide domestic law enforcement agencies with access to INTERPOL information on stolen and lost travel documents.

USNCB response: Agree. Over the past several years, in an attempt to make stolen/lost travel document (SLTD) data more readily available to domestic state and local law enforcement, the USNCB enabled access to the SLTD database through an interface with the National Law Enforcement Telecommunications System (NLETS). In order to activate the query, NLETS state administrators must make technical modifications to local system configurations. To date, 21 states have made the necessary changes. The USNCB continues to encourage additional states to implement these modifications as their resources and policies permit. We note that INTERPOL policy does not allow for the wholesale downloading of INTERPOL SLTD data to national databases, therefore USNCB is unable to enter these records directly into TECS or NCIC.

Since the audit was performed in March 2008, the USNCB and FBI/CJIS agreed to test a direct connection between the NCIC system and INTERPOL for query purposes. The results of this pilot, currently ongoing for subject record queries, will determine if this interface can also deliver SLTD data to state and local law enforcement in a timely manner. We anticipate the completion of a preliminary assessment of the INTERPOL-NCIC interface pilot for subject records by the end of the calendar year.

Recommendation 12. Work with the FBI to assess the feasibility of developing and implementing a direct connection between the INTERPOL databases and NCIC.

USNCB Response: Agree. The USNCB is presently exploring with the FBI and the INTERPOL General Secretariat (IPSG) in Lyon, France, the possibility of integrating queries of INTERPOL databases into queries of NCIC by U.S. domestic authorities. In Spring 2009, the USNCB began a pilot project with the ultimate goal of federating NCIC wanted subject queries with queries of INTERPOL's Automated Search Facility/Nominal Database. The pilot project simulates the millions of subject record queries made each day to NCIC and runs these queries against INTERPOL databases to test the ability and capacity of INTERPOL systems to provide timely and accurate responses to the huge volume of queries by NCIC users. We anticipate the pilot to be completed and results assessed by the end of this calendar year. We will then address the technical, policy, legal, and resource requirements for integrating queries of INTERPOL databases by foreign counterparts to NCIC queries. The ability to check INTERPOL databases through a single NCIC query will provide U.S. law enforcement authorities the widest possible access to critical international information in real-time.

In the long term, the USNCB will also explore the feasibility of a business-to-business (B2B) solution for sharing investigative data between INTERPOL and U.S. database systems. (B2B involves the integration of database systems for high-volume search and response functions). It should be noted that a B2B model requires direct coordination with multiple domestic and international stakeholders, and would be a fundamental shift in INTERPOL's current philosophy of centralized storage of law enforcement data. Implementing this new approach, would require a clear and well defined IT sharing and security model, and has far-reaching resource implications. We believe that the USNCB is ideally positioned to provide a level of demarcation between INTERPOL and national systems in the United States, to allow for the proper control and validation of information flows between the two systems, in accordance with DOJ and INTERPOL security policies. The USNCB advocates the B2B concept through its representation in the INTERPOL Law Enforcement Advisory Group (ILETAG), the INTERPOL technical user group which is tasked with examining INTERPOL's current IT architecture to identify strategies for expanding information sharing regimes. The ILETAG will meet again in early FY2010.

Recommendation 13. Review existing USNCB-generated lookout records to ensure that the notice and diffusion information is accurate and consistent, including those identified by the OIG in this review as being inaccurate or inconsistent.

USNCB Response: Agree. The USNCB will review the OIG identified cases and make appropriate updates and corrections. Further, the USNCB will review all current TECS entries for accuracy. NCIC entries are reviewed annually through the NCIC validation process. The USNCB has issued a directive reminding Supervisors that they are required to review all TECS and NCIC entries made by subordinate caseworkers within 48 hours to ensure the accuracy and completeness of the information. All discrepancies are to be corrected immediately. Adherence to this policy is reviewed annually as part of the USNCB's Compliance Review Program.

Recommendation 14. Ensure that the notice and diffusion information retained in DHS's IDENT system and the FBI's IAFIS is compliant with the INTERPOL Rules for Processing Information. The USNCB should also coordinate with DHS and the FBI to implement an agreement regarding the inclusion of fingerprints and photographs in their internal databases. This agreement should describe the type of information to be shared, appropriate uses, retention period, removal requirements, and written confirmation of removal.

USNCB Response: Agree. Over the past two years, the USNCB has facilitated the download of INTERPOL fingerprint files to both the FBI and DHS for inclusion in the IAFIS and IDENT systems respectively. (IDENT makes INTERPOL fingerprint files available for use by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system.) This interim approach allowed us to ensure fingerprint files associated with known international criminals and terrorists would be readily available to U.S. law enforcement and border security agencies in real-time, until the IAFIS and IDENT systems were made compatible. Since the OIG audit was conducted in Spring 2008, USNCB has performed a review of files in DHS' IDENT and recommended the deletion of 250 fingerprint files, in accordance with the INTERPOL Rules for

the Processing of Information (RPI). While we have received email confirmation, we are requesting formal written confirmation of the deletion of these files by the DHS/US-VISIT Program Office. Further, FBI/CJIS has provided the USNCB with a list of all deletions completed since June 2008 and now provides the USNCB with confirmation on each IAFIS deletion request at the time the deletion is made.

Our ultimate goal is to use the FBI/CJIS IAFIS database as the central repository for INTERPOL fingerprint data in the United States, simplifying the updates/cancellations of the data by the USNCB and allowing FBI/CJIS to share the data with DHS/IDENT. Last year, the USNCB concluded an informal agreement with FBI/CJIS and the US-VISIT Program Office to include INTERPOL fingerprint records stored in IAFIS in the interim Data Sharing Model (iDSM). iDSM is an interagency initiative permitting NCIC information to be available to DHS personnel at ports of entry. Under the arrangement, the USNCB will continue to be responsible for creating and updating INTERPOL records in IAFIS. FBI/CJIS will ensure that users of IAFIS, including DHS personnel, have the most current information in conformity with the INTERPOL RPI. Full implementation of the iDSM will also allow DHS to discontinue the storage of any INTERPOL information, and to remove all INTERPOL information previously stored in the IDENT database. FBI/CJIS is presently conducting a Privacy Impact Assessment for the inclusion of INTERPOL-USNCB data into the iDSM. As the process moves forward the USNCB will seek to formalize the agreement. DHS and CJIS anticipate that iDSM will be fully implemented by end of FY2010. Until that time, the USNCB has implemented procedural changes to ensure that modifications to and deletions of INTERPOL records are communicated to US-VISIT for timely updates to the IDENT database.

