(4) Enter other relating record numbers, if any, such as FBI, FPS, NCIC, Driver's License, etc. in the comments field;

(5) The comments field must contain, at a minimum, the following information elements:

- Full date of event;
- Port-of-entry, or DHS office;
- Brief explanation of event;
- Explanation of actions taken at the time of the event, including officer's specific reasons used in the determination of the case;
- Citation of the applicable section(s) of law;
- Action to be taken if the person is encountered again;
- Name, telephone number (24 hours if needed), and office/agency of case agent, if appropriate, for further contact;
- Subsequent update of the case, if deferred or paroled into the United States, to appear at another port of entry.

The writer provides information that explains fully the reason for the creation of the lookout in the Comments field of the lookout, or notifies an originating port-of-entry or DHS office with the Message Function that the subject of the lookout was intercepted or encountered.

In composing the comments of the lookout record, the writer must consider the audience that will have access to the lookout information. It may used by officers at ports-of-entry, or at DHS offices in the United States or abroad, or by officers from other law enforcement agencies, where the subject may appear to request a benefit or apply for admission to the United States.

The facts of the case and its disposition shall be written clearly and concisely so that they answer any questions from the reader. The comments describe the purpose of the lookout information, and the actions that are being requested from any officer that may intercept the subject. The comments include a brief description of the contents of the A-file such as sworn statements taken, legal orders issued by any competent authorities, and any documents retained.

The writer shall avoid jargon, technical terminology, abbreviations, acronyms, or codes unless they are terms well known throughout DHS or routinely used in written communications. The writer will provide a succinct narrative that will eliminate or reduce the need to contact an originating officer for additional basic information to complete the ongoing proceedings. However, there may be exceptions where unusual circumstances arise, or the user is requested to contact specific individuals

or offices.

The most crucial facts of the narrative are contained within the first four lines of the comments. These are the only lines that are copied in the PALS CD that provides lookout information via laptops for use during seaport and remote sites inspections.

(f) Creation of Record File (A-file) for Permanent Lookout Records. A search of the Central Index System (CIS) is necessary to verify whether an A-file already exists. If no record file exists, one must be created. There must be an A-file for every permanent CBP lookout posted to NAILS. The documentary evidence used to provide the information for the lookout record will be contained in the A-file.

There are some exceptions:

(1) A temporary lookout record created for 90 days or less;

(2) A permanent lookout record created for 90 days or less;

(3) Lost or stolen passports; or

(4) A lookout record created by request of another law-enforcement agency.

As mentioned in the exceptions above, the creation of an A-file is not required for any CBP lookout record that is needed for 90 days or less. The lookout record may be given permanent status, within the 90-day temporary period, upon supervisory review without the need to create an A-file. The documentary evidence used to create a permanent 90-day lookout record may be contained in a chronological file maintained at the local port-of-entry that created the lookout record. The chronological file designation will be referenced in the appropriate record number field on the screen.

(g) Worksheet for the creation of lookout records based on information received from law enforcement agencies other than CBP. It is well recognized that local offices have established good working relationships with local law enforcement offices and agencies to enhance border security. As part of this relationship, the offices and agencies occasionally request that CBP create lookout records for persons that are of interest to these agencies.

The worksheet included as Appendix 31-1 standardizes the procedure used to document the receipt of such requests through telephone calls, faxed requests, or any other type of communication received from local agencies such as state police, sheriff's department, local police department, or local office of the Federal Bureau of Investigation.

The contact person information refers to the requesting law enforcement agency's contact person that will be included in the comments. The officer that creates the lookout record completes the routine contact information field on the second page of the lookout record.

The worksheet must be attached to any materials and documents received from the agency; it will be filed in the chronological monthly folders maintained at each port or Service office, as described above.

(h) Supervisory review of temporary lookout records. When a CBP officer creates a CBP lookout it will remain in temporary status in NAILS for 90 days. During that 90-day period, the supervisory CBP officer will review the temporary lookout record to determine whether the information conforms to the standards established in the following paragraphs. Upon approval by the reviewer, the lookout record has permanent status in NAILS. Supervisors may delegate the authority to review lookout records to senior officers who have experience in lookout activities.

The reviewing officer will review the lookout record in NAILS through the NAILS on-line Review Function. The lookout record may be approved, updated, returned to the originating officer, deleted, or bypassed for later review. When the lookout record is approved it has permanent status and remains in NAILS for the validity period programmed for each lookout case code used. Some case codes are programmed to be valid for one, five, or twenty years or until a certain age of the person for whom the lookout record is created. In cases where several case codes are used in one lookout record, the case code with the longest validity will give the lookout record its expiration date. The NAILS Simplified Operating Instructions (rev. October 1995) includes additional information on this topic.

(i) Maintenance of record files for lookout records. Record files (A-files) will be maintained at the National Records Center. No active lookout file will be sent to the Federal Record Center (FRC), since the intercept of an alien who is the subject of a lookout may result in a removal hearing. In such cases material from the A-file may become the record of proceeding and should be readily available.

CBP officers will ensure that the local Systems Control Officer (SCO) has updated the necessary user level to access NAILS at his/her authorized level.

(j) Responsibility for initiating lookouts. Field offices are responsible for the timely initiation of lookout records.

(k) Responsibility for updating lookouts. Field offices are responsible for the timely update of lookout records on persons who have been granted relief from removal. Any officer who encounters new information on the subject of a lookout may update the

record on-line, if the lookout is under that port-of-entry's or office's jurisdiction, or notify the originating officer that additional information on the person is available. The notification may be done on-line in NAILS by using the Message Function.

(l) Clearance for lookouts on subversive cases. Headquarters CBP/OFO shall review all lookout records on subversive cases. The A-file containing the information shall be forwarded to Headquarters CPB/OFO for review and approval. Emergency lookouts on subversive cases may be cleared through Headquarters CBP/OFO by telephone to be followed by the submission on the A-file containing the source material such as the investigative report or a request from another agency detailing the derogatory information.

The lookout system is not a 'classified system'; its information is considered sensitive. Reference to confidential source information shall be limited to a general reference only.

(m) Expiration and/or deletion of lookout records. All DFOs will receive monthly 30-60-90 day warning notices from Headquarters on lookouts that are about to expire from NAILS. A separate monthly notice on lookouts that have expired will also be sent to all DFOs.

When expiration or warning notices are received, each DFO is responsible for the review of the files listed to determine whether posting, amendment, or deletion is necessary.

No action is necessary when the lookout is to be deleted by the expiration date. If a lookout is to be amended after a file review, or if the file control office is to be amended, the file control office that received the lookout record on its expiration list is responsible for taking appropriate action.

Lookouts may be removed before the expiration date at the request of the originating agency, or if the alien's ineligibility is permanently waived through the granting of a waiver or if the alien is determined not to be excludable.

(n) Codes used in the lookout system.

(1) Soundex. A coding system of putting a numeric value of 0 to 6 to the letters in the alphabet is explained in detail in Chapter 5(C) of the Records Operations Handbook. A summarized guide to Soundex coding is also available on Form M-114 that is included as Appendix 31-4 of this manual.

(2) Nationality codes. Codes used in the Service lookout system to denote nationality are listed in the INSERTS **Statistics Handbook, Statistical Codes,**

**Country and Nationality Codes**. A list is also found in NAILS by using key PF-11. The screen provides a list of tables available to the user.

(3) Case codes. Codes are used to label the lookout by type. A list of the case codes with the definition of each is on Lookout Case Codes, Form M- 114. A copy of Form M-114 is included in the NAILS Simplified Operating Instructions, rev. October 25, 1995. A list is also found in NAILS by using key PF-11. The screen provides a list of tables available to the user.

CBP Case Codes are separated on the form **M-114** into two categories, "Case Codes Keyed to Section 212 of the Immigration and Nationality Act (INA)" and, "Special Case Codes". Field users may use any of the codes designated as keyed to the sections of the INA. Use of Special case codes, with a few exceptions listed below, are restricted for exclusive use by the Headquarters Lookout Unit.

[redacted]

The list two codes are for use when no other code fits the case or action desired. A full list of codes is included in Appendix 31-4. (Revised IN99-20)

[redacted]

## 31.6 Lookout Intercepts.

Effective immediately, the NAILS Message Function will be used to prepare reports on all intercepts of lookout records, except in the circumstance described above. As a result, any port or DHS office that created lookout records will be notified that there is more information relating to lookout records that originated at those sites, as well as any additional offices that may have some interest on the same lookouts. The officer at the originating port or DHS office will append any new information to the existing comments in the lookout record. The information is automatically converted into a new paragraph in the Comments field of the lookout, with a heading that includes the sending officer's name, location, telephone number, date and time of the message.

