Privacy Impact Assessment
for the

Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System

June 1, 2009

Contact Point
Bradley E. Shepherd,
Acting IT Section Chief
OCDETF Fusion Center
Department of Justice
703-561-7144

Thomas W. Padden,
Deputy Director
OCDETF
Department of Justice
202-514-0922

Reviewing Official
Vance Hitch,
Chief Information Officer
Office of the Chief Information Officer
Department of Justice
202-514-0507

Approving Official
Nancy Libin
Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 514-2101

Introduction

The Organized Crime Drug Enforcement Task Forces (OCDETF) Program was created twenty-five years ago to pursue comprehensive, multi-jurisdictional investigations of major drug trafficking and money laundering organizations to include the international supply sources, the domestic transportation cells, and the regional and local distribution networks. At the same time, OCDETF attacks the money flow that supports the drug trade – depriving drug traffickers of their criminal proceeds and the resources needed to finance future criminal activity.

Recognizing that no single law enforcement entity is in a position to disrupt and dismantle sophisticated drug and money laundering organizations alone, OCDETF combines the resources and expertise of its seven member federal agencies -- the Drug Enforcement Administration (DEA); the Federal Bureau of Investigation (FBI); the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the U.S. Marshals Service (USMS); the Internal Revenue Service (IRS); U.S. Immigration and Customs Enforcement (ICE); and the U.S. Coast Guard (USCG) -- in cooperation with the Department of Justice's Criminal and Tax Divisions, Bureau of Consular Affairs (CA) of the Department of State (DOS), the 94 U.S. Attorneys' Offices, and state and local law enforcement, to identify, disrupt, and dismantle the drug trafficking and money laundering organizations most responsible for the nation's supply of illegal drugs.

To enhance OCDETF's overall capacity to engage in intelligence-driven enforcement and to accomplish its mission, OCDETF created the OCDETF Fusion Center (OFC) – a comprehensive intelligence and data center containing all drug and drug related financial intelligence information from seven OCDETF-member investigative agencies, the Financial Crimes Enforcement Network (FinCEN), the National Drug Intelligence Center, and others. The OFC is designed to conduct cross-agency integration and analysis of drug and drug related financial data to create comprehensive intelligence pictures of targeted organizations, including those identified as Consolidated Priority Organization Targets (CPOTs) and Regional Priority Organization Targets (RPOTs), and to pass actionable leads through the multi-agency Special Operations Division (SOD) to OCDETF participants in the field.

Through its Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System (hereinafter referred to as "Compass")(Unique ID: 011-05-01-03-01-2061-00-113-215), the OFC gathers and fuses data from multiple disparate sources to analyze previously unidentified relationships and links. This allows the OFC to gain multi-source knowledge from the fused data in a manner that is not possible using the information

technology systems of OCDETF's partners without hundreds of hours of manual review.

Drug and International Organization Crime

The Attorney General's Organized Crime Council (AGOCC) is chaired by the Deputy Attorney General and has as members the heads of nine federal law enforcement agencies and presidentially appointed prosecutors. It is an outgrowth of an Executive Order, issued by President Lyndon B. Johnson in 1968, placing the Attorney General in charge of coordinating all federal law enforcement activity against organized crime. The traditional role of the AGOCC has been to promote interagency coordination, evaluate the threat presented by organized crime, and advise the Attorney General on national priorities and a national organized crime strategy. In 2008, the AGOCC began to consider the threat from international organized crime, rather than La Cosa Nostra, to be the primary organized crime threat facing the United States.[1] In response, the AGOCC has begun the work of developing a new 21st Century organized crime program that will be nimble and sophisticated enough to combat the threat posed by international organized criminals for years to come.

In May 2009, the AGOCC established the International Organized Crime Intelligence and Operations Center (IOC-2). Its mission is to significantly disrupt and dismantle those international criminal organizations posing the greatest threat to the United States by:

(1) gathering, storing, and analyzing all-source information and intelligence related to international organized crime;

(2) disseminating such information and intelligence to support law enforcement operations, investigations, prosecutions, and forfeiture proceedings; and

[1] "International organized crime" refers to those self-perpetuating associations of individuals who operate internationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through an international organizational structure and the exploitation of international commerce or communication mechanisms.

(3) coordinating multi-jurisdictional and multi-agency law enforcement operations, investigations, prosecutions, and forfeiture proceedings.

IOC-2 combines the resources and expertise of its nine federal member agencies -- Federal Bureau of Investigation; Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms, and Explosives; U.S. Immigration and Customs Enforcement; U.S. Secret Service; Internal Revenue Service, Criminal Investigation; U.S. Postal Inspection Service; U.S. Department of State, Bureau of Diplomatic Security; and U.S. Department of Labor, Office of the Inspector General – in cooperation with the Department of Justice's Criminal Division, the 94 U.S. Attorneys' Offices, and others, to pursue this mission.

In recognition of the demonstrated interrelationship between criminal organizations that engage in illicit drug trafficking (and related criminal activities) and those that engage in international organized crime, involving a broader variety of criminal activity, and the corresponding need for IOC-2 to gain multi-source knowledge from the fused data in a manner that is not possible using the information technology systems of IOC-2 individual members without hundreds of hours of manual review, OCDETF and IOC-2 formed a partnership. In furtherance of the partnership, OFC and IOC-2 have collocated, and will pool data input and share access to Compass.