Recommendation 15. Develop and implement automated processes to transmit INTERPOL information to U.S. agency systems.

USNCB Response: Agree. The USNCB will coordinate with stakeholders from NCIC, relevant domestic systems, and INTERPOL's General Secretariat (IPSG), to explore technological solutions for pushing INTERPOL updates/changes directly to NCIC. Such a system will require that IPSG develop push technology, as present systems allow only for pulling of INTERPOL subject records. Ultimately, the USNCB will pursue full system integration as a more efficient data sharing model, one that addresses data storage and maintenance concerns more effectively than the current central repository model.

Recommendation 16. Eliminate the backlog of notices and diffusions and develop procedures to regularly monitor the timeliness of workflow processes.

USNCB Response: Agree. As a stopgap measure, the USNCB utilized existing resources to address the current backlog. We anticipate that the backlog identified in the report will be eliminated by the end of this calendar year. We also have begun preliminary plans to conduct a "clean sweep" that will have agents, analysts, and supervisors work together to conduct a thorough review of all open and suspended cases. Evaluations of workflow processes and

workforce utilization will be elements of the USNCB's IT Strategic Plan, discussed in Recommendation 26, and its Human Capital Strategic Plan, discussed in Recommendation 20. In the long-term, several planned initiatives should greatly improve the USNCB ability to monitor the timeliness of workflow processes. These include deployment of USNCB's new management system, Customer Relationship Management Software (CRM), and related workflow processes designed to provide a supervisory notification of inactivity for all assigned tasks. In the interim, USNCB will monitor the timely handling of notices/diffusions through a weekly report of those cases with no activity.

Recommendation 17. Review all active notices and diffusions to ensure that appropriate database searches have been conducted.

USNCB Response: Agree. Over the last several months, the USNCB has utilized existing resources to address a backlog of 1,537 cases requiring additional database searches. As of 24 July 2009, 1173 cases had been completed, and we will continue to work on the backlog until it is eliminated. Consequently, the USNCB submitted funding requests for FY2011 for additional resources to fully staff our Command Center and ensure our Notices Section can operate 24/7. In the meantime, as part of the USNCB Human Capital Strategic Planning process, we will look to additional workforce utilization techniques to prevent future backlogs.

The USNCB Compliance Officer will provide a weekly report to USNCB Assistant Directors (ADs) and Supervisory Analysts identifying all open and suspended diffusion and notice cases where no query has been performed. ADs and Supervisors will be responsible for ensuring that searches are conducted in a timely manner. The previously mentioned "clean sweep" project (Recommendation 16) will help the USNCB catch any and all previously unidentified cases.

Recommendation 18. Develop and implement policies and procedures, including technological solutions, to determine if subjects of INTERPOL notices and diffusions have entered the United States subsequent to the receipt of the notice or diffusion.

USNCB Response: Agree. The USNCB maintains approximately 40,000 subject lookouts in the TECS system for the primary purpose of being alerted by U.S. Customs and Border Protection (CBP) if an INTERPOL wanted subject enters the country. In order to more accurately track movements of INTERPOL fugitives and wanted persons and share that information with appropriate domestic and international counterparts, the USNCB has asked DHS to provide supplemental data concerning secondary inspection results and disposition of cases involving passengers who were referred to CBP secondary inspection based on INTERPOL lookouts (i.e., TECS IO-95 query results). CBP has advised the USNCB that they are reviewing our request for expanded access to TECS and disposition of cases. The USNCB has directed caseworkers to re-query TECS crossing data each time a suspended case reaches its review date. USNCB will explore, with DHS/CBP, the feasibility of routine batch load comparisons of INTERPOL wanted person data against TECS crossing data.

Recommendation 19. Develop a formalized process to ensure that searches of federal law enforcement agency databases have been conducted on subjects of foreign notices or diffusions to determine if they are persons of interest to these agencies.

USNCB Response: Agree. Presently, the USNCB checks INTERPOL notices and diffusions against TECS, NCIC, and NADDIS (Narcotics and Dangerous Drugs Information System) to determine if subjects of international interest are wanted or have a criminal history in the United States. In addition, agents assigned to the USNCB from approximately 23 federal agencies have access to their agencies' databases. The USNCB will seek to increase staffing from its participating agencies to ensure routine checking of agency internal databases to identify common targets. In order to facilitate this effort, the USNCB will examine the technical feasibility of pushing weekly lists of INTERPOL notices and diffusions to its participating law enforcement agencies.

The USNCB will work with its participating agencies, the ODAG and the DOJ Office of the Chief Information Officer (OCIO) to explore technical mechanisms that would enable routine searches of INTERPOL data against US agency databases.

Recommendation 20. Develop the capability to use INTERPOL information to identify trends and patterns in international criminal activities, such as transnational organized crime.

USNCB Response: Agree. The USNCB recognizes the potential for using the wealth of criminal data that is available at USNCB and is obtainable through INTERPOL channels to perform criminal intelligence analysis. Our unique access to 18,000 domestic law enforcement agencies and 186 INTERPOL counterparts positions the USNCB to develop and disseminate substantive law enforcement analytical products. We recognize that this objective will require integrating both human and technology systems.

Working within the confines of current resource limitations, the USNCB's efforts have included developing and recruiting personnel for key occupational specialties such as analysts specializing in gangs and child exploitation. The USNCB will seek to train these personnel, both in-house and externally, in analytical techniques associated with their specialties. In April 2008, the USNCB arranged for a 2-week Federal Law Enforcement Analysts Training (FLEAT) course developed in cooperation with the Drug Enforcement Administration, specifically for INTERPOL Analysts. We have provided in-house training on analytics through commercial vendors. While our ad-hoc efforts have made small advances in capability, the USNCB management team recognized that a more concerted and focused effort was needed. Consequently, the USNCB Training Committee was established in February 2009 to begin to identify specific gaps in current capabilities and make recommendations for training and development that would bridge those gaps. To bolster the Training Committee's efforts, the USNCB is in the process of entering into a reimbursable agreement with the Office of Personnel Management's Training and Management Assistance Program to assist us in analyzing, designing, developing, implementing, and evaluating customized training, learning, knowledge management, and human resource management. With this tool in place, the USNCB will both establish curricula

to ensure analytical capabilities are developed and build a Human Capital Strategic Plan to carry this organization forward.