The NAILS Message Function is used with key PF7 - Send Message from any of the NAILS Inquiry/Search screens to communicate with a port or DHS office that originated the lookout record or any other office that is interested in the lookout record. There are on-screen instructions that provide guidance to the user. The NAILS Simplified Operating Instructions (Revised October 1995) provides detailed instructions.

Any officer who is authorized to conduct queries or searches in NAILS may use the Message Function. Any officer who reviews or updates lookout records created by other officers at the originating port or DHS office can append a message to an existing lookout record that originated at that port or DHS office.

The port or DHS office that intercepts the subject of a lookout record will maintain a local record of the lookout intercept by making a screen copy of the message sent to the originating office or officer. The copies may be used for statistical analysis and other necessary record keeping.

As in the case of any other office, the Headquarters Office of Field Operations (Office Code - COW) creates its own lookout records in NAILS. Intercepts on lookout records created by Headquarters that specifically request notification from the field will continue to be reported to Headquarters CBP/OFO via the NTC (703) 621-7700, as requested in the lookout record. Otherwise a notice of intercept and action will be done through the NAILS Message Function.

Additionally, all lookout record intercepts originating from the Consular Lookout and Support System (CLASS), the Non-Immigrant Inspection System (NIIS), or the Deportable Alien Control System (DACS) in NAILS will be sent to COW through the Message Function for proper disposition.

In the case of lookout records that originated from CLASS, each POE or office will maintain a record of such intercept by making a screen copy of the message. If the intercepting office needs to send documentary materials to the Visa Office, make a screen copy of the message, attach the relating documents, and send the package directly to the following address:

Chief, Systems Liaison Division, CA/VO/F/S
Visa Office, SA-1
Department of State
Washington, DC. 20522-0116

or, by facsimile, to: (202) 663-3897.

(Revised IN99-20)

(a) Intercept of lookout record during primary inspection. During primary inspection, a lookout intercept will be processed according to the case codes in the record, generally the case codes specify whether the person is to be detained or not. One of two actions will take place when a person is intercepted:

[redacted]

During the secondary inspection, a full NAILS query must be made to review the background information that is available for the lookout. If a lookout record is based on unclassified information, NAILS will contain as much information as held in the lookout file that is unclassified. If possible, the A-File should be reviewed to obtain comprehensive information.

(b) Secondary inspection of persons with lookout intercepts. Secondary inspection of persons who are the subjects of lookout intercepts includes gathering all possible information from a full NAILS query and from all other available automated systems. When available, the A-file should be reviewed to obtain comprehensive information.

Intercepts on every lookout posted by Headquarters requesting notification shall be reported to OFO through the NTC at (703) 621-7700 or as specified in the lookout record.

Lookout intercepts that appear sensitive because of national security concerns or because of potential public interest shall be immediately brought to the attention of NTC (preferably while the subject is still at CBP secondary inspection). (IN99-20)

[redacted]

# Inspector's Field Manual

[redacted]

## 31.7 Responding to Inquiries Concerning Lookout Records.

CBP has implemented an agency-wide procedure to respond to inquiries from the public concerning the existence of lookout records in the National Automated Immigration Lookout System (NAILS) for certain individuals who may be inadmissible to the United States. The procedure is designed to standardize the manner and content of the CBP responses regarding this type of inquiry.

The criteria to create lookout records for individuals encompass two categories of persons. First, CBP creates lookout records for nonimmigrant aliens, or lawful permanent residents, who may be inadmissible to the United States under Section 212 of the INA, or other persons who may be violating the immigration laws of the United States. Second, CBP creates lookout records for persons who are of interest to another law enforcement agency.

Private individuals and attorneys occasionally request explanations or information related to the possible reasons for an individual having been questioned at the time of application for admission to the United States. If an individual was questioned as part of the normal inspectional process, the response should be drafted accordingly. However, in those cases when lookout information was the reason for the referral to secondary inspection, the director having jurisdiction over the port-of-entry where the event occurred shall evaluate and answer any subsequent inquiry using the guidance set forth below.

The lookout database is considered a law enforcement system of records of which CBP is not the sole proprietor. The records to which CBP officers have access during the inspection process include entries made by other law enforcement and government agencies.

CBP may not disclose lookout information that has been provided by another law enforcement agency or government agency. CBP will forward the inquiry to the agency that owns the record. Without making any reference to the agency when responding to the inquiring party, the CBP response to the inquiring party will be limited to stating that the inquiry is being taken under consideration. [redacted] A copy of the CBP response will be included with the inquiry that is forwarded to the appropriate agency.

Section 601(c) of the Immigration Act of 1990 states that the Attorney General and the Secretary of State shall develop protocols and guidelines for updating lookout systems and similar mechanisms for the screening of individuals applying for visas for admission, or for admission, to the United States. Such protocols and guidelines are to be developed to ensure that in the case of an individual whose name is in such a system, and who either applies for admission or requests a review, without seeking admission, for the continued inadmissibility under the INA, if the individual is no longer inadmissible, his/her lookout record shall be removed from the lookout system and the individual shall be informed of such removal. If the individual continues to be inadmissible, the individual shall be informed of such determination.

Section 601(c) of the Immigration Act of 1990 authorizes CBP to disclose information relating to an individual's inadmissibility when the pertinent content of the record indicates that grounds already exist to support removal proceedings against the individual. The disclosure of an individual's lookout record is limited to information that confirms specific removal grounds, such as prior or final deportation from the United States, conviction for crimes that render the individual inadmissible from the United States, prior withdrawal of an application for admission to the United States and prior refusal of entry to the United States.

Any inquiries generated by lookout records created by the Department of State (DOS) may be forwarded to DOS for appropriate action. The DOS intends to implement an analogous procedure to respond to inquiries posed at the time of application for admission where an individual has been entered into the DOS CLASS database. Appendix 31-2 contains copies of the DOS letter that may be given to any individual who asks for information or assistance if his/her name appears in CLASS.

The sample letters contained in Appendix 31-2 contain suggested language for a variety of situations.

- Letter 1- Letter from the Office of Chief Counsel, when no specific information may be provided to the requester
- Letter 2- Letter from the Office of Chief Counsel, when grounds for removal exist
- Letter 3- Letter when grounds for removal exist
- Letter 4- Letter when grounds for removal exist
- Letter 5- Letter when no specific information may be provided to the requester

Appendix 31-3 contains an information notice used by the Department of State concerning procedures for inquiring about their lookouts.

## 31.8 DFO Random Quality Review of CBP Permanent Lookout Records.

The development of a quality review function for NAILS is a key part of the continuing effort to restructure CBP lookout system procedures that began in Fiscal Year 1993. In March 1994, the Office of the Inspector General (OIG) issued a NAILS Inspection Report that listed as one of its

recommendations the need to institute a routine systematic assessment of the content and the quality of the information used to create an INS lookout record. The implementation of this procedure is in response to that recommendation.

The reviewing officer contacts the reviewing officer at the field office in cases when a lookout record appears to be lacking sufficient information. After discussing any outstanding issues concerning the lookout record, the reviewing officer at the field office corrects any deficiencies in the record, approves it, and notifies the reviewing officer that the correction has been completed. In the event that the deficiency of the lookout record cannot be corrected, the record must be deleted immediately.

## Chapter 31.9 [redacted] (Added 2/16/06; CBP 18-06)

[redacted]

1. [redacted]

2. [redacted]

4. [redacted]

5. [redacted]

Accountability

[redacted]

3. [redacted]

Types of Records

[redacted]

## Chapter 32: Intelligence (Added INS - TM2)

32.1 INS Intelligence Program - General
32.2 Intelligence Collection Requirements; Instructions for Completing an Intelligence Report (Forms G-392 and G-392A)
32.3 The OASIS Database (Reserved)
32.4 Headquarters INS Intelligence Bulletin Board
32.5 INS Forensic Document Laboratory (INS/FDL)
32.6 EPIC Operations; Instructions for Completing Report of Documented False Claim to Citizenship (Form G-329)
32.7 Interpol

### 32.1 INS Intelligence Program - General.

(a) Organization. Under the general direction of the Associate Commissioner, Enforcement, the Assistant Commissioner Intelligence is responsible for administering the Service intelligence program. The program is directed in each region by the Regional Intelligence Officer who is assisted in its execution by intelligence officers in the major districts and Border Patrol sectors, by designated intelligence officers at the smaller districts and interior suboffices, and by Senior Immigration Inspectors and Special Operations Immigration Inspectors at ports-of- entry.