Section 1.0 The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

Compass collects the information pertaining to individuals, entities, and organizations charged with, convicted of, or known, suspected, or alleged to be involved with, illicit narcotic trafficking or other potentially related criminal activity, including but not limited to facilitating the transportation of narcotics proceeds, money laundering, financial crimes, firearms trafficking, alien smuggling, and terrorist activity. Pursuant to the partnership with IOC-2, Compass also collects the information pertaining to individuals, entities, and organizations charged with, convicted of, or known, suspected, or alleged to be involved with, international organized crime. Information regarding individuals, entities, and organizations with pertinent knowledge of some circumstances or aspect of a case or record subject, such as witnesses, associates of record subjects,

informants, and law enforcement or intelligence personnel is also collected. Information about relevant immigrant and nonimmigrant visa applicants, including visa adjudication, issuance, and refusal information is also collected. Finally information of individuals, entities, and organizations identified in or involved with the filing, evaluation, or investigation of reports under the Bank Secrecy Act and its implementing regulations is also gathered.

Because the source of Compass data is both structured and unstructured textual reports, the precise data that is collected and contained in Compass can be almost anything. Included in the data are all the principal identifiers such as name, social security number (SSN), and address. But it can also include scars, marks, tattoos, license plate numbers, bank account numbers, etc. This is especially true of the information in reports of investigations filed by special agents. These reports are often free flowing narratives of events, meetings, and surveillance. All of the text, every word, is indexed and searchable.

1.2 From whom is the information collected?

All the necessary information is contributed by the Department of Justice; Drug Enforcement Administration; Federal Bureau of Investigation; the Bureau of Alcohol, Tobacco, Firearms & Explosives; United States Marshals Service; Financial Crimes Enforcement Network (FinCEN); National Drug Intelligence Center; Internal Revenue Service; the United States Coast Guard; Bureau of Consular Affairs and Bureau of Diplomatic Security of the Department of State; U.S. Immigration and Customs Enforcement and Customs and Border Protection of the Department of Homeland Security; U.S. Secret Service; U.S. Postal Inspection Service; and the Department of Labor. These agencies collect the information via various methods consistent with their authorities in support of their respective missions, and may include information from state, local, tribal, territorial, and foreign law enforcement agencies.

Although Compass contains no direct links to commercial databases or sources, there are rare instances where commercial organizations are the source of information contained in the database. These occasions arise when analysts during the normal conduct of an investigation also refer to internet and other open sources for information. These sources are sometimes included/referenced in OFC reports and products. Upon completion of an investigation and its associated OFC report/product, these new reports/products are ingested into Compass. Once ingested, they are in turn retrievable by future queries. The same is true with IOC-2 reports.

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The Fusion Center's use of merged or "fused" drug, financial, and related investigative information from multi-agency sources will likely identify, when comprehensively reviewed through higher level analytical processes (versus manual data manipulation), previously unknown links within the data. This, in turn, should result in a more complete picture of the activities of drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorist, and other criminal organizations and their memberships, than any one such agency or individual analyst can produce by itself. Specifically, the OFC will develop investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats which will assist law enforcement in reducing the drug supply by identifying, disrupting and dismantling the most significant international and domestic drug supply and money laundering organizations and related criminal operations (e.g., arms traffickers, alien smugglers, terrorists).

Likewise, IOC-2's use of merged or "fused" international organized crime, financial, and related investigative information from multi-agency sources will likely identify, when comprehensively reviewed through higher level analytical processes (versus manual data manipulation), previously unknown links within the data. This, in turn, should result in a more complete picture of the activities of international criminal organizations and their memberships, than any one such agency or individual analyst can produce by itself. Specifically, IOC-2 will develop investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats which will assist law enforcement in significantly disrupting and dismantling those international criminal organizations posing the greatest threat to the United States.

Finally, by fusing the OFC and IOC-2 data into Compass both missions will likely benefit from a more complete picture of the activities and interrelationships between international criminal organizations and drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorist, and other criminal organizations.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The Consolidated Appropriations Act, 2004, Pub. L. No. 108-199, 118 Stat. 3 (2004); the Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. 91-513 (84 Stat. 1236); and the Single Convention on Narcotic Drugs, 1961. Additional authority is derived from Treaties, Statutes, Executive Orders, and Presidential Proclamations which the Department of Justice (DOJ) has been charged with administering.

The legal authority for including international organized crime to the development and maintenance of this system is provided by:

The Organized Crime Control Act of 1970, Pub. L. 91-452 (84 Stat. 922); the Convention on Transnational Organized Crime, 2004; Executive Order 11396 (1968). Additional authority is derived from Treaties, Statutes, Executive Orders, and Presidential Proclamations which the Department of Justice (DOJ) has been charged with administering.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

(a) Privacy Risk: Access by unauthorized individuals
Mitigation: The data resides in a closed system that is only available to cleared OFC and IOC-2 personnel with a need to know. In addition, there are controls regarding who has access to particular information and controls on how information is disseminated to the Special Operations Division. Moreover, the records are housed in a secure building restricted to DOJ employees and other authorized personnel. Physical and electronic access to Compass is safeguarded in accordance with DOJ rules and policies governing automated systems security and access, including the maintenance of technical equipment in restricted areas. The system is contained in a room secured by intruder alarms and other appropriate physical and electronic security controls.

(b) Privacy Risk: Misuse by individuals with authorized access
Mitigation: Every query requires entry by a user of a "Reason Code" signifying the case number. Queries are audited and pertinent information about the query, including the reason code and the query parameters is saved in the audit log.

Policies and procedures are being developed regarding access and periodic review of the audit log. At this time, users with Supervisor position privileges can

view the audit log to ensure that users follow the policies defined for Compass.