The USNCB will develop a formal IT Strategic Plan as recommended in the OIG report. Our plan will not only address the items proposed in Recommendation 26, but will include identifying tools that will strengthen the analytical capabilities of USNCB personnel. The USNCB has already begun to procure certain off-the-shelf IT tools, such as i2 Analyst's Notebook, and we are incorporating them into our IT systems (i2 Analyst's Notebook is an off-the-shelf, state of the art visual investigative analysis software program).

Recommendation 21. Develop procedures to ensure that information is added to an existing case only if additional information is available to confirm the identity of the subject, such as fingerprints and photographs. In the absence of this additional information, a new case on the subject should be opened and linked to the original case.

USNCB Response: Agree. The USNCB has implemented new procedures to ensure that dispatchers confirm the following data before saving a new request to an existing case: name, date of birth, place of birth, parents' names, and requesting country. We will also use photo and fingerprints whenever possible. The new policy instructs caseworkers to create a new case file when they are unable to confirm, with confidence, that a new subject matches the identity of an existing record. If a new request about a subject for whom the USNCB maintains an existing record is received from a different country than the country identified in the existing case, a new case will be opened and cross-referenced. **We consider this recommendation closed.** (See Attachment B).

Recommendation 22. Ensure that its case management system provides the ability to: (a) adequately maintain, control, and dispose of case-related information, including access restrictions by user and audit trails; (b) compile management statistics; and (c) generate standardized correspondence.

USNCB Response: Agree. The USNCB is currently developing a case management system using Customer Relationship Management (CRM) software. The next phase of the CRM project will address integration with the current case management system; define user roles and access rights; and build in tools to appropriately archive and dispose of case-related data. The USNCB is developing improved reports for compiling management statistics.

Additionally, USNCB will provide managers and supervisors with access to a 'dashboard' where they can view statistics for their respective divisions' and subordinates' work performance. Statistics will include messages sent, cases opened, and items in queue. The dashboard will contain links to a user portal where ad hoc reports can be generated and exported to Excel spreadsheet software. This capability will allow USNCB managers to effectively administer resources and to identify productivity problems. Further, the evaluation of additional audit and statistical requirements will be incorporated into current and future development projects.

CRM will provide standard message templates for use by the USNCB's investigative divisions. Finally, as discussed in Recommendation 26, the USNCB will initiate a comprehensive IT strategic planning process to assess legacy systems and current IT plans, to chart a roadmap toward future IT objectives.

Recommendation 26. Develop a formal IT plan that systematically evaluates current operations and uses of data and accounts for the various ways in which INTERPOL information might potentially be used and accessed by other agencies. This plan should address: (a) IT staffing needs, (b) controls to ensure data integrity, and (c) future improvements in the areas of database inter-connectivity.

USNCB Response: Agree. The USNCB will work with DOJ OCIO, DHS OCIO, IPSPG and the USNCB Executive Committee, to formalize an IT Strategic Plan. A critical first step will be to identify an IT Strategic Planning consultant to assist us in conducting an IT assessment that addresses visioning, strengths, weaknesses, opportunities, threats, and constraints. This external assessment will lead to identifying immediate solutions and help to chart the path forward. The USNCB's IT staff has begun preliminary discussions with both the OCIO's office and IPSPG to review and develop the current approach to delivering INTERPOL services throughout the United States. These discussions will be critical to ensuring that USNCB's plan and IT architecture are congruent and compatible with INTERPOL and the Department of Justice.

Recommendation 27. Work to develop formal agreements with domestic and federal law enforcement agencies regarding staffing commitments and length-of-duty assignments.

USNCB Response: Agree. The USNCB has developed a model MOU for use with outside agencies for the purpose of securing commitments for staffing and funding of the USNCB. The USNCB hopes to expand a staffing initiative for our domestic state and local law enforcement agencies to the federal law enforcement agencies within the Departments of Justice and Homeland Security. Successful implementation of Recommendation 1 as well as the Human Capital Strategic Plan referenced in Recommendation 20 should provide the support and legal framework for long-term staffing arrangements between USNCB and its federal participating agencies. The support of the ODAG and DHS Deputy Secretary in concluding such arrangements will be critical, as agencies may be reluctant to commit scarce resources to another agency in a time of shrinking budgets. USNCB will examine its staffing needs with a view to prioritizing a list of agencies with which to engage in an MOU.

DEPARTMENT OF JUSTICE RESPONSE



U.S. Department of Justice

Office of the Deputy Attorney General

Washington, D.C. 20530

August 3, 2009

Mr. Raymond J. Beaudet
Assistant Inspector General
Office of the Inspector General
U.S. Department of Justice
1425 New York Avenue
Suite 5000
Washington, D.C. 20005

Subject: Draft Audit Report – The United States National Central Bureau (USNCB)

Dear Mr. Beaudet:

Thank you for providing your Draft Audit Report dated July 13, 2009, to the Office of the Deputy Attorney General for our review and comment. We appreciate the thoroughness of your report, your thoughtful recommendations, as well as the opportunity to comment on those recommendations.

Under the new leadership of Deputy Attorney General David Ogden, this office is committed to working closely with the Department of Homeland Security and taking a more active role in the management of the USNCB. Your report is a very helpful tool in making that transition efficiently and effectively.

Attached, please find our responses to Recommendations 1, and 23 to 25, which were directed at this office.

Should you have any questions regarding our response, please do not hesitate to contact me at (202) 616-1621 or Candace.Kelly2@usdoj.gov.

Very Truly Yours,

A handwritten signature in black ink that reads "C. Kelly".

Candace Kelly
Senior Counsel to the Deputy Attorney General

Attachment

Recommendation 1. Work with DHS, the USNCB, and the USNCB Executive Committee to establish formal agreements between federal law enforcement agencies that describe the type of case information these agencies should share with foreign counterparts through the INTERPOL network.

Response: Agree in part. We agree that it is critical that law enforcement information about international criminals be communicated to our foreign partners efficiently and effectively. INTERPOL is one of a number of options for sharing investigative information with the international law enforcement community, but it is not the exclusive method to accomplish this goal. Each agency and each investigation has unique characteristics and sensitivities. Accordingly, each agency must choose the option for information sharing that best suits the needs of the investigation. To make an informed choice, the agencies must be well versed in the capabilities of each of the communication methods – including INTERPOL. We recognize that some U.S. law enforcement agencies may not be well informed on the capabilities and usefulness of INTERPOL and that is a situation that must be rectified. As an initial step, the Office of the Deputy Attorney General (“ODAG”) will support the USNCB in its outreach efforts to educate U.S. law enforcement agencies on the merits of using INTERPOL tools and information network.