(b) Mission. The Intelligence Program provides support to the Enforcement, Benefits, and Inspections operating divisions as well as to the Commissioner. The primary program missions are:

(1) Supply reports which allow managers to make decisions on a national and international level in support of the Service mission;

(2) Provide tactical intelligence support and analytical reports for use by INS field units and other law enforcement organizations in the detection and disruption of smuggling operations and fraud schemes;

(3) Provide strategic analyses measuring the scope and nature of domestic and foreign illegal immigration activities which affect the United States;

(4) Provide fraud detection training to INS operational components, international immigration and enforcement agencies and international air carriers to maximize INS' deterrence effort;

(5) Furnish forensic laboratory support required for the enforcement of INS statutes;

(6) Carry out Service liaison commitments with federal law enforcement agencies and with members of the intelligence community responsible for the national security of the United States;

(7) Maintain liaison with foreign law enforcement agencies via Interpol; and

(8) Achieve Service commitments through use of EPIC's joint data bases.

(c) Headquarters Intelligence Division (HQINT). HQINT develops and implements the Service's intelligence policy and provides operational and administrative program oversight. Service intelligence collection requirements are established to obtain information which will aid policy makers in identifying trends which significantly impact on the operation of the Service. HQINT efforts are also designed to aid enforcement personnel by providing investigative and enforcement leads.

Liaison between INS and intelligence community agencies is authorized in 8 U.S.C. 1105. The purpose of this liaison is to exchange information for use in enforcing the provisions of the

Immigration and Nationality Act in the interest of the internal security of the United States.

Direct communication with districts, sectors, and sub-offices is authorized in connection with intelligence matters.

(d) Inspections Officers' Contributions. Immigration Inspectors play a vital role in identifying foreign and domestic based smuggling/vending operations through careful questioning of persons and examination of physical evidence such as business cards and stationery, address books, travel tickets, etc. Inspections is a key source of information on fraudulent and counterfeit documents and visas used to attempt fraudulent entry.

(e) The Intelligence Cycle. The Intelligence Cycle consists of four basic steps:

(1) Planning/Direction of Target Selection - A target (which can be a person, organization, or any issue of intelligence value) is selected, based on the needs of the Service, to support both enforcement and management objectives. Intelligence Collection Requirements have been developed to assist Intelligence Program elements in this step;

(2) Collection - The collection cycle starts with the gathering of raw or unprocessed information from a variety of sources including: public records, newspapers, foreign radio reports, travelers, refugees, confidential informants, physical and electronic surveillance, businesses, law enforcement services, foreign governments, military services, and other organizations;

(3) Processing Information - The information gathered (raw data) is organized (collated) into a logical sequence or pattern in such a way that relationships may be seen and acted upon. The potentially valuable information is separated from the raw data and converted into a finished product (report) which clearly distinguishes between facts and assumptions; and

(4) Dissemination - The finished product of the Intelligence Cycle is distributed to all entities of the Service that could benefit from the information, on a need to know basis.

## 32.2 Intelligence Collection Requirements; Instructions for Completing an Intelligence Report (Forms G-392 and G-392A).

(a) Standard Intelligence Collection Requirements. These standard Intelligence Collection Requirements (ICRs) relate to individuals and organizations, and their methods of operations and assets. These general ICRs apply to all threat categories which have been designated for intelligence collection.

(1) Organizations. The identity, role, and background of key figures, members, associates, and cooperating corrupt officials; member selection and recruitment criteria; organization history, purpose, strategy, and goals; hierarchy and geographic structure; front organizations; associations with other organizations and supporting groups; political, economic, and other influences exerted; rivalries, weaknesses, and other factors which

contribute to organizational instability and limit operations.

(2) Method of Operation.

(A) Operations: The areas, patterns, and methods of operation; the times, frequency, and sequence of actions in planning and conducting operations; capabilities and intentions for future criminal activities; false documents and information used in operations; transportation and travel patterns, routes, areas, and methods, use of commercial carriers, and corruption of carrier personnel; border crossing sites and methods; indicators of preparation for criminal activities; characteristics of clientele, methods, and locations for recruiting clients; cost of criminal services to clients, methods and schedules of obtaining payment; means of collecting, transporting, and laundering money; use of firearms and violence; other criminal activities and enterprises; political or other unusual motivation for criminal activities.

(B) Management: The means of organizational control and management; location, procedures, and roles in planning, decision-making, training, and preparing for activities; recruitment, advancement, discipline, and training methods; intelligence gathering against rivals; security methods and devices; methods of identifying, evading, and countering rival organizations.

(C) Communications: The methods of communication; types, operational characteristics and locations of communication equipment used, radio frequencies and range; telecommunication numbers; code words; encryption devices, and methods; computer software and passwords.

(D) Countermeasures: The methods of intelligence gathering against law enforcement; methods of soliciting and rewarding official corruption; means of identifying, evading, and countering law enforcement; countermeasures to INS patrols, inspections, and investigations; methods to access, review, create, alter, or destroy files in official record systems.

(3) Assets. The source, location, physical characteristics, ownership, identification, and registration identifiers of property and resources used or controlled by an organization or individual, including business, residence, safe house, and other facilities, conveyances, equipment, weapons, bank accounts, credit accounts, safe deposits, investments, real property, business records, currency, and other forfeitable property.

(4) Individuals.

(A) Persons: Identity, biographic date, fingerprint classification, physical features; locations associated with the individual's activities; marital status and family relationships; Social Security and law enforcement file numbers; criminal record and use of violence; identity and travel documents used and travel history; false identities and documents used; motivation, strategy, and goals; front organizations; associations with other individuals, organizations and supporting groups; political, economic, and other influence exerted; rivalries, weaknesses and other factors which limit individual operations.

(B) Aliens: Immigration admission record, prior removal, exclusion or deportation, current immigration status, equities in the United States, eligibility for asylum and other relief.

(b) Threat-Related Intelligence Collection Requirements. These threat-related ICRs identify specific information needs for each threat category. They apply to all individuals, organizations, methods of operations, and assets involved in the events and actions which constitute the threat.

(1) Foreign Conditions Affecting Immigration.

(A) Socio-economic conditions: Political, social, economic, public health, and similar conditions in foreign countries, and violent, severe, or rapid changes in those conditions, that may have an effect on: claims for refuge or asylum; resettlement in third countries; immigration, illegal, or fraudulent entry to the United States; and overstays or violations of status by nonimmigrants.

(B) Government policies: Attitudes and intentions of high level foreign government officials and international organizations towards emigration, refugee resettlement, and the transit of third country nationals for entry to the United States; cooperation with State Department and Service immigration control operations; and the creation of special benefits or programs for aliens.

(C) Corruption: Official corruption which facilitates immigration fraud, smuggling, counterfeiting, or illegal entry to the United States.

(2) Domestic Conditions Affecting Immigration.

(A) Socio-economic conditions: Political, social, economic, public health, and similar conditions in the United States, and violent, severe, or rapid changes in those conditions, that may have an effect on immigration, illegal, or fraudulent entry to the United States, and overstays or violations of status by nonimmigrants.

(B) Government policies: Attitudes and intentions of high level United States Federal, State, or local government officials toward immigration quotas and preferences, refugee resettlement, nonimmigrant entry, immigration control, border security, Service enforcement operations and resources, and the creation of special benefits or programs for aliens.

(C) Corruption: Official corruption which facilitates immigration fraud, smuggling, counterfeiting, or illegal entry to the United States.

(3) Fraud to Obtain Immigration Benefits and Naturalization.

(A) Method of Operation: The type of fraud scheme; type and source of documents used to support fraud claims; false issuance or creation of supporting documents or issuance of

quasi-official documentation; instructions to clients.

(B) Individuals: The identity, location, background, and characteristics of petitioners and beneficiaries involved in fraud; relationship to other persons involved in fraud schemes; place and manner of meeting fraud arranger; knowledge of fraud arranger operations before meeting; source of documents used to support fraud claim; means of obtaining funds for payment of arranger, and amount paid to arranger and others; intended destination, and arrangements for employment and residence; purpose of fraud scheme, if other than for permanent residence.