Although the information is provided for entry into Compass by various agencies, those agencies do not have direct access to Compass either for data entry or retrieval. Moreover, users of Compass have read only access to the original records provided by the participating agencies thus eliminating the possibility of altering the records.

To protect the privacy rights of the public and employees, oversight of the use and maintenance of Compass and its data is provided by the Director of the OFC.

Section 3.0 Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

Compass will serve two primary purposes. The first purpose of this system of records is to facilitate the mission of the OCDETF Program, which is to reduce the drug supply by identifying, disrupting and dismantling the most significant international and domestic drug supply and money laundering organizations and related criminal operations (e.g., arms traffickers, alien smugglers, terrorists). By establishing a central data warehouse for the compilation, fusion, storage, and comprehensive analysis of drug, financial, and related investigative information from multiple agencies, OCDETF expects to produce a more complete picture of the activities of drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorist, and other criminal organizations and their memberships than any one such agency can produce by itself. Specifically, the OFC will develop investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats. The OFC intends to disseminate these analytical products through SOD, as appropriate, to Federal, State, local, tribal, territorial, and foreign law enforcement and regulatory agencies and to agencies of the U.S. foreign intelligence community and the military community, to assist them in enforcing criminal, civil, and regulatory laws related to drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorism, and other crimes, including the identification, apprehension, and prosecution of individuals who threaten the United States' national and international security and interests through their involvement in such crimes.

The second purpose of this system of records is to facilitate the mission of IOC-2 and its member agencies to significantly disrupt and dismantle those international criminal organizations posing the greatest threat to the United States. By establishing a central data warehouse for the compilation, fusion, storage, and comprehensive analysis of international organized crime, financial, and related investigative information, IOC-2 expects to produce a more complete picture of the activities of international criminal organizations and their memberships than any one such agency can produce by itself. Specifically, IOC-2 will develop investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats. IOC-2 intends to disseminate these analytical products, as appropriate, to Federal, State, local, tribal, territorial, and foreign law enforcement and regulatory agencies and to agencies of the U.S. foreign intelligence community and the military community, to assist them in enforcing criminal, civil, and regulatory laws related to organized crime, terrorism, and other crimes, including the identification, apprehension, and prosecution of individuals who threaten the United States' national and international security and interests through their involvement in such crimes.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

It is anticipated that the merging or "fusion" of drug, financial, and related investigative information from multi-agency sources will identify, when comprehensively reviewed through higher level analytical processes (versus manual data manipulation by an individual analyst), previously unknown links within the data. This, in turn, may result in a more complete picture of the activities of drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorist, and other criminal organizations and their memberships than any one such agency or individual analyst can produce by itself. Specifically, the OFC expects to develop, based on the determinations made, investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats. The new data will be placed in folders and will be used to generate OFC products and leads.

Likewise, it is anticipated that the merging or "fusion" of international organized crime, financial, and related investigative information from multi-agency sources will identify, when comprehensively reviewed through higher level analytical processes (versus manual data manipulation by an individual analyst), previously unknown links within the data.

This, in turn, may result in a more complete picture of the activities of international criminal organizations and their memberships than any one such agency or individual analyst can produce by itself. Specifically, IOC-2 expects to develop, based on the determinations made, investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats. The new data will be placed in folders and will be used to generate IOC-2 products and leads.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The initiating Intelligence Analyst will incorporate all relevant open source and legacy system information into one of the five approved OFC products. Attached to the completed product will be an "OFC Final Product Approval Worksheet" (Form OFC-2), as well as the completed OFC-1 form and all accompanying raw data from the legacy system checks. If the product was initiated by an Intelligence Analyst, the completed product, worksheets, and raw data will be forwarded to his/her appropriate Desk Officer, who will then ensure, by the procedure set forth below, that the information was properly and inclusively researched, that it is current, and that it addresses all issues or explains the intent to follow-up.

If the product was initiated by a Desk Officer, the Desk Officer will follow the same procedures with his/her own product. Desk Officers and Intelligence Analysts will take particular care to ensure that all relevant agency caveats are prominently included in the OFC product. The Desk Officer will then circulate the completed product, Form OFC-2 and Form OFC-1, with attachments, to other Drug and/or Financial Intelligence units within the OFC who may have an interest in the discussed target or final product. Those groups will initial the Form OFC-2 in the appropriate place and return it to the Desk Officer. The Desk Officer will certify by signature that the product meets the established guidelines and will forward it to the appropriate Section Chief for review and approval. Agency heads or their designees will certify by signature and date that appropriate coordination has been effected regarding agency proprietary information to be included in OFC products.

The Section Chief will review all OFC products for completeness and compliance with the standards listed above. The Section Chief will approve by signature and forward the product to the OFC Deputy Director.

The OFC Deputy Director will be the last reviewer of the OFC product prior to release to the Special Operations Division. The Deputy Director will provide a review for completeness and

proper adherence to established procedures within the OFC. Upon completion of the review, the Deputy Director will sign off on the product for release and return it to the OFC Section Chief for dissemination to SOD.

According to its Charter and memorandums of understanding with its participating agencies, IOC-2 will follow the policies and procedures of the OFC. Thus, IOC-2 will create an analogous procedure for its personnel to follow.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration?

Records in this system are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration.

Pursuant to the U.S. Department of Justice regulations governing Procedures for Disclosure of Records Under the Freedom of Information Act, the OFC will "preserve all correspondence pertaining to the requests that it receives under [FOIA], as well as copies of all requested records, until disposition or destruction is authorized by Title 44 United States Code (USC) or the National Archives and Records Administration's General Records Schedule 14. Records will not be disposed [by the OFC] while they are the subject of a pending request, appeal, or lawsuit under the Freedom of Information Act (28 C.F.R. §16.10).