ODAG will also work with the USNCB and the USNCB Executive Committee to explore whether formal agreements with U.S. law enforcement agencies can be drafted in a way that that allows for sufficient flexibility to meet the unique needs of each agency and each investigation. We are concerned that formal agreements may not lend themselves to the necessary level of flexibility, so we will also consider the option of accomplishing the same goal through policy directives and guidance to U.S. law enforcement agencies.

Recommendation 23. Ensure that the Executive Committee meets as prescribed in the MOU and takes the lead in developing a new strategic plan for the USNCB.

Response: Agree. The Deputy Attorney General will hold a meeting of the USNCB Executive Committee within 60 days to address issues related to the management of the agency and the development of a new strategic plan. This meeting will be followed by additional meetings to be held as necessary, but at a minimum, every quarter. Additionally, ODAG has instituted monthly component meetings with USNCB’s Director and Deputy Director to establish and maintain a close working relationship between the two offices.

Recommendation 24. Evaluate options to enhance the USNCB’s executive management structure to help ensure identification of the most qualified candidates for its senior executive positions. Potential enhancements might include adopting a higher-ranking level for the Director and Deputy Director positions, eliminating the practice of the Deputy Director succeeding the outgoing Director at the end of the 3-year term, and revising the term length.

Response: Agree. ODAG will work with the Office of the Deputy Secretary to review the current executive management structure of the USNCB and explore options for improvement.

Additionally, ODAG has already begun to work with the USNCB and its Executive Committee to begin the selection process for the USNCB's Deputy Director, which will become vacant in early FY10.

Recommendation 25. Determine the best method to budget and pay for the United States' membership dues to INTERPOL to help minimize the operational impact on the USNCB.

Response: Agree. ODAG will work with Department's Controller and the Justice Management Division to determine the best mechanism for payment of U.S. financial obligations to INTERPOL and to ensure that future increases to U.S. INTERPOL dues do not negatively impact USNCB's operating budget.

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

The OIG provided the USNCB and the ODAG a draft of this audit report for review and comment. We also provided a draft of this audit report to the FBI and DEA for their review of those portions of our report pertaining to their agencies. Our report did not include any recommendations addressed to the FBI or DEA, and the DEA provided no comments on our report. The FBI provided technical clarifications on a small number of items in the report and, where appropriate, we adjusted language in the report to reflect these clarifications. The USNCB stated that it agreed with the 23 recommendations we made to the USNCB, and the ODAG stated that it agreed with the 4 recommendations we directed to the ODAG. The comments that we received from the USNCB and ODAG, which detail the actions taken or plans for implementing our recommendations, have been incorporated in Appendices IX and X, respectively.¹¹¹ Our analysis of these responses and a summary of the actions necessary to close each recommendation is presented below.

Recommendation Number:

1. **Resolved.** The ODAG agreed in part with our recommendation to work with DHS, the USNCB, and the USNCB Executive Committee to establish formal agreements between federal law enforcement agencies that describe the type of case information these agencies should share with foreign counterparts through the INTERPOL network. According to the ODAG, it agrees that critical law enforcement information about international criminals should be communicated to foreign partners efficiently and effectively, but that INTERPOL is only one of a number of options to accomplish this task. The ODAG further stated that each agency and investigation is unique, and therefore each agency must select its best option for sharing the information according to the needs of the investigation. The ODAG also acknowledged that some U.S. law enforcement agencies might not know of INTERPOL's capabilities and that this must be corrected.

The ODAG stated that it will support the USNCB in the USNCB's efforts to reach out and educate U.S. law enforcement agencies on INTERPOL's services. The ODAG also stated that it will work with the USNCB and USNCB Executive Committee to determine whether formal agreements can be developed with U.S. law enforcement agencies that

¹¹¹ The USNCB's response included two attachments. We have not included these attachments in our report due to their technical nature.

can provide enough flexibility to meet the unique needs of each agency and investigation. The ODAG further stated that it will consider accomplishing this goal through policy directives and guidance to U.S. law enforcement agencies.

We believe that the ODAG's statements are responsive to our recommendation and underlying finding that increased participation and cooperation between the USNCB and its domestic partners should be encouraged and supported.

This recommendation can be closed when the ODAG provides evidence of its support of the USNCB's outreach efforts. Additionally, the ODAG should provide copies of the formal agreements with federal law enforcement agencies or policies and guidance that describe the type of case information these agencies should share with foreign counterparts through the INTERPOL network.

2. **Resolved.** The USNCB agreed with our recommendation to work with domestic law enforcement partners to ensure that the agencies issue INTERPOL notices for appropriate international fugitives, particularly those already publicly identified on the agencies' websites or elsewhere. The USNCB stated that it has implemented policy and procedures to regularly monitor U.S. 'Most Wanted' programs to identify subjects for inclusion in INTERPOL's notice program. The USNCB stated that it will contact the appropriate U.S. law enforcement agencies to ensure that they are advised on INTERPOL's notice program and will provide assistance to issue INTERPOL notices for those fugitives where international leads have been or may be identified. Additionally, the USNCB stated that the Assistant Directors of its investigative divisions will report in monthly significant activity reports the publication of notices for these types of subjects. Further, the USNCB stated that it will document cases where an agency has declined to pursue a notice publication on the basis of investigative considerations.

In addition, the FBI advised that its Office of International Operations has mandated that the FBI seek the issuance of red notices for all Top Ten Fugitives and Most Wanted Terrorists.

This recommendation can be closed when the USNCB provides evidence of its efforts to advise U.S. law enforcement agencies on INTERPOL's notice program. Additionally, the USNCB should provide a copy of its policy requiring regular monitoring of "most wanted"

programs and examples of monthly significant activity reports that contain mention of this monitoring.

3. **Resolved.** The USNCB agreed with our recommendation to encourage federal law enforcement agencies to provide USNCB and INTERPOL-related training to their employees. The USNCB stated that it is in the process of formalizing a training outreach plan and developing an INTERPOL-USNCB training course for all Federal Law Enforcement Training Center (FLETC) law enforcement and analytical trainees. Once established, the USNCB will consider using the training program at the FBI and DEA academies in Quantico, Virginia.