(C) Aliens: Immigration admission record, prior removal, exclusion or deportation, current immigration status, equities in the United States, eligibility for asylum and other relief.

(4) Alien Smuggling.

(A) Method of Operation: The places and means of entry; use and location of staging areas or facilities; associations with employers, document vendors, and other smugglers.

(B) Smuggled Aliens: The demographic characteristics of smuggled aliens; relationship to other smuggled aliens; route and means of alien's travel to and from the border; place and means of entry; place and manner of meeting smuggler and knowledge of smuggler operations; source of travel documents; means of obtaining funds for payment of smuggler and amount paid to smuggler and others; intended destination, and arrangements for employment and residence; purpose of entry if other than employment.

(5) Counterfeiting Immigration-Related Documents.

(A) Method of Operation: The type and cost of documents loaned, altered, or counterfeited; documents included in package deals; ordering, production, and delivery times, locations, and methods; instructions to clients when documents are delivered; method of retrieving documents to be used again; means of obtaining valid documents for alteration; methods to falsely issue or certify documents, or access, review, create, alter, or destroy files in record systems to support counterfeiting; actions to assist or encourage alien noncompliance with alien registration requirements; issuance of quasi-official identification or travel documentation.

(B) Stolen, Compromised, or Missing Documents: Characteristics of forged, altered, fraudulently used, compromised, missing, and stolen documents, security forms, stamps, seals, printing materials, and equipment; description, quantity, serial number and other identifying data; security identifiers and methods of detecting fraudulent documents; identity of person or entity from whom stolen or lost; date, circumstances, and location of theft or loss; description, quantity, and identifiers of lost or stolen documents which are recovered.

(C) Method of Production: Methods of production or alteration of documents; source and types of inks, stamps, paper, and other materials, equipment, and processes used; production site.

(D) Individuals: The identity of a person or entity from whom a counterfeit, compromised, or stolen document was recovered or confiscated; date, circumstances, and location of recovery; characteristics and identities of other persons who may be in possession of similar documents; purposes for which the document was obtained or used; means of obtaining the document; relationship to other individuals using or in possession of fraudulent documents; route and means of travel using fraudulent documents; place and manner of meeting counterfeiter; knowledge of counterfeiter operations before meeting; means of obtaining funds for payment, and amount paid to counterfeiter and others.

(E) Aliens: Characteristics of aliens using or in possession of fraudulent documents; intended destination, and arrangements for employment and residence if used for entry.

(6) Terrorism.

(A) Method of Operation: Identity and location of a target of terrorist action; reason for selecting the target person, place, or time; means, nature, place, and time of attack; method of gaining access to target; use of warnings, timing, and nature of warnings.

(B) Devices: Types of weapons, explosives, chemical agents, and other destructive devices used by terrorists; triggering mechanism; sources and means of obtaining or producing devices; means of transportation, emplacement, and concealment; means of detection, and disarming; safety measures to take during a search for a device and when encountered.

(C) Terrorist Individual or Entity: Motivation, beliefs, values, strategy, and goals of terrorism activity; prior terrorism actions alleged, claimed, or proved; association with other terrorism or criminal organizations, or individuals; association with other criminal organizations or individuals.

(7) Drug Trafficking.

(A) Method of Operation: The activities which indicate preparations for drug production, smuggling, or distribution operations or other criminal acts; selection criteria and methods of recruiting couriers for drug smuggling.

(B) Drugs: The location, type, amount, purity level, form, and value of drugs to be smuggled into or sold in the United States, or seized by, found, purchased as evidence, or surrendered to INS; source, route, and destination of raw materials, precursor chemicals, and drugs.

(C) Method of Concealment: The methods of concealment for drug production, storage, and transportation; source and type of materials used for packaging, labeling, concealing, and transporting; the location of facilities used to construct or alter containers and conveyances for concealment; the location of facilities and identification of persons who provide packaging, storage, and concealment services; indicators of concealment and means of detection.

(8) Entry Without Inspection and Mass Migration.

(A) Illegal Entry Infrastructure: Staging areas, lodging, travel, transportation, and other facilities which are available to and used by aliens prior to, during, and after entry without inspection.

(B) Method of Operation: Routes and methods of entry without inspection; knowledge of and countermeasures to Service patrols, inspections, and investigations; activities which indicate the preparation for illegal entry; indications of the presence of aliens, especially in large numbers, who may seek to be smuggled or attempt illegal entry.

(C) Aliens: Demographic characteristics of aliens who enter without inspection; number of times aliens have previously attempted entry or entered without inspection; time elapsed from prior visa denial, port-of-entry refusal, exclusion, filing or approval of visa petition, or prior deportation or other removal; employment and other living conditions in home country, knowledge of conditions in the United States, and the relative importance of factors which caused aliens to seek entry and choose their intended destination in the United States; source and type of information leading to the alien's choice of time, place, and manner of entry, route to and from the border, and means of travel; relationship to persons in the United States or other aliens attempting illegal entry; arrangements for residence and employment after entry.

(9) Employment of Unauthorized Aliens.

(A) Method of Operation: The hiring methods and employment practices of employers; type of employment violations committed; methods of committing violations; other employment discrimination, labor law or related laws violated; methods of transporting, harboring, or concealing unauthorized alien employees; methods of inducing or encouraging the illegal entry of aliens, or encouraging or soliciting the use of smugglers or counterfeiters, to obtain unauthorized aliens for employment; efforts to resist or obstruct the enforcement of employer sanctions, or encourage employer noncompliance.

(B) Employers and Facilitators: The identity, location, and characteristics of employers who engage in the employment of unauthorized aliens; job markets, entities or individuals which assist unauthorized aliens to obtain employment; the relationship of employer violators to other employers; employees involved in committing violations.

(10) Aliens Involved in Crime.

(A) Organizations: The hierarchy, methods of operation, and assets of criminal organizations and groups which are led by or composed largely of aliens, and the characteristics, background, location, role, and identity of alien leaders, members, and associates.

(B) Criminal aliens previously deported: The identity, location, and characteristics of criminal aliens who have previously been excluded, deported, or removed at government expense,

and are likely or attempting to seek reentry to, or have reentered, the United States, the intention of such aliens to reenter.

(11) Sensitive Events.

(A) Visits, Meetings and Other Events: The date, place, duration, sponsors, purpose, and parties involved in international competitions, festivals, conferences, diplomatic or political visits and meetings, or other events to be held in the U.S. or adjacent countries; the number and characteristics of aliens who are likely to participate or attend as spectators and will seek entry to or transit through the U.S.; incidents which may require the Service to control or prohibit the entry or departure of an alien or group of aliens; actions, preparations, and intentions of citizens or aliens to oppose or disrupt visits, meetings, and other events.

(B) Individuals: The identity, characteristics, and travel plans of foreign heads of state, government officials, celebrities, or other well-known or notorious persons whose presence in or travel through the United States is likely to arouse the interest of or opposition by citizens, aliens or groups in the United States; the identity and characteristics of aliens who have been denied a visa to seek entry to or transit the U.S. to attend conferences or other events.

(12) Threats Against Service Operations.

(A) Method of Operation: Identification and location of Service personnel, detainees, facilities, or operations which are the target of a threat; place, time, and nature of hostile or disruptive action; means of access to Service personnel, operations, and facilities; use of warnings, and the timing and nature of warnings.

(B) Devices: Types of weapons, explosives, chemical agents, traps, and other hazardous or destructive devices used; source and means of obtaining or producing devices; triggering mechanism; means of transportation, emplacement, concealment, and detection of devices; safety measures to take during a search for a device and when encountered.

(C) Threat Individual or Entity: Motivation, beliefs, values, strategy, and goals of activity; prior disruptive or threatening actions alleged, claimed, or proved.

(13) Excludable or Deportable Aliens.

(A) Excludable or Deportable Aliens, and Refugees and Other Aliens: The identity, location, and characteristics of aliens who are excludable or deportable, or are likely to seek to be removed from the U.S. at government expense, or are likely to seek refuge, asylum, or temporary protected status in the United States.

(B) Aliens Previously Deported: The intentions and preparations of such aliens to reenter.

(14) Threats to National Security.

(A) Method of Operation: Identity and location of a target of terrorist action; reason for selecting the target person, place, or time; means, nature, place and time of attack; method of gaining access to target; use of warnings, timing and nature of warnings.