OFC's Standard Operating Procedures, dated September 30, 2005 also states that:

The OFC will adhere to the records storage and disposition requirements under the Federal Records Act and Federal Records Disposal Act. Specifically, the OFC will make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities. The OFC Director, in consultation with the OCDETF Director, will also establish a program of management of the records of the OFC by establishing safeguards against the removal or loss of records determined to be necessary and required by regulations of the National Archives and Records Administration, including that records in the custody of the agency are not to be alienated or destroyed except in accordance with Title 44 USC §§3301-3314 and notifying the Archivist of any actual, impending, or threatened unlawful removal, defacing, alteration, or destruction of records in the custody of the OFC.

The OFC will consider transfer of records from the OFC to the Archivist for storage, processing, and servicing intra-agency disclosures. Additionally, the OFC shall ensure the appropriate protection of non-record material containing information which is restricted from release under the Privacy Act or other statutes, when such restricted non-record material is removed from the OFC (36 C.F.R. §1222.42(c)). For records transferred to an agency or commercial records storage facility, the OFC understands that the storage, maintenance, and disposal of the records must also not violate the Privacy Act's disclosure provisions.

According to its Charter and memorandums of understanding with its participating agencies, IOC-2 will follow the policies and procedures of the OFC.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

There will be one data base maintained at the OFC (the OFC System). Access to the OFC System will be accomplished via the Merlin Network which is a DEA classified platform that has been installed at the desk of every Special Agent and Intelligence Analyst at the OFC/IOC-2. All users that require access to the OFC System and Merlin resources must receive approval by their supervisors in written or electronic form before that access can be established. The OFC System will require a separate password, and will not be accessible by other Merlin users who are not assigned to the OFC or IOC-2. While using Merlin resources, users are responsible for their actions and for ensuring that those actions meet existing policy and guidelines. First line supervisors are responsible for directing the removal of Merlin access for all persons under their supervision upon transfer of the user, termination of employment, or when there is no longer any need for that user to access the OFC System and Merlin resources. The OFC System will maintain an audit trail of all queries conducted and information accessed by users of the system. Policies and procedures are being developed regarding periodic review of the audit log. At this time, users with the Supervisor position privileges can view the audit log to ensure users follow the policies defined for Compass.

Each user of the classified Merlin Network or unclassified parent agency systems will be held individually accountable for their actions while logged on to system resources.

These records are housed in a secure building restricted to DOJ employees and other authorized personnel, and those persons transacting business with the DOJ who are escorted by DOJ or other authorized personnel. Physical and electronic access to the System is safeguarded in accordance with DOJ rules and policies governing

automated systems security and access, including the maintenance of technical equipment in restricted areas. The selection of containers or facilities is made in consideration of the sensitivity or National Security Classification as appropriate, of the files. The System is contained in a room secured by intruder alarms and other appropriate physical and electronic security controls. Access to the System terminal(s) are further restricted to DOJ employees, detailees to DOJ from other government agencies, and individual contractors who have authorized access (including individual passwords and identification codes), appropriate security clearances, and a demonstrated and lawful need to know the information in order to perform assigned functions on behalf of the OCDETF Fusion Center and/or IOC-2. All OCDETF Fusion Center and IOC-2 personnel capable of accessing the OCDETF Fusion Center and IOC-2 System will have successfully passed a background investigation. Unauthorized access to the telecommunications terminals is precluded by a complex authentication procedure.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

The following questions are intended to describe the scope of sharing both within the Department of Justice and with other recipients.

4.1 Within which internal components of the Department is the information shared?

4.1.1 Identify and list the name(s) of any components, offices, and any other organizations within the Department with which the information is shared.

The name of organizations within the Department of Justice with which the information is shared is as below:

Organized Crime Drug Enforcement Task Force (OCDETF)
Drug Enforcement Administration (DEA)
Federal Bureau of Investigation (FBI)
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
National Drug Intelligence Center (NDIC)
United States Marshals Service (USMS)
The Criminal Division

4.2 For each recipient component or office, what information is shared and for what purpose?

All information contained in Compass is shared with representatives from each of the agencies listed above that are assigned to the OFC/IOC-2 and given access to Compass for purposes of supporting the OFC/IOC-2 mission. Intelligence analysts and agents from the agencies listed above have access to this information to develop intelligence products and leads

to aid field investigators from the OCDETF/IOC-2 member agencies in identifying, investigating, prosecuting and disrupting/dismantling organizations involved in drug trafficking, money laundering and associated criminal activities. These intelligence products and leads, which contain information derived from Compass, are made available to agents and analysts in the field pursuing such investigations. The distribution of this information is coordinated through the Special Operations Division to ensure information is properly handled and coordinated among the law enforcement agencies.

Memorandums of Understanding between OCDETF/IOC-2 and each of the agencies that participate in, or contribute data to, Compass provide the OFC/IOC-2 with authority to share the information. In addition, the OFC's Concept of Operations, Charter and Standard Operating Procedures, and IOC-2's Charter, were authorized by each of the participating agencies and provide specific parameters governing the sharing of this information.

The purpose of such sharing is to support coordinated, multi-jurisdictional investigations focused on the disruption and dismantlement of significant drug trafficking and money laundering enterprises, and international criminal organizations.