The USNCB also said that it has initiated specialized INTERPOL database training for various components of DOJ and DHS and has provided refresher training to the DHS Law Enforcement Support Center (LESC). Moreover, the USNCB said that it will continue to work with its law enforcement partners and the INTERPOL General Secretariat to enhance INTERPOL training opportunities for the U.S. law enforcement community.

This recommendation can be closed when we receive a copy of the USNCB's formalized training outreach plan and additional information regarding the FLETC INTERPOL-USNCB training course, including evidence that the course has been scheduled as a regular part of the curriculum for FLETC trainees. Please also submit an update on progress made in developing a media program for training and whether it is being used at the FBI and DEA. Additionally, the USNCB should provide documentation of the INTERPOL database training and evidence of the USNCB's efforts to work with the INTERPOL General Secretariat to augment training opportunities for the U.S. law enforcement community.

4. **Resolved.** The USNCB agreed with our recommendation to develop a method for domestic law enforcement agencies to submit a notice application electronically. The USNCB stated that it will utilize a contractor and develop a plan to implement a web portal called "IPOLNET" that will allow domestic law enforcement agencies to submit electronic notice applications in a format compatible with the USNCB case management system. The USNCB stated that it anticipates completion of IPOLNET by the end of FY 2010 and that it will develop training methods to accompany the electronic notice application form. The USNCB also said that in the interim it will continue to facilitate the electronic submission of notice applications by domestic law

enforcement agencies via existing infrastructure (e.g., secure e-mail, Regional Information Sharing System, and Law Enforcement Online).

This recommendation can be closed when the USNCB provides us with evidence that IPOLNET has been implemented and that it provides a method for domestic agencies to submit notice applications electronically. Additionally, while IPOLNET is in development the USNCB should provide evidence of its efforts to facilitate electronic notice submissions using existing infrastructure.

5. **Resolved.** The USNCB agreed with our recommendation to implement information technology solutions to more broadly share U.S. stolen motor vehicle information with INTERPOL members. According to the USNCB, the FBI's Criminal Justice Information Services (CJIS) component allows limited foreign country access to U.S. stolen motor vehicle data through a USNCB-CJIS interface. However, the FBI has not supported the uploading of U.S. data into the INTERPOL database due to the volume of these data transactions. The USNCB further stated that CJIS has reported that it does not possess the required approval from the NCIC Advisory Policy Board (APB) to authorize full INTERPOL access through the interface. The USNCB said that it will re-engage the FBI and the INTERPOL General Secretariat to explore whether these agencies will support making the necessary legal and policy changes (and subsequent technical and procedural changes) to U.S. and INTERPOL systems to allow more INTERPOL countries access to U.S. stolen motor vehicle files through a proposed NCIC-INTERPOL interface.

This recommendation can be closed when we receive evidence of the USNCB's efforts to re-engage the FBI and the INTERPOL General Secretariat on this matter, as well as the final result of this interaction.

6. **Resolved.** The USNCB agreed with our recommendation to ensure that a reliable communications network is maintained with all state and local liaison offices. The USNCB stated that currently it communicates with its State Liaison Offices using existing secure networks and the Regional Information Sharing System Networks (RISS) as a backbone. The USNCB stated that it will improve monitoring of these connections by polling each State Liaison e-mail server. Additionally, the USNCB State and Local Liaison Division will undertake a monthly poll of individual offices for any personnel changes in the user directory to avoid communication errors. The USNCB stated that in the future its "IPOLNET" web portal will support expanded networking capability for its State Liaison Offices.

This recommendation can be closed when the USNCB provides evidence of its polling of state liaison e-mail servers and individual offices, as well as the results of these polls. Also, the USNCB should provide evidence of how the IPOLNET web portal supports expanded networking capability for the state liaison offices.

7. **Resolved.** The USNCB agreed with our recommendation to develop a formal outreach plan that identifies and prioritizes law enforcement organizations that would benefit from a better understanding of the USNCB and INTERPOL. In addition, the USNCB stated that it will continue to explore areas to enhance INTERPOL training and raise awareness within the U.S. law enforcement community. The USNCB also said that it will improve its statistical reporting capability to better identify and prioritize those law enforcement agencies that would most benefit from USNCB outreach programs.

This recommendation can be closed when we receive the USNCB's formal outreach plan, as well as evidence of how its improved statistical reporting capability better identifies and prioritizes those agencies that would most benefit from USNCB outreach.

8. **Resolved.** The USNCB agreed with our recommendation to review current and incoming green notices and determine if they are appropriate for inclusion in NCIC. The USNCB stated that it has received approval from the FBI's CJIS to enter foreign-issued INTERPOL green notices on gang-related offenders into the Violent Gang and Terrorist Offender File (VGTOF), and the USNCB will begin making these entries once the USNCB and CJIS have implemented necessary system modifications. The USNCB also stated that it submitted a request to the NCIC Advisory Policy Board (APB) to propose the inclusion of INTERPOL foreign-issued green notice information on sexual offenders into the NCIC Sexual Offender File. The USNCB stated that in the interim it will identify all active foreign green notice cases to determine those eligible for inclusion into the appropriate NCIC files, update the offense codes in the USNCB case management database, and issue revised handling procedures to ensure that newly published green notices are appropriately reviewed for inclusion into the NCIC VGTOF or Sexual Offender Files.

This recommendation can be closed when USNCB provides evidence that it is entering foreign-issued INTERPOL green notices on gang-related offenders into VGTOF. Further, the USNCB should provide evidence of its efforts to: (1) identify all active foreign green notice

cases to determine those eligible for inclusion into the appropriate NCIC files, (2) update the offense codes in the USNCB case management database, and (3) issue revised handling procedures to ensure that newly published green notices are appropriately reviewed for inclusion in the NCIC VGTOF or Sexual Offender Files.

9. **Resolved.** The USNCB agreed with our recommendation to modify its policies and procedures regarding notice and diffusion information to ensure that the appropriate data is shared with U.S. agency databases and is made available to domestic law enforcement personnel in a timely manner. The USNCB noted that its procedures for handling notice and diffusion information must differentiate between foreign and domestic-issued notices and diffusions because U.S. law enforcement agencies are responsible for placing entries on their fugitives and subjects of interest into national lookout systems while the USNCB is responsible for placing entries on subjects of foreign INTERPOL notifications into U.S. lookout systems. The USNCB stated that on August 1, 2009, USNCB staff began making NCIC entries on subjects of foreign diffusions when NCIC criteria are met. In addition, the USNCB stated that it will make entries on foreign-issued notices and diffusions in either NCIC or TECS, but not both because TECS queries are incorporated into NCIC queries, which enables TECS users access to USNCB entries in NCIC.