(B) Devices: Types of weapons, explosives, chemical agents, and other destructive devices used by terrorists; triggering mechanism; sources and means of obtaining or producing devices; means of transportation, emplacement, and concealment; means of detection and disarming; safety measures to take during a search for a device and when encountered.

(C) Terrorist Individual or Entity: Motivation, beliefs, values, strategy, and goals of terrorism activity; prior terrorism actions alleged, claimed, or proved; association with other terrorism or criminal organizations or individuals; association with other criminal organizations, or individuals.

(c) Intelligence Reports.

(1) Preparation. Please assure that all of the following categories are filled in appropriately before the report is submitted to HQINT or the field for distribution. An Intelligence Report that is properly and completely filled out is of greater value than ones which contain missing or incomplete information.

(A) File Number: This space may be used by the reporting office for their own internal reference and file codes. HQINT does not currently use this space. Preparing officers should NOT use an alien's file number for this purpose.

(B) CCX: Cross-references may be listed in this space. At a later date, this space may be used by HQINT for a referencing and indexing system.

(C) Date of Information: The date of the occurrence of the event being reported or the date the information is first received by the writer of the G- 392. This is not necessarily the same as the date the report is written. The Date of Info. is always a date earlier or equal to the Date of Report.

(D) Subject: The major topic of the report. Generally, the subject should be the same as the Collection Requirements, e.g., Alien Smuggling, Drug Trafficking, Document Fraud, Illegal Entry, etc. Aliens names are not to be used as the subject of a report.

(E) Country: This space is used to provide the country of birth of the alien(s) involved in the incident being reported. Intelligence Reports are reviewed by HQINT analysts based upon the nationality (country of birth, not citizenship). The nationality of the smugglers/arrangers or the country of citizenship of the alien(s), as additional information, is beneficial; but the most important country indicator for intelligence purposes is the country of birth of the alien(s). Do not put U.S. or USA in this space unless the individual was actually born in the United States.

(F) OASIS and OASIS ID No: The report writer should indicate whether or not OASIS was checked. If the information is checked in OASIS and there is an existing record, the OASIS ID Number should be recorded on the Form G-392. If no existing information is found, but a new record is created, the new OASIS ID Number should be recorded on the Form G-392.

(G) Databases Checked: Any databases checked for information related to individuals involved in the incident should be noted. This will eliminate duplication of efforts. Information derived from any positive hits should be included in the body of the report.

(H) Synopsis: A brief description of the incident or intelligence reported under Details.

(I) Details: A description of a single event or topic which responds to a Collection Requirement. A continuation sheet, Form G-392A, may be used if more space is needed. The body of the report should begin with a narrative assessment of the reliability of the source of the information and the accuracy or validity of the information itself. The report should contain specifics of the incident, the nationalities of the parties involved, any associated trends, and the outcome of the incident.

Review the intelligence collection requirements which relate to the information you are reporting. Be timely, specific, and complete. Provide information in the Details section in the following order.

Include in the first paragraph of details a reference to any previous reports submitted on the same incident or subject, or identify the specific request for information which the report answers.

Evaluate, and provide a brief statement indicating the reliability of the source of the information. The statement should indicate the source's record, if any, for providing reliable information, and the method or closeness of the source's access to the information. Do not identify sources of information by name, address, position in an organization, relationship to another person, or any other information which may compromise the identity or location of the source. However, if the source is a representative of another agency, indicate the agency and the level within the agency, such as headquarters, field office, etc. If the source is the one of the subjects of the report, describe the source's actions or statements from the viewpoint of a third party observer.

To the greatest extent possible, provide background information which reveals and explains methods of operation, capabilities, intentions, vulnerabilities, and interrelationships of individuals and organizations, and specifically identifies individuals, organizations, conveyances, assets, and locations involved.

If appropriate, explain unusual terms or practices, or provide a brief assessment of the information reported. This can include a prediction of future actions or trends, a comparison to past actions, or an estimate of the significance of the reported information.

Conduct record system checks relating to all persons, organizations, and, if applicable,

addresses, conveyances, and telephone numbers listed in the report. Identify systems checked and provide file numbers or other data, or indicate that there is no record. If possible, attach a printout.

(J) Writer: The writer of the report should type their full name, job title, and telephone number. All inspectors should identify the type of inspector that they are, i.e. II, SRI, SOI, IIO, etc. HQINT has been tasked with providing HQINS with a monthly status report on Inspectors' participation in the G-392 reporting program. Investigators should put INV after their names. Border patrol agents should put BPA after their names, as a monthly status report is also provided to HQBOR. Telephone numbers should be given so that if additional information is needed, the writer can be contacted.

(K) Date of Report: The date the report is written. This should not be confused with the Date of Information, which is the date the information was received or the date the incident occurred. The Date of Report is always equal to or later than the Date of Information.

(L) Reporting Office/Activity: The three-letter office code assigned to the writer's location. For example, if the writer is assigned to New York City, the code would be NYC. If the writer is assigned to Swanton, the code would be SWB. If the location has a suboffice, then the code would be, for example, Toronto, TOR/BUF. Do not use numbers for program elements in this space. In the past, writers have used 1221, for example. This could be any Border Patrol location and does not specifically designate a single writer's location. Please use only specific three-letter codes. It is very important to fill in this space correctly so that HQINT will know where to return the evaluation of the report and any other correspondence relating to a report.

(M) Additional Pages: If addition pages are required, use Form G-392.1 (Intelligence Report Continuation Page). Indicate the topic which was entered in the same block on the first page of the report and (if applicable) cite the Request For Information (RFI). Since the synopsis of the report is written on the first page, it should not be repeated on any continuation page.

(N) Attachments: Attach other reports, record check printouts, maps, photographs, or other materials. Cite attachments in the report. Do not repeat large amounts of information reported in attached documents.

(O) National Security Information: Call HQINT (number below) or the Headquarters Command Center (202-514-8289) by secure telephone if the information reported relates to national security and may require security classification.

(2) Distribution: Routine distribution is indicated on the bottom right corner of the various multi-part copies of Form G-392, as follows:

Original - HQINT,
Copy 1 - ROINT,
Copy 2 - District or Sector,

Copy 3 - EPIC, and
Copy 4 - Originator.

Copy 2 is for use when Form G-392 is prepared in offices under the jurisdiction of a district or sector, i.e., border patrol stations, ports-of-entry, suboffices within a district, etc.

When additional distribution is made, the offices to which the form is sent should be identified at the top of the form. Examples of supplementary distribution include FDL, ROINTs, other than the one with jurisdiction over the reporting office, neighboring districts and/or sectors, etc.

All reports containing drug trafficking information must be forwarded to EPIC. EPIC has been designated as the primary office with responsibility for collection of intelligence relating to drug trafficking. Analysis and evaluation of all drug reports is performed at EPIC. Please forward these reports to:

EPIC
11339 SSG Sims Street
El Paso, TX 79908-8098
Attn: R&A Trends.

These reports may also be faxed to EPIC, Attention: R&A Trends, at (915) 564-2102.

Forward copies of the report immediately to HQINT, ROINT, EPIC, and the district or sector. Also forward copies immediately to any other INS office or other agency which has jurisdiction over, or a likely interest in, the reported information. Notify receiving offices by telephone if appropriate, and send time-sensitive information by telefacsimile or teletype. Retain the Originator copy in the local office intelligence files. Do not place a copy of this report in any alien file or case file.

(3) Obtaining Intelligence Reports. HQINT generates a number of reports in various formats which are disseminated through the Service as indicated. Each month a list of reports and bulletins issued during that month is published in the Immigration Monthly Summary, along with information on obtaining copies of any reports which might have been missed.

(A) Officer Safety Bulletin Document Intelligence Alert - This report describes dangers or threats to line officers. It may involve terrorist threats, concealed weapons, particular diseases to which officers may be exposed. It is disseminated to all offices as soon as the threat or danger becomes known.

(B) Executive Intelligence Brief FDL Reference Paper - This ad hoc report deals with priority issues and is normally distributed to the INS Executive Staff, to Main Justice, and to district directors and chief patrol agents. Although not targeted to individual officers, any officer needing a particular copy may request it through HQINT.

(C) Intelligence Bulletin - This ad hoc report describes trends in various illegal entry and

smuggling schemes. It is targeted to the Inspector and other line officers.