The following information is shared:

Department of Justice:
- Consolidated Priority Organizational Target (CPOT) List
- OCDETF Management Information System
- OFC Products
- Joint Automated Booking System (JABS)
- Top International Criminal Organizations Target (TICOT) List
- IOC-2 Products

Drug Enforcement Administration:
- DEA-6 Documents
- DEA Communication Automated Profiling System (CAPS)
- DEA M204 Events
- Narcotics and Dangerous Drugs Information System (NADDIS)
- El Paso Intelligence Center (EPIC) Internal Query Database
- El Paso Intelligence Center (EPIC) Gatekeeper (Special Report of Southwest Boarder)

Federal Bureau of Investigation:
- FBI Automated Case Support (ACS)
- FBI South Texas Joint Assessment Bulletin (JAB)

Bureau of Alcohol, Tobacco, Firearms and Explosives
- NFORCE Case Management System

National Drug Intelligence Center

Real-time Analytical Intelligence Database (RAID)

United States Marshals Service
Warrant Information Network (WIN)

4.3 How is the information transmitted or disclosed?

All the information is loaded into the OFC's database and representatives of the sharing partners assigned to the OFC/IOC-2 have direct access to the information through OFC's Compass.

Information such as intelligence products and investigative leads is transmitted electronically through OFC's Compass to the DEA-led, multi-agency Special Operations Division (SOD). OCDETF, the OFC, IOC-2, and SOD have specific policies and MOUs in place governing the dissemination of OFC/IOC-2 products. SOD/IOC-2 disseminates documents electronically and in writing as circumstances require.

4.4 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, if another Departmental component, office, or organization has access to the system that your office controls, discuss how access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing of information.

Potential privacy risks could include access by unauthorized individuals and misuse by individuals with authorized access. These risks are mitigated as detailed below.

There is one data base maintained at the OFC (Compass). Access to Compass will be accomplished via the Merlin network system which is a DEA classified platform that will be installed at the desk of every Special Agent and Intelligence Analyst at the OFC/IOC-2. All users that require access to Compass and Merlin resources must receive approval by their supervisors in written or electronic form before that access can be established. Compass will require a separate password, and will not be accessible by other Merlin users who are not assigned to the OFC/IOC-2. While using Merlin resources, users are responsible for their actions and for ensuring that those actions meet existing policy and guidelines. First line supervisors are responsible for directing the removal of Merlin access for all persons under their supervision upon transfer of the user, termination of employment, or when there is no longer any need for that user to access Compass and Merlin resources. Compass will maintain an audit trail of all queries conducted and information accessed by users of the system.

DOJ components and personnel that merely receive intelligence products and investigative leads from the OFC/IOC-2 do not have access to Compass.

Section 5.0 External Sharing and Disclosure.

The following questions are intended to define the content, scope, and authority for information sharing external to the Department which includes Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

The external (non-DOJ) recipients are as below:

Financial Crimes Enforcement Network (FinCEN, U.S. Department of the Treasury)
Internal Revenue Service (IRS, U.S. Department of the Treasury)
United States Coast Guard (USCG, U.S. Department of Homeland Security)
Bureau of Consular Affairs (CA, U.S. Department of State)
Bureau of Diplomatic Security (DS, U.S. Department of State
U.S. Postal Inspection Service (USPIS, U.S. Postal Service)
Office of the Inspector General (OIG, Department of Labor)

It is expected that information in this system will also be shared with the U.S. Immigration and Customs Enforcement (ICE, U.S. Department of Homeland Security) and the U.S. Secret Service (USSS, U.S. Department of Homeland Security) in the near future upon finalization of Memorandums of Understanding with those agencies.

5.2 What information is shared and for what purpose?

As stated in paragraph 3.1, the purpose of this system of records is twofold: (1) to facilitate the mission of the OCDETF Program, which is to reduce the drug supply by identifying, disrupting and dismantling the most significant international and domestic drug supply and money laundering organizations and related criminal operations (e.g., arms traffickers, alien smugglers, terrorists); and (2) to facilitate the mission of IOC-2 and its member agencies to significantly disrupt and dismantle those international criminal organizations posing the greatest threat to the United States. The purpose and information shared with FinCEN and USCG is listed in Question 4.2. The information shared with the Department of State (DOS) involves the identification of drug traffickers, fugitives and other persons of interest who may apply for non-immigrant visas.

Memorandums of Understanding between OCDETF, IOC-2, and each of the agencies that participate in, or contribute data to, the OFC/IOC-2 provide the OFC/IOC-2 with authority to share the information. In addition, the OFC's Concept of Operations, Charter and Standard Operating Procedures, and IOC-2's Charter, were authorized by each of the participating agencies and provide specific parameters governing the sharing of this information. FinCEN is sharing Bank Secrecy data, USCG is sharing Marine Information for Safety and Law Enforcement (MISLE) data; IRS is in the process of sharing Criminal Investigation Management Information System (CIMIS); CA is sharing information of Immigrants and Non Immigrants visa applications, visa adjudication, issuance, and refusal information; DS is sharing information from the DSS RBII database and the DS Criminal Investigative Division Case Management System; USPIS is sharing case information and related linked record information pertaining to priority targets as well as certain Data on $3000 logs, certain Data reported on CTRs, certain Data reported on USPS SARs, and digital images of money orders reported on USPS SARs; Labor/OIG is sharing records maintained in the United States Department of Labor Office of Inspector Generals investigative files. As stated above in Section 5.1, it is expected that ICE and USSS will become external sharing partners with the OFC/IOC-2, and therefore, will share certain information in accordance with appropriate Memorandums of Understanding.

5.3 How is the information transmitted or disclosed?

All the information is loaded into the OFC's database and representatives of the sharing partners assigned to the OFC/IOC-2 have direct access to the information through the OFC's Compass.