The USNCB further stated that it is working with the Department of State to enhance the exchange of INTERPOL data for purposes of passport and visa application reviews and that it has determined that the State Department Consular Lookout and Support System (CLASS) receives wanted person records daily from NCIC and this includes USNCB wanted persons entries.

The USNCB stated that it has made several changes to improve its timeliness. According to the USNCB, it is exploring the establishment of a 24/7 Notice Section that will allow for the uninterrupted processing of incoming foreign notices and will improve the timeliness of related entries into U.S. lookout systems. The USNCB also stated that it will continue to streamline and improve its processes in this area.

We agree with the USNCB that its procedures for handling notice and diffusion information will differ between foreign and domestic-issued notices and diffusions. However, because representatives from many law enforcement agencies are stationed at the USNCB, we believe that the USNCB is in a unique position to help consolidate and streamline

the sharing of international criminal information. We do not believe that the USNCB should be responsible for entering information into all of the various databases. Nonetheless, the USNCB can help ensure that the information is shared.

This recommendation can be closed when we receive evidence that the USNCB has modified its policies and procedures regarding notice and diffusion information to ensure that the appropriate data is shared with U.S. agency databases, including both foreign and domestic-issued notices and diffusions. In addition, the USNCB should provide us with more information regarding the establishment of a 24/7 Notice Section.

10. **Closed.** The USNCB agreed with our recommendation to develop procedures to ensure that any additional information the USNCB obtains that augments previously provided domestic law enforcement agency data is made available to all relevant agencies. The USNCB provided a copy of a memorandum containing a policy directive and new case management procedures designed to ensure continuous information sharing. The USNCB also stated that it will include this policy in its new employee and refresher training programs. We consider this action sufficient to close this recommendation.
11. **Resolved.** The USNCB agreed with our recommendation to provide domestic law enforcement agencies with access to INTERPOL information on stolen and lost travel documents. According to the USNCB, over the past several years, in an attempt to make information from the Stolen and Lost Travel Document (SLTD) database more readily available to U.S. state and local law enforcement, the USNCB enabled access to the SLTD database through an interface with the International Justice and Public Safety Information Sharing Network (Nlets). However, to activate the access Nlets state administrators must make technical modifications to local system configurations. The USNCB stated that as of August 3, 2009, 21 states had made the necessary changes, and the USNCB continues to encourage additional states to implement these modifications as their resources and policies permit. The USNCB noted that because INTERPOL policy does not allow for the wholesale downloading of INTERPOL SLTD data to national databases, the USNCB is unable to enter these records directly into TECS or NCIC.

The USNCB also stated that the USNCB and FBI's CJIS have agreed to test a direct connection between the NCIC system and INTERPOL for query purposes. The results of this initiative will determine if this

interface can also deliver SLTD data to state and local law enforcement in a timely manner. The USNCB stated that it anticipates a preliminary assessment of the initiative by the end of 2009.

This recommendation can be closed when we receive evidence that the 21 states have access to SLTD data and that the USNCB is encouraging the remaining states to make the necessary changes needed to activate similar access. In addition, the USNCB should provide us with the results of the preliminary assessment of the INTERPOL-NCIC interface initiative for the subject records.

12. **Resolved.** The USNCB agreed with our recommendation to work with the FBI to assess the feasibility of establishing a direct connection between the INTERPOL databases and NCIC. The USNCB stated that it has initiated a pilot project to assess the feasibility of integrating NCIC and INTERPOL queries and that it anticipates the pilot to be completed and results assessed by the end of this calendar year. The USNCB stated that it will then address the technical, policy, legal, and resource requirements for similar integration for foreign counterparts conducting INTERPOL queries.

The USNCB stated that in the long term it will explore other solutions for sharing investigative data between INTERPOL and U.S. database systems. These solutions involve the integration of database systems for high-volume search and response functions. However, the USNCB anticipates that implementing the new processes will require direct coordination with multiple domestic and international stakeholders, which would be a fundamental shift in INTERPOL's current philosophy of centralized storage of law enforcement data.

This recommendation can be closed when we receive the USNCB's assessment of the results of the pilot project aimed at integrating NCIC wanted subject queries with queries of INTERPOL data. In addition, the USNCB should provide us with the results of its efforts to address technical, policy, legal, and resource requirements for similar integration of INTERPOL queries by foreign counterparts. Lastly, the USNCB should provide information on its progress to develop a more far-reaching information technology solution.

13. **Resolved.** The USNCB agreed with our recommendation to review existing USNCB-generated lookout records to ensure that the notice and diffusion information is accurate and consistent, including those identified by the OIG in this review.

The USNCB stated that it has issued a directive reminding supervisors that they are required to review all TECS and NCIC entries made by subordinate caseworkers within 48 hours to ensure the accuracy and completeness of the information, and that all discrepancies are to be corrected immediately.

This recommendation can be closed when the USNCB provides evidence that it has reviewed the OIG-identified cases and made appropriate updates and corrections. Additionally, the USNCB should provide a copy of the directive reminding supervisors that they are required to review all TECS and NCIC entries made by subordinate caseworkers within 48 hours and that all discrepancies are to be corrected immediately.

14. **Resolved.** The USNCB agreed with our recommendation to ensure that the notice and diffusion information retained in the FBI's IAFIS and DHS's IDENT system is compliant with the INTERPOL Rules for Processing Information. The USNCB stated that it ultimately intends to use the FBI's IAFIS database as the central repository for INTERPOL fingerprint data in the United States. The USNCB said that in 2008 it concluded an informal agreement with the FBI and DHS to include INTERPOL fingerprint records stored in IAFIS in the interim Data Sharing Model (iDSM), an interagency initiative permitting NCIC information to be available to DHS personnel at ports of entry. Under the arrangement, the USNCB stated that it will continue to be responsible for creating and updating INTERPOL records in IAFIS, while the FBI's CJIS will ensure that users of IAFIS, including DHS personnel, have the most current information. The USNCB also stated that full implementation of the iDSM will allow DHS to discontinue the storage of any INTERPOL information and to remove all INTERPOL information previously stored in the IDENT database. The USNCB stated that DHS and CJIS anticipate that iDSM will be fully implemented by end of FY 2010, and until that time the USNCB has implemented procedural changes to ensure that modifications to and deletions of INTERPOL records are communicated to DHS for timely updates to the IDENT database.