(D) Strategic Assessment - This is a rather lengthy type of report which is very analytical and detailed. It provides information on particular large scale smuggling trends and similar issues.

(E) Operations Analysis - This case support report deals with a particular case, problem, or issue affecting an individual office. It is only distributed beyond the office involved upon the permission of that particular office.

(F) Immigration Monthly Summary - This is the only report which is published on a scheduled basis. In addition to the listing of the reports and bulletins issued during the preceding month, it also contains summaries of reports issued by regional intelligence officers, with contact points. On a semi-annual basis, it also contains a listing of all reports and bulletins issued during the immediately preceding six month period.

A listing of recent document alerts and other intelligence information is contained in Appendix 32-1.

## 32.3 The OASIS Database. [reserved.]

## 32.4 Headquarters INS Intelligence Bulletin Board.

(a) General. Headquarters Intelligence established a Intelligence Bulletin Board (HQINSINTEL) on the Treasury Enforcement Communications System (TECS) on March 21, 1996. All TECS users have read only access to the bulletin board. Posting capability to the system is limited to selected INS personnel. The purpose of the bulletin board is to exchange pertinent and timely Immigration intelligence.

(b) Rules for Bulletin Board Operation.

(1) HQINT is final authority on article content, length, duration of posting, and officer access.

(2) No national security information or case sensitive information will be posted.

(3) Articles must be short and concise (usually less than two screens).

(4) Articles must have value for INS readers outside of writer's district or sector.

(5) The title of the article must describe the article content.

(6) The bulletin board will rarely be used for lookout entries, such as for terrorists.

(7) Posting articles does not alleviate the responsibility to submit G-392s as required.

## 32.5 INS Forensic Document Laboratory (INS/FDL).

(a) General. The Forensic Document Laboratory (FDL) provides a wide variety of forensic document analysis and law enforcement support services for the Immigration and Naturalization Service. The FDL Forensic Section conducts scientific examinations of questioned document evidence and testifies to their findings as expert witnesses in judicial proceedings. On a case by case basis, forensic examinations are conducted for other Federal, State, and local law enforcement agencies. The FDL Intelligence Section develops and presents training programs in the detection of fraudulent documents, assists field personnel in identifying fraudulent documents, and conducts ongoing liaison with other Federal, State, local agencies and foreign governments to promote common efforts to combat international document fraud.

The FDL provides the following primary services and products:

(1) A full range of forensic support through the scientific examination of handwriting, hand printing, stamps, seals, printing, typewriting, the restoration of obliterated or altered documents, the examination of suspected counterfeit documents, and the processing of evidence for latent fingerprints.

(2) Expert witness testimony by qualified forensic personnel in judicial proceedings and hearings on the examinations they conducted. Preparation of photographic court charts to support the prosecution of these cases.

(3) Technical advice and assistance in developing major cases involving fraudulent documents. This includes support to approved undercover operations.

(4) Training programs in detecting fraudulent documents, and recognizing and handling documentary evidence. Training programs can be geared to specific programs or areas of concern. In order to request a training program, contact the FDL Intelligence Staff at (703) 285-2482 during business hours. A listing of several recent training programs is contained in Appendix 32-2.

(5) Preparation and distribution of Document Intelligence Alerts (high quality, color photo bulletins distributed worldwide to assist field personnel in the identification of fraudulent documents recently encountered at the FDL). The FDL currently distributes over 500 copies of Document Intelligence Alerts worldwide to INS offices, U.S. Embassies, and other law enforcement agencies. If your INS office is not receiving copies or if you would like to request previously distributed copies, please contact the FDL's Intelligence Section at (703) 285-2482. An updated listing of the *Alerts* can be found on the cc:Mail Forensic Document Laboratory Bulletin Board.

(6) Maintenance of an extensive library of exemplars of visas, passports, vital statistics documents, immigration documents, and other documents for use by both Forensic Document Examiners and Intelligence Officers for comparison with questioned documents. Copies of documents and other material needed in connection with a specific case may be obtained upon request. Field personnel are encouraged to submit intercepted fraudulent documents to the FDL for the FDL Library and for use in document training and in the production of Document Intelligence Alerts. Whenever possible, original documents should be provided to the FDL.

(7) Assistance via Photophone in resolving questions concerning suspect travel documents on a real-time basis. Extended hours of service to INS field by Senior Intelligence Officers seven days a week.

(8) A close working liaison with the Office of Fraud Prevention Programs (CA/FPP) and the Bureau of Diplomatic Security (DS), U.S Department of State.

(b) Requests to FDL for Forensic Examination of Evidence.

(1) Assistance in Preparation of Evidence for Submission. For assistance and advice in the preparation of a case for submission to the FDL for forensic examination, submitters are encouraged to contact the Chief Forensic Document Examiner at (703) 285-2482 or fax (703) 285-2208.

(2) Transmission of Evidence to FDL. Each transmission of evidence to the FDL must be accompanied by a "Request For Laboratory Examination" (G-1021). Form G-1021 is available in electronic format on the FDL Bulletin Board, or may be obtained by contacting the FDL as above.

All evidence must be transmitted inside a sealed inner envelope, with the completed G-1021 attached to the outside of that inner envelope. Multiple cases may be submitted in a single Federal Express mailer or other mail medium, but each case within the outside envelope must be separately packaged exactly in the manner described above.

Any cases that do not adhere to these instructions will be returned to the requestor, accompanied by instructions on submitting the case in the prescribed manner. Requests and evidence should be sent via registered U.S. Mail, Certified U.S. Mail, or the current courier/package delivery service (e.g., Federal Express) in order to maintain tracking of the chain of evidence. Requests and evidence must be addressed to:

Chief Forensic Document Exarniner

INS Forensic Document Laboratory
Warren Building, Suite 325
8000 Westpark Drive
McLean, VA 22102-3108

In keeping with standard legal requirements, the FDL will return the examination report and the evidence to the same person who submitted and signed the "Request For Examination", unless other specific instructions are received.

(c) Preparation for Court. In the event that a case is scheduled for a trial or hearing, it is very important that the following procedures be followed.

The case officer who submitted the evidence must immediately contact the FDL Forensic Document Examiner or Fingerprint Specialist who examined the evidence.

The evidence must be returned to the FDL at least two weeks (if possible) before the trial to permit preparation of court charts.

A subpoena for the Forensic Document Examiner or Fingerprint Specialist must be obtained and should be faxed to the FDL. The FDL case control number should be included on the subpoena.

(d) FDL Support of Undercover Operations.

(1) Guidelines. The FDL provides technical support upon request for undercover operations that have been properly authorized in accordance with the Attorney General's Guidelines on INS Undercover Operations. FDL Policy Memorandum #3 (April 1997), a copy of which can be provided upon request, provides guidance in the submission and handling of requests from INS officers for FDL support for approved undercover operations.

(2) Approval. FDL is authorized to support INS undercover operations only in those cases where the proposed undercover operation has been approved at the appropriate level in accordance with The Attorney General's Guidelines for INS Undercover Operations. The three categories of approved undercover operations are:

- Those undercover operations which must be authorized by the INS Commissioner, with the concurrence of the Assistant Attorney General for the Criminal Division;
- Those which must be authorized by the INS Regional Director; and
- Those which must be authorized by the appropriate District Director or Chief Patrol Agent.

(3) Preliminary Feasibility Discussions. When an INS officer is planning an undercover operation which will require support from the FDL in the form of "operational documents", that officer should call the Chief Intelligence Officer to discuss the technical feasibility of the proposed request. If the proposed action is considered technically feasible to carry out, the Chief Intelligence Officer will inform the FDL Director, and will advise the requesting officer to take the following steps:

- Ensure that a generalized statement is included in Form G-819 (or addendum to the G-819, if the decision to utilize an undercover document was made subsequent the preparation of the G-819) that the proposed operation will use documents which will be provided by the FDL. The G-819 or addendum should clearly state how the documents will be used in the operation.

- Once the G-819 is approved, a written request from the Assistant District Director, Investigations or the Appropriate Assistant Chief Patrol Agent must be forwarded to the Director, INS Forensic Document Laboratory, which will include the following:

- A copy of the approved G-819, including the approval signatures;

- A statement as to precisely what is needed (as previously discussed in the preliminary feasibility discussions);

- Both the cover data and genuine identifying data of the person for whom the document is to support;

- A statement as to who will be the responsible INS officer to control and return the documents; and

(4) Approval for FDL Production. Upon receipt of the request from the field with the approvals as described above, the request will be reviewed and considered for approval both by the Director, FDL and the Assistant Commissioner, Intelligence (HQINT). This final approval will be attached to the incoming request and becomes a part of the FDL case file. Actual production and delivery of operational documents to support approved INS undercover operations will be carried out only after the above approval process, and in consideration of other INS cases pending.