Information such as intelligence products and investigative leads is transmitted electronically through OFC's Compass to the DEA-led, multi-agency Special Operations Division (SOD). OCDETF, the OFC, IOC-2, and SOD have specific policies and MOUs in place governing the dissemination of OFC/IOC-2 products. SOD/IOC-2 disseminates documents electronically and in writing as circumstances require.

Agencies and personnel external to the OFC/IOC-2 that merely receive intelligence products and investigative leads from the OFC/IOC-2 do not have access to Compass.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared? If possible, include a reference to and quotation from any MOU, contract, or other agreement that defines the parameters of the sharing agreement.

Memorandums of Understanding (MOU) and the OFC Standard Operating Procedures, signed by OCDETF and each of the participating agencies, represent the agreements governing the security and privacy of the data once it is shared.

See OFC Standard Operating Procedures, Appendix 4: Privacy Act and Freedom Of Information Act Procedures - "The OFC and its personnel, including contractors and those detailed from the participating agencies, are subject to the Privacy Act of 1974 (5 U.S.C. §552a), and the Freedom of Information Act (FOIA) (5 U.S.C. §552). The following policies and procedures discuss the application of these federal statutes to the OFC's record-keeping and disclosure actions. See also Privacy Act Assessment for the OFC (2004), completed by the Narcotic and Dangerous Drug Section, Criminal Division, U.S. Department of Justice, for a comprehensive analysis of the application of the Privacy Act and FOIA to the OFC and its personnel." [Sample language, not full Appendix]

See OFC standard Operating Procedures, Chapter 3: Information Sharing/Information Security and Appendix 6: Security Procedures - No individual assigned to the OFC will share any information contained in the OFC with any individual or organization outside the OFC except through SOD. Direct contact with S/As, I/As, or other individuals in the field is prohibited unless specifically authorized by the Director of the OFC and coordinated with SOD. Such unauthorized disclosure will be grounds for dismissal from the OFC and immediate investigation of the information compromised.[Sample language, not full Chapter/Appendix]

Memorandums of Understanding (MOU) and IOC-2's Charter, signed by IOC-2 and each of the participating agencies, represent the agreements governing the security and privacy of the data once it is shared.

See IOC-2 Charter, Section IX: Policies/Protocols – [T]he established polices and protocols in place at SOD and the OFC shall apply to IOC-2. To the extent necessary, the IOC-2 Director shall establish additional policies and protocols to address the daily operations of IOC-2. These policies and protocols shall include the following: IOC-2 will ensure that each agency's data is handled and protected in accordance with the policy and procedures of the participating agencies to be defined in a Memorandum of Understanding with each agency. IOC-2 shall abide by currently existing SOD and OFC guidelines, and will adopt additional guidelines as needed, to ensure the protection of each agency's data. IOC-2 will be diligent in assuring that the information provided by the parties will be properly protected and secure.

5.5 What type of training is required for users from agencies outside the Department prior to receiving access to the information?

Users of Compass include Agents and Analysts from the OFC and IOC-2 participating agencies who will be housed in the OFC facility in Merrifield, Virginia. Only those persons who have a need-to-know the information in the performance of their official duties will have access to the information. Prior to obtaining access, all new users are required to complete the "Merlin Rules of Behavior". Although primarily aimed at security issues this document also covers privacy issues.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

Users' access will be restricted based on group and role. Every query requires entry by a user of a "SOD Request Number" (reason code) signifying the case number. Queries are audited and pertinent information about the query, including the reason code and the query parameters is saved in the audit log. Policies and procedures are being developed regarding access and periodic review of the audit log.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and how were they mitigated? For example, if an MOU, contract, or agreement is in place, what safeguards (including training, access controls, and security measures) have been implemented by the external agency to ensure that information is used appropriately?

Privacy risks include access by unauthorized individuals and misuse by individuals with authorized access. OFC mitigates these risks as detailed in the OCDETF Standard Operation Procedures, which describes guidelines to ensure the information is used appropriately, e.g., "In the event an OFC product is misused by an individual in the field, the matter will be referred to the individual's parent agency headquarters for investigation and possible disciplinary action." The individual will also be barred from receiving future OFC products. Other possible sanctions will be determined by the OFC Board of Governance. IOC-2 uses the same policies and protocols as OFC, as detailed in the IOC-2 Charter and quoted in Section 5.4, above.

Section 6.0 Notice.

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to the collection of information?

The Fusion Center Compass system relies solely on the information provided by the participating agencies rather than soliciting information directly from any individual.

A System of Records Notice was published in the Federal Register Notice, see 69 FR 61403 (October 18, 2004), as well as a proposed rule with invitation to comment, see 69 FR 61323 (October 18, 2004). No comments were received. The Final Rule can be found at 69 FR 72114 (December 13, 2004). Modifications to the System of Records Notice and the rule to reflect the updates and changes to the system of records have been sent to the Federal Register for publication.

6.1.2 Was the person aware that his or her information was being collected?

The Fusion Center and IOC-2 collect data from the participating agencies engaged in law enforcement activities and not from individual persons. As stated above, a notice was published in the Federal Register and no comments were received, and a Final Rule was published. In addition, modifications to the System of Records Notice and the rule to reflect the updates and changes to the system have been sent to the Federal Register for publication.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

The Fusion Center and IOC-2 collect data from the participating agencies engaged in law enforcement activities and not from individual persons.

6.3 Do individuals have an opportunity to consent to particular uses of the information? If such an opportunity exists, what is the procedure by which an individual would provide such consent?