Further, the USNCB stated that it has performed a review of files in IDENT for compliance with the INTERPOL rules and recommended the deletion of 250 fingerprint files. The USNCB is currently awaiting formal written confirmation of the deletion of these files.

This recommendation can be closed when we receive documentation supporting the USNCB's policies and procedures regarding inclusion of

INTERPOL fingerprints in IAFIS and IDENT, including the agreement with the FBI regarding inclusion of fingerprints in IAFIS. In addition, pending implementation of the iDSM, the USNCB should provide copies of agreements between the USNCB, FBI, and DHS regarding the inclusion, use, and deletion of INTERPOL fingerprint records. Once the iDSM has been fully implemented, the USNCB should provide a copy of the formal agreements between the USNCB, FBI, and DHS regarding the storage and use of INTERPOL fingerprints, as well as documentation that the 250 INTERPOL fingerprints contained within IDENT have been deleted.

15. **Resolved.** The USNCB agreed with our recommendation to develop and implement automated processes to transmit INTERPOL information to U.S. agency systems. The USNCB stated that it will coordinate with personnel from NCIC, relevant domestic agencies, and INTERPOL's General Secretariat to explore technological solutions for pushing INTERPOL data directly to NCIC. The USNCB stated that ultimately it will pursue full system integration as a more efficient data sharing model.

This recommendation can be closed when the USNCB provides evidence that it has developed automated processes to transmit INTERPOL information to U.S. agency systems. In the interim, the USNCB should provide evidence of its coordination with various stakeholders to develop a technological solution for accomplishing this task.

16. **Resolved.** The USNCB agreed with our recommendation to eliminate the backlog of unissued or unprocessed notices and diffusions and develop procedures to regularly monitor the timeliness of workflow processes. The USNCB stated that it has utilized existing resources to address the current backlog and anticipates that the backlog identified in our report will be eliminated by the end of 2009. The USNCB also stated that it has begun planning for a "clean sweep" that will have agents, analysts, and supervisors work together to conduct a thorough review of all open and suspended cases.

The USNCB stated that it believes that in the long term several planned initiatives should greatly improve its ability to monitor the timeliness of workflow processes. In the interim, the USNCB stated that it will monitor the timely handling of notices and diffusions through a weekly report of those cases with no activity.

This recommendation can be closed when the USNCB provides evidence that the notice and diffusion backlog identified in the report has been eliminated. Additionally, the USNCB should provide the results of its “clean sweep” review of all open and suspended cases and evidence of weekly reports with no activity.

17. **Resolved.** The USNCB agreed with our recommendation to review all active notices and diffusions to ensure that appropriate database searches have been conducted. The USNCB stated that over the last several months it has utilized existing resources to address a backlog of 1,537 cases requiring additional database searches, and as of July 24, 2009, 1,173 cases had been completed. The USNCB stated that it has submitted funding requests for FY 2011 for additional resources to fully staff its Command Center and ensure its Notices Section can operate around the clock. In the meantime, as part of the USNCB Human Capital Strategic Planning process, the USNCB stated that it will look to additional workforce utilization techniques to prevent future backlogs. The USNCB Compliance Officer will provide a weekly report to USNCB Assistant Directors and Supervisory Analysts identifying all open and suspended diffusion and notice cases where no query has been performed and Assistant Directors and Supervisors will be responsible for ensuring that searches are conducted in a timely manner.

This recommendation can be closed when the USNCB provides evidence that it has completed the review of cases requiring additional database searches. Additionally, the USNCB should provide evidence of its Compliance Officer's weekly report and the subsequent action taken on those cases identified in the report as having had no query performed.

18. **Resolved.** The USNCB agreed with our recommendation to develop and implement policies and procedures, including technological solutions, to determine if subjects of INTERPOL notices and diffusions have entered the United States subsequent to the receipt of the notice or diffusion. The USNCB noted that it maintains approximately 40,000 subject lookouts in the TECS system so that the USNCB will be alerted by U.S. Customs and Border Protection (CBP) if the subject of an INTERPOL red notice enters the country. The USNCB also stated that to more accurately track movements of INTERPOL fugitives and wanted persons and share that information with appropriate domestic and international counterparts, it has asked DHS to provide supplemental data concerning secondary inspection results and the disposition of cases involving passengers who were referred to CBP

secondary inspection based on INTERPOL lookouts. According to the USNCB, CBP has advised that it is reviewing the USNCB's request. The USNCB stated that it has directed caseworkers to re-query TECS each time a suspended case reaches its review date and that the USNCB will explore with CBP the feasibility of routine high-volume batch comparisons of INTERPOL wanted-persons data against TECS data.

This recommendation can be closed when we receive evidence of the direction given to USNCB caseworkers to re-query TECS each time a suspended case reaches its review date. The USNCB should also provide updated information on its request for expanded access to TECS and disposition of cases and its discussions with CBP regarding the possibility of routine high-volume batch comparisons of INTERPOL wanted-persons data against TECS data.

19. **Resolved.** The USNCB agreed with our recommendation to develop a formalized process to ensure that searches of federal law enforcement agency databases have been conducted on subjects of foreign notices and diffusions to determine if they are persons of interest to these agencies. According to the USNCB, it checks INTERPOL notices and diffusions against TECS, NCIC, and NADDIS (Narcotics and Dangerous Drugs Information System) to determine if subjects of international interest are wanted or have a criminal history in the United States. The USNCB added that agents assigned to the USNCB from approximately 23 federal agencies also have access to their agencies' databases. The USNCB stated that it will seek to increase staffing from its participating agencies to ensure routine checking of agency internal databases to identify common targets, and to facilitate this effort the USNCB will examine the technical feasibility of pushing weekly lists of INTERPOL notices and diffusions to its participating law enforcement agencies. The USNCB also stated that it will work with its participating agencies, the ODAG, and the DOJ Office of the Chief Information Officer to explore technical solutions that would enable routine searches of INTERPOL data against U.S. agency databases.

This recommendation can be closed when we receive evidence of the USNCB's efforts to increase staffing from its participating agencies to ensure routine checking of agency internal databases to identify common targets. Additionally, the USNCB should provide the results of its efforts to send weekly lists of INTERPOL notices and diffusions to participating law enforcement agencies, as well as its efforts to explore technical solutions that would enable routine searches of INTERPOL data against U.S. agency databases.