(e) Undercover Support to Agencies Other than INS. Support to agencies other than INS will be subject to:

(1) Case load,

(2) Feasibility, and

(3) Review by the Chief Intelligence Officer and approval on a case-by-case basis by the Director, FDL and the Assistant Commissioner, Intelligence. (Requests must come from an appropriate level official at the requesting agency's headquarters.)

Priority will be given to supporting INS operations and INS forensic casework. It is a general policy of FDL to support only INS undercover operations.

(f) FDL Points of Contact. Questions concerning FDL should be addressed to:

Forensic Document Laboratory
8000 Westpark Drive, Suite 325
McLean, VA 22102-3108

Address the query to the attention of the appropriate FDL staff person(s), as follows:

RE: FDL policy matters: Director,

RE: Forensic and Fingerprint matters: Chief Forensic Document Examiner,

RE: Support to INS Undercover Operations: Chief Intelligence Officer,

RE: Document Intelligence matters: Intelligence Staff, or

RE: Fraudulent Document Training: Intelligence Staff.

(g) FDL Communications Capabilities. Any of the following communications media may be used in contacting the FDL.

- Telephone at (703) 285-2482 (7am – 8:30pm, Monday – Friday and 10am – 6:30pm, Saturday/Sunday/Holidays).
- Photophones: [redacted]
- STU-III Secure Telephone: Call in advance to set up a secure telephone link.
- Facsimile Machine: [redacted]NEC NEFAX-D800 high resolution terminal).
- INS Headquarters 24-Hour Emergency Number: (202) 616-5000 (INS Command Center). Ask for assistance in reaching an FDL representative if unable to reach at FDL numbers above.

(h) Guide for the Collection and Submission of Exemplars in Cases of Suspected Passport Fraud. If you suspect that a passport may have been fraudulently altered,

be sure to collect handwriting and fingerprints from the person who is carrying that passport. You should do the following:

The use of this guide when submitting a passport for examination will help ensure that the Forensic Document Laboratory will be able to provide the very strongest conclusion possible from the evidence provided.

**FOR ANY ASSISTANCE PRIOR TO COLLECTION OR SUBMITTING EVIDENCE, PLEASE CONTACT THE CHIEF FORENSIC DOCUMENT EXAMINER AT 703-285-2482.**

(Revised IN00-10)

## 32.6 EPIC Operations; Instructions for Completing Report of Documented False Claim to Citizenship (Form G-329).

(a) General. - The El Paso Intelligence Center (EPIC) is a multi-agency tactical and operational intelligence facility located in El Paso, Texas. The EPIC Charter has three basic tenets for the coordination of tactical and operational intelligence as it relates to:

- Narcotics trafficking,
- Alien smuggling and other related immigration violations, and
- Weapons trafficking.

INS is a full-member agency of EPIC, and provides staff through its Intelligence Division. The INS Advisory Board Member is the Assistant Commissioner for Intelligence, and INS is represented at EPIC by a Senior Special Agent of the Intelligence Division who also functions as the agency Program Coordinator.

(b) INS Mission at EPIC. EPIC was established to collect, process and disseminate intelligence information concerning illicit drug and currency movement, alien smuggling, weapons trafficking, and related activity. These EPIC intelligence requirements are connected directly or indirectly to the duties of INS officers in the field. Individual INS officers may query EPIC for intelligence on these topics in support of their enforcement activities in the field. If there is information on file or if there is a negative response to a query, EPIC will respond directly to the requestor. If there is an active case involving the subject of the query by a participating agency, EPIC will advise both the requestor and original owner of any information or record depositied with EPIC. EPIC will not release information pertaining to an active investigation (unless the subject is armed and dangerous), but will facilitate contact between the requester and the relvant case officer.

The INS mission functions at EPIC are listed below:

(1) INS Special Agents support the EPIC Watch Command. The EPIC Watch Command is operated 24 hours a day, 365 days a year and responds to telephonic, wire, and computer inquiries from member agencies. EPIC provides real time access to member agency databases and the El Paso Intelligence Database (EID).

(2) INS staffs the Nationality Identification Search Unit (NISU) which is a sub- unit of the Watch Command. This unit provides a wide variety of services to INS and member agencies, as listed below:

NISU receives and databases into OASIS between 6,000 and 9,000 Alien Smuggler Data Input Sheets (Form G-170s) per year. The G- 170 is a standard form used by Border Patrol Agents to report events involving the apprehension of individuals involved in alien smuggling. It is an excellent source of information for intelligence purposes.

NISU maintains the Fraud Document Index and Database. This system has been in existence at EPIC for 22 years and is an index of documented false claims to citizenship. The system presently has 550,000 database records and 1,600,000 documents on microfilm.

INS maintains a staff of Intelligence Analysts who conduct analysis of all smuggling organizations based on multi-source reporting (i.e., G- 170s, G-166s, and I-392s). Additionally, all I-44s of drug seizures are evaluated and databased.

(c) Access to EPIC Information. INS officers, since they work for a member agency, can have a variety of database and lookout systems searched by EPIC if they are not immediately accessible to the officer in the course of his duties. These include CIS, NIIS, TECS/IBIS, STSC, NAILS, DACS, and CLAIMS. EPIC itself owns a system known as the "Fraudulent Document Index System" or FDIS. FDIS contains information on more than 500,000 cases involving fraudulent documents. More than 1.6 million individual documents connected to these cases have been microfilmed.

EPIC is also the home of the Nationality Identification Search Unit (NISU). The NISU stores and maintains case files realting to individuals who have presented documents in support of false claims to U.S. citizenship, the true names of impostors, suspect issuing officials, individuals who have fraudulently filed birth certificates, and other situations incident to false claim activity.

(d) Contacting EPIC. An INS officer can contact the EPIC General Watch at 1-800-351-6047 (outside of Texas) or 1-800-527-4062 (inside Texas) for general inquiries. The NISU can be contacted throught the General Watch (NISU is a sub-unit of the Watch Command) or directly at 915-564-2140/2142/2143 for assistance.

(e) Instructions for Reporting False Claims and the Fraudulent Use of Documents, and Related Matters.

(1) Use of Form G-329. Form G-329 provides a statistical and case record of the confiscation of documents used or produced fraudulently, and a summary of information about the arrest or identification of an alien who can be charged for a criminal violation involving a false claim to a lawful status or citizenship in the United States, or other fraudulent production, use, or possession of a document. Data on Form G-329 is used by INS and other agencies for intelligence purposes, and may be reported to the Uniform Crime Reports System.

Form G-329 should be executed immediately when a false, altered, counterfeit, or fraudulently used document is seized, collected, or purchased as evidence by a Service employee during a law enforcement activity, or when it is determined that an alien has made a false claim to a lawful status in the United States.

Form G-329 is a record of information obtained through direct observation by a Service officer, provided by an arrestee, or derived from other sources, concerning the type, source, and manner of acquisition and use of documents, and the circumstances in which a false claim was made by an alien. The original or photocopy of reported fraudulent documents must always be submitted with Form G-329. Therefore, data reflected on the document, such as name, registration number, or issuing agency, does not need to be recorded on Form G-329, and space is not provided for this information. **Classified national defense security information should NOT be entered on Form G-329.**

(2) Preparation of Form G-329. To ensure legibility Form G-329 should be typed, but may be printed by hand. Preparing officers are requested to heed the following comments.

(A) Checklists. Checklists and block formats on Form G-329 generally provide all possible choices and indicate whether only one choice or several choices can be checked. When information is checked off on a checklist, or provided in a block on the form, it is not necessary to repeat the information in the narrative, unless additional identifying details are available.

(B) Negative Responses. When Form G-329 is prepared there should not be any narrative block or checklist section left blank except when specifically allowed in paragraphs f and g below, or when the information is included in an attached report on another form, such as Form I-213 or Form I-44. Generally, negative responses will be indicated by entering the word "None", "N/A" or "Unknown", or checking a block labeled "No", "Not Applicable", "None", or "Unknown".