Neither the Fusion Center nor IOC-2 collects data directly from any individual. Therefore, individuals will not have the opportunity to consent to or decline the particular uses of the information given by the agencies to the Fusion Center and IOC-2. However, as stated above, a Notice was published in the Federal Register inviting comment regarding the OFC's use of this information and no comments were received. In addition, modifications to the System of Records Notice and the rule to reflect the updates and changes to the system have been sent to the Federal Register for publication.

6.4 Privacy Impact Analysis: Conspicuous and transparent notice allows individuals to understand how their information will be used and disclosed. Describe how notice for the system was crafted with these principles in mind or if notice is not provided, what was the basis for this decision.

In preparation of the previous system of records notice, OCDETF sought the assistance of Department's Narcotic and Dangerous Drug Section, Office of Enforcement Operations, and Justice Management Division in analyzing the Privacy Act and Freedom of Information Act implications of creation of the OFC and Compass. It was determined that the OFC was creating a "system of record" and notice was published in the Federal Register. The System of Records Notice described the nature of the OFC's function, the types of information it intended to collect, how it intended to use the information, how information would be retrieved, security controls for the handling of the data, etc. Furthermore, with the establishment of the partnership between OCDETF and IOC-2, OCDETF and IOC-2 enlisted the support of the Department of Justice Office of Privacy and Civil Liberties to ensure that the required privacy documentation was updated to reflect the updates and changes to the system.

Section 7.0 Individual Access and Redress.

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Per the Federal Register Notice, inquiries should be addressed to: OCDETF Fusion Center Privacy Act/FOIA Unit, OCDETF Fusion Center, Executive Office for the Organized Crime Drug Enforcement Task Force, Criminal Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

RECORD ACCESS PROCEDURES: A request for access to a record from this system shall be made in writing to the System Manager, with the envelope and the letter clearly marked "Privacy Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

CONTESTING RECORD PROCEDURES: Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access Procedures listed

above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. Some information may be exempt from contesting record procedures as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Pursuant to the Final Rule published in the Federal Register for the OCDETF Fusion Center, the Fusion Center is exempt from 5 USC §552a (d)(1) and its requirement to provide access to individuals. Specifically, the Fusion Center is exempt from subsection (d)(1) because disclosure of records in the system could alert the subject of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of confidential witnesses and informants, of the investigative interest of Organized Crime Drug Enforcement Task Force Fusion Center and other intelligence or law enforcement agencies (including those responsible for civil proceedings related to laws against drug trafficking or related financial crimes); lead to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life, health, and physical safety of law enforcement personnel, confidential informants, witnesses, and potential crime victims. Access to records could also result in the release of information properly classified pursuant to Executive Order 12958 (or successor or prior Executive Order) or by statute, thereby compromising the national defense or foreign policy.
In addition, the Fusion Center is exempt from subsection (d)(2) because amendment of the records thought to be incorrect, irrelevant, or untimely would also interfere with ongoing investigations, criminal or civil law enforcement proceedings, and other law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised. Additionally, modifications to the rule have been sent to the Federal Register for publication to cover the changes to the system to include information maintained in furtherance of the OCDETF and IOC-2 partnership.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

A notice was published in the Federal Register notifying individuals of the procedures for seeking access to or amendment of information pertaining to them. As noted above, certain exemptions were published in the Final Rule for the OCDETF Fusion Center. Additionally, modifications to the notice and the rule to reflect changes to this system have been sent to the Federal Register for publication.

7.3. If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

As discussed above, the vast majority of the information contained in Compass is obtained from federal law enforcement agencies who maintain the original version of these records. Per the Standard Operating Procedures for the OFC, the OFC is in the process of standing up a Privacy Act/FOIA Unit to address any requests for access or amendment to records on individuals. Per the SOP, the OFC's Privacy Act/FOIA Unit will forward any requests relating to those records to the agency that owns the record. Those agencies would have to evaluate the request for record access and record amendment and whether or not they can address the individual's concerns. As discussed above because the information contained in Compass relates to active law enforcement investigations that could be compromised if information is disclosed it is not anticipated that individuals will have access to or the ability to amend records. However, the owning agency might be able to provide some redress if the records sought pertain to an investigation that has closed where the concerns that supported the Privacy Act exemption no longer apply. This would have to be reviewed on a case by case basis taking into account the facts and sensitivities of each investigation.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

See responses above.

Section 8.0 Technical Access and Security.

8.1 Which user group(s) will have access to the system?

OCDETF and IOC-2 analysts and agents physically on-site have access to Compass. Access is controlled via user accounts and operating system authentication. The system runs on a controlled network.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

The restrictive access to the system is given only to those contractor personnel who are involved in the development of Compass, systems administration, and providing on-site support for the OCEFTF Fusion Center and IOC-2. All contractor personnel have the appropriate security clearance and their work is closely monitored by the COTR, and they must adhere to all security requirements. Please see attached contract.

8.3 Does the system use 'roles' to assign privileges to users of the system?

Compass uses the concepts of permissions, also known as Access Control List (ACL) Entities, and roles to assign privileges. Permissions are granular and mainly control access to data sources. There are 37 roles in all. Roles, on the other hand, control access to Compass functionality. Roles contain groupings of ACL Entities into an Access Control List.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The Compass Account Management document located at the Project Management Office (PMO) identifies which OCDETF and IOC-2 users access Compass and their associated permissions. A complete list of users is also documented.

8.5 How are the actual assignment of roles and rules verified according to established security and auditing procedures?

User's access to Compass functionality is verified against the security system programmatically as they attempt to access it.