20. **Resolved.** The USNCB agreed with our recommendation to develop the capability to use INTERPOL information to identify trends and patterns in international criminal activities, such as transnational organized crime. The USNCB stated that its current efforts have included developing and recruiting personnel for key occupational specialties, such as analysts specializing in gangs and child exploitation. The USNCB stated that it will seek to train these personnel, both in-house and externally, in analytical techniques associated with their specialties.

The USNCB stated that it has provided in-house training on analytics through commercial vendors, and while its ad-hoc efforts have made small advances in capability, the USNCB management team recognized that a more concerted and focused effort was needed. Consequently, the USNCB Training Committee was established in February 2009 to begin to identify specific gaps in current capabilities and make recommendations for training and development that would bridge those gaps. According to the USNCB, to bolster the Training Committee's efforts the USNCB is in the process of entering into a reimbursable agreement with the Office of Personnel Management's Training and Management Assistance Program to assist it in analyzing, designing, developing, implementing, and evaluating customized training, learning, knowledge management, and human resource management. The USNCB also stated that it intends to strengthen its IT environment and that through this effort the USNCB hopes to develop automated tools that will strengthen the analytical capabilities of USNCB personnel.

This recommendation can be closed when we receive documentation of the USNCB's efforts to improve the analytical capabilities of its staff and evidence that the USNCB has developed the capability to identify trends and patterns in international criminal activities and that such trend analysis activities are underway.

21. **Closed.** The USNCB agreed with our recommendation to develop procedures to ensure that information is added to an existing case only if information is available to confirm the identity of the subject, such as fingerprints and photographs. The USNCB provided a policy memorandum that requires dispatchers to confirm subject identities before saving a new request to an existing case. The policy instructs dispatchers to create a new case file if they determine the subject is not the same or if they determine the subject is the same, but that the new request does not relate to an existing case. The policy also states that in the latter instance, the new case will be cross-referenced to the

original case. We consider this action sufficient to close this recommendation.

22. **Resolved.** The USNCB agreed with our recommendation to ensure that its case management system provides the ability to: (1) adequately maintain, control, and dispose of case-related information, including access restrictions by user and audit trails; (2) compile management statistics; and (3) generate standardized correspondence. The USNCB stated that it is currently developing a case management system using Customer Relationship Management software. The next phase of the Customer Relationship Management project will define user roles and access rights, and will build in tools to appropriately archive and dispose of case-related data. The USNCB also stated that it is developing improved reports for compiling management statistics. Further, the USNCB stated that the evaluation of additional audit and statistical requirements will be incorporated into current and future development projects and that Customer Relationship Management will provide standard message templates for use by the USNCB's investigative divisions.

This recommendation can be closed when the USNCB provides evidence that the Customer Relationship Management software has been successfully implemented and that the software provides the USNCB with the ability to: (1) adequately maintain, control, and dispose of case-related information, including access restrictions by user and audit trails; (2) compile management statistics; and (3) generate standardized correspondence. Also, the USNCB should provide evidence that it can view workload statistics and generate ad-hoc reports.

23. **Resolved.** The ODAG agreed with our recommendation to ensure that the Executive Committee meets as prescribed in the MOU and takes the lead in developing a new strategic plan for the USNCB. The ODAG stated that the Deputy Attorney General will hold a meeting of the USNCB Executive Committee within 60 days to address issues related to the management of the agency and the development of a new strategic plan, and that this meeting will be followed by additional meetings to be held at least quarterly. Additionally, the ODAG stated that it has instituted monthly component meetings with the USNCB's Director and Deputy Director to establish and maintain a close working relationship between the two offices.

This recommendation can be closed when the ODAG provides evidence that the Executive Committee has been convened and continues to

meet throughout FY 2010 to discuss issues related to the management of the USNCB and the development of a new strategic plan. In addition, the ODAG should provide evidence that monthly component meetings between the ODAG and USNCB Director and Deputy Director are taking place. Further, when completed the USNCB should provide us with a copy of its new strategic plan.

24. **Resolved.** The ODAG agreed with our recommendation to evaluate options to enhance the USNCB's executive management structure to help ensure identification of the most qualified candidates for its senior executive positions. The ODAG stated that it will work with DHS to review the current executive management structure of the USNCB and explore options for improvement. Additionally, the ODAG stated that it has already begun to work with the USNCB and its Executive Committee to begin the selection process for the USNCB's Deputy Director position, which will become vacant in early FY 2010.

This recommendation can be closed when we receive the results of the ODAG's evaluation of options to enhance the USNCB's executive management structure to help ensure identification of the most qualified candidates for its senior executive positions.

25. **Resolved.** The ODAG agreed with our recommendation to determine the best method to budget and pay for the United States' membership dues to INTERPOL to help minimize the operational impact on the USNCB. The ODAG stated that it will work with the Department's Controller and the Justice Management Division and ensure that future increases to U.S. INTERPOL dues do not negatively impact the USNCB's operating budget.

This recommendation can be closed when the ODAG provides us with the results of its efforts to determine the best method to pay for U.S. financial obligations to INTERPOL without negatively impacting the USNCB's operating budget.

26. **Resolved.** The USNCB agreed with our recommendation to develop a formal IT plan that systematically evaluates current operations and uses of data and accounts for the various ways in which INTERPOL information might potentially be used and accessed by other agencies. The USNCB stated that it will work with the DOJ and DHS Chief Information Officers, the USNCB Executive Committee, and INTERPOL to formalize an IT Strategic Plan. According to the USNCB, a critical first step will be to identify an IT Strategic Planning consultant to

assist in conducting an IT assessment that addresses visioning, strengths, weaknesses, opportunities, threats, and constraints.

This recommendation can be closed when we receive a copy of the USNCB formal IT plan. In the interim, the USNCB should keep us informed of progress made on this recommendation.

27. **Resolved.** The USNCB agreed with our recommendation to work to develop formal agreements with domestic and federal law enforcement agencies regarding staffing commitments and length-of-duty assignments. The USNCB stated that it has developed a model MOU for use with outside agencies for the purpose of securing commitments for staffing and funding of the USNCB. The USNCB added that successful implementation of Recommendations 1 and 20 should provide the support and legal framework for long-term staffing arrangements between the USNCB and its federal participating agencies. Additionally, the USNCB stated that it will examine its staffing needs with a view to prioritizing a list of agencies with which to engage in an MOU.

This recommendation can be closed when the USNCB provides us a copy of the model MOU developed for use with outside agencies. Finally, the USNCB should provide us with its prioritized list of agencies with which it will attempt to engage in an MOU.