Additionally, any user whose account has been dormant for 30 days has their account suspended; 90 days of dormancy results in termination. Lastly, all individuals holding federal secret clearances are re-investigated every five years.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

A complete and comprehensive audit log is maintained that captures users' actions, queries, and search terms, within Compass. Users with the Supervisor position privileges can view the audit log to ensure users follow the policies defined for Compass. Users must enter an "SOD Request Number" signifying the case number for every query.

8.7 Describe what privacy training is provided to users either generally or specially relevant to the functionality of the program or system?

All users on any DOJ computer system, to include Compass, are required to complete on an annual basis the DOJ Computer Security Awareness training. That training covers "…DOJ security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act and DOJ Records Management Regulations…".

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The Intelligence Research Support System (IRSS) network in DEA's Office of Special Intelligence has followed FISMA requirements and received Certification & Accreditation in August, 2008. DEA's Merlin's most recent accreditation is dated January, 2007. OCDETF's Compass System resides on the IRSS network and is accessible through the Merlin network. Compass' accreditation is now completed and is dated March 2008.

8.9 Privacy Impact Analysis. Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Compass documents often contain information subject to Privacy Act restrictions. To mitigate risks access to the information is controlled. Information can only be viewed via Compass and restrictions can be placed on individuals' access to any document. No access to the information is provided to outside systems. Access controls are in place to prevent unauthorized users from gaining access to the Compass database.

Given the physical protections in place at the Fusion Center (collocated with IOC-2), the biggest risk to privacy is the unauthorized release of information by an OFC or IOC-2 employee. To summarize, the preventative controls in place are:

- Only secret cleared federal employees allowed as users.
- Clearances are re-investigated every 5 years.
- Compass access requires supervisory authorization.
- Account usage is documented in an audit log.
- Audit logs are reviewable by supervisory personnel.
- Users are not allowed to introduce or remove media into the Fusion Center/IOC-2 facility.
- Users may be subject to disciplinary action to include termination and prosecution.
- Account dormancy results in account suspension or termination.
- Checkout process for transferring/departing employees requires Compass account termination.

Section 9.0 Technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

At the request of OCDETF, DOJ's Office of the Chief Information Officer evaluated existing systems and technologies available to the Department to determine if the requirements for Compass could be accomplished with existing IT capabilities available to the Department. Ultimately, it was determined that a new system would need to be developed, but that it would leverage some of the capabilities of deployed systems. As specific requirements were identified for Compass, various technologies were evaluated to assess and compare their ability to effectively achieve system goals.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity is enforced by not allowing users to be able to edit any information in Compass. From the user's standpoint, it is a view-only system. Privacy is enforced by nature of being a controlled access system on a closed network. Data and Compass security are enforced by the nature of the granular ACL Entity list that facilitates restricting specific data sources on an individual user basis.

9.3 What design choices were made to enhance privacy?

The system is deployed on a closed network to prevent access from unauthorized users. For authenticated users, access is controlled through role-based permissions at the group level and at the user level, as required. Users do not have the ability to edit or change any data within the system. No external system or user access is provided.

Conclusion

In creating the OCDETF Fusion Center and Compass, the OCDETF Executive Office was keenly aware of its obligations under the Privacy Act and the Freedom of Information Act. As such, OCDETF enlisted the assistance of DOJ's Narcotic and Dangerous Drug Section and Office of Enforcement Operations to undertake preparation of an in-depth analysis of plans for OCDETF Fusion Center Operations and Compass. This analysis resulted in a comprehensive document exceeding one hundred pages that was circulated to all the agencies participating in the OCDETF Fusion Center for review and comment, and no issues were raised by the participating agencies. Ultimately this analysis supported the development of the Federal Register Notice and Final Rules for the OCDETF Fusion Center that was prepared by NDDS, OEO, OCDETF Executive Office and the Justice Management Division. This document also served as the basis for

developing the sections of the Fusion Center's Standard Operating Procedures that relate to Privacy Act obligations and information security. Furthermore, when the OCDETF Fusion Center sought to enter into a partnership with IOC-2, OCDETF and IOC-2 worked closely with the DOJ Office of Privacy and Civil Liberties to ensure privacy documentation was updated to reflect the changes to the system.

The OCDETF Fusion Center, IOC-2, and their respective employees are well aware of the privacy protections afforded American citizens. The agents and analysts who are the core users of Compass are trained to understand the legal restrictions that govern their use of the information with which they are entrusted. This training starts with their entrance into government service and continues with periodic refreshers throughout their careers.

A second layer of protection is provided by virtue of the design and implementation of the Compass application. As mentioned, Compass is a fully audited system that resides on a standalone infrastructure of computers rated to operate at the secret level. As such, this infrastructure maintains a number of physical and electronic protections that minimize the likelihood of intrusion to a near zero level. Moreover, Compass users are fully aware of the personal, career and legal ramifications of revealing Compass information to unauthorized individuals. Penalties for such behaviors range from suspensions to firings to prison sentences.

Lastly, both the OCDETF Fusion Center and IOC-2 maintain memorandums of understanding with the various agencies that supply the original data housed in Compass. Mechanisms are in place for the updating/correcting of privacy information when ever the source agency issues revised information.

Responsible Officials:
1. Privacy Act Officer:

___/s/_____ (6/1/09)
Rena Y. Kim, Criminal Division/Office of Enforcement Operations/FOIA/PA Unit

2. Program Managers:

_____/s/_____ (6/1/09)
Stuart G. Nash, Associate Deputy Attorney General and Director, OCDETF

_____/s/_____ (6/1/09)
Jennifer Shasky Calvery, Acting Director, AGOCC

Approval Official:

____/s/_____ (6/1/09)
Nancy Libin
Chief Privacy and Civil Liberties Officer
Department of Justice