(C) Abbreviations. Some blocks require the entry of abbreviations. Care should be used to ensure that abbreviations are clearly legible and not written in a manner which would cause the answer to be confused with another possible answer.

(D) Date and Time. Dates should be reported in the format mmddyy or mm- dd-yy or mm/dd/yy with leading zeroes. Times should be reported on the basis of a 24 hour clock, e.g. 4:25 p.m. would be stated as 1625.

(E) Other Information. When the space available in the narrative block or other blocks on Form G-329 is not adequate to contain all the pertinent information, provide the additional information on an attached memo, G-166 or other report.

(F) Redundant Information on Form I-213. When Form I-213 is used to report the apprehension of an alien relating to a document reported on Form G-329, enter the Subject name, and Suspected of Using blocks, and leave the rest of the Subject section of Form G-329 blank. Complete the remaining sections of Form G-329. It is not necessary to include in the Narrative information which is included in the Narrative of Form I-213.

(G) Definitions of Block Headings: Most blocks on Form G-329 are self- explanatory and these instructions are therefore general in nature. These instructions follow the sequence of blocks as they appear on the form.

- Program, Office, INS File Number. Indicate the program responsible for completing the Form G-329. Enter the three letter code designating the district or sector, and the suboffice, station, port, or other location of the reporting office. Enter the number of the Service "A" file or case file relating to the principal person or case.

- False Claim to (Checklist). Indicate the type of false claim made by the alien, or for which the document was used or is intended to be used. Check all blocks which apply, and enter a two or three word description of any other false claim or fraudulent use. Identify the location, date, and time when the false claim or fraud occurred.

- Subject. Provide summary information about the person who was in possession of the document, or who made the reported false claim. Report as much identifying information as is known. If an arrest report such as Form I-213 is attached, enter name, date of birth, and file number to assist in cross referral to the arrest report, and complete only those blocks not included in the attached report.

- Suspected of Using. Indicate whether the subject was under the influence of drugs or alcohol, or used a computer in the commission of the false claim or fraud offense.

- Document Data. Provide information relating to the form of the document and apparent alterations, and the purposes for which the form has been used. Each checklist indicates the correct number of blocks to check.

- Narrative. The narrative should clearly state the information which will support administrative or judicial revocation or forfeiture, and prosecution. If pertinent information is contained in other reports or memoranda, refer to those reports. Provide a brief description of the articulable facts which gave rise to probable cause for the search, arrest, or apprehension which led to the reported document. Report other significant information which is not reported or not completely reported elsewhere on Form G-329.

- Source. Provide information about the identity of the source of the document, and the place and manner in which the document was obtained from the source.

Type of Location. Briefly describe the type of location where the document was obtained. Use terms such as "travel agency," "convenience store," "street corner," and similar phrases.

Other person involved. Identify any other person who was involved in producing or obtaining the document.

Summary of Documents Provided by the Source (Checklist). Indicate each type of document provided by the source. Check as many blocks as apply, and enter in the blank spaces any other type of document not listed.

- Other Documents In Possession of the Subject (Checklist). Indicate each type of document found in the subject's possession, whether or not provided by the source. Check as many blocks as apply. The first section relates to documents which are known or believed to be valid and relate to the true identity of the subject, and the second section relates to documents which are known or suspected to be fraudulently obtained, produced, or altered. If the Subject was not in possession of documents, check "None" and leave these sections blank.

- Disposition. Indicate the administrative and criminal proceedings authorized against the subject of the report. Enter the Title and Section of the United States Code and number of counts charged against the Subject of the report. If prosecution was accepted by a State or local jurisdiction, indicate the State by abbreviation, and enter a short title for the criminal violation charged, e.g. "NY - use false DL".

(3) Disposition of seized documents. Valid documents relating to an arrested subject should be stored with the subject's other personal property and turned over to the appropriate custodial agency. Documents which will be used in evidence should be inventoried and stored in a secure cabinet. Documents which must be forensically examined should be forwarded to the INS Forensic Document Laboratory.

(4) Filing and distribution of Form G-329. Place the original Form G-329 in the relating Service A file or case file. Send a photocopy to HQINT and EPIC.

## 32.7 Interpol. (Revised 2/10/06; CBP 17-06)

(a) General. INTERPOL stands for the International Criminal Police Organization, the worldwide law enforcement confederation created to facilitate international police investigative inquires on individuals, groups, businesses, and organizations involved in international crime. INTERPOL headquarters are referred to as the Office of the General Secretariat (SG), and are located at Lyons, France.

INTERPOL has 182 member countries, whose police forces cooperate with those of other member countries to combat international crime. INTERPOL communications occur through National Central Bureaus (NCBs) established and maintained by member countries. The U.S. National Central Bureau of INTERPOL (INTERPOL - USNCB) is located at Washington, DC, and is an agency within the Department of Justice [Member Countries Listed in Appendix 32-3].

The INTERPOL organization has no police powers or arrest authority. Instead, INTERPOL member country NCBs exchange information with other member country NCBs, each of which relays incoming investigative requests to the appropriate police agencies in their respective countries. The receiving police agency then handles the investigative request in accordance with its country's laws and regulations.

(b) History. The concept of achieving cooperation among police agencies in different countries was realized with the creation of the International Criminal Police Organization (ICPO) in 1923. Initially conceived as a means for a small number of European countries to facilitate reciprocal police matters, INTERPOL has grown to a worldwide consortium of 182 member countries.

In 1938, appropriate legislative authority permitted the Attorney General to accept membership in INTERPOL on behalf of the United States. The Federal Bureau of Investigation was initially designated as the U.S. agency to perform INTERPOL functions. Shortly thereafter, however, INTERPOL operations ceased under German domination of Europe during World War II. In 1946, INTERPOL was re- established under a new constitution, which provided for elected directors and other safeguards to prevent usurpation by any single member country.

The United States resumed participation in 1947, with the FBI again designated to perform INTERPOL functions. The FBI withdrew from this role in 1950. The U.S. Treasury Department, however, wanted to maintain international police contacts for its far-ranging enforcement responsibilities over currency, customs, and narcotics violations, and continued an informal liaison with INTERPOL. In 1958, the Attorney General officially designated the U.S. Treasury Department to perform the INTERPOL role for the United States.

Early in 1977, a Memorandum of Understanding was effected between the U.S. Departments of Justice and Treasury to share official U.S. INTERPOL representation and operating activities. The memorandum was subsequently amended, and in 1981 the INTERPOL - U.S. National Central Bureau (USNCB) was designated as an agency within the U.S. Department of Justice. In the spring of 2003, this memorandum was again revised to share official U.S. INTERPOL representation and operating activities and outline the relationship between the U.S. Department of Justice and the Department of Homeland Security.

The INTERPOL network utilizes the support of a permanent administrative and technical staff at the Office of the General Secretariat (SG) at Lyons, France. The Lyons SG headquarters maintains an extensive and sophisticated, state-of-the-art telecommunications system, which provides rapid exchange of information between and among the member countries and the General Secretariat. The United States also has several investigative personnel seconded to the General Secretariat.

(c) National Central Bureaus (NCBS). Each INTERPOL member country establishes a point of contact and coordination to perform INTERPOL functions. Generally, this activity is undertaken by a component of the national police in the capital city of each country. The designated agency of the member country is then identified as the INTERPOL National Central Bureau (NCB).

Each INTERPOL member country operates its NCB within the parameters of its respective national law and polices, and within the framework of the INTERPOL constitution. As previously stated, the INTERPOL U.S. National Central Bureau is an agency with the U.S. Department of Justice. Known within the international community as INTERPOL-Washington, the USNCB fills a unique role within the complex network of U.S. police and federal enforcement jurisdictions, serving as a point of contact for both domestic and foreign police seeking assistance in criminal investigations, which extend beyond national boundaries.

(d) USNCB Staffing. The USNCB is staffed by federal and state law enforcement agency representatives, complemented by full-time case analysts and telecommunications specialists. CBP presently has one Senior Program Manager

assigned to the USNCB. Investigative personnel are also detailed from: Bureau of Alcohol, Tobacco, and Firearms (ATF); Drug Enforcement Administration (DEA); Federal Bureau of Investigation (FBI); U.S. Food and Drug Administration (FDA); Immigration and Customs Enforcement (ICE); Department of Defense/Counter Intelligence Field Activity (DoD/CIFA); Environmental Protection Agency (EPA); U.S. Mint (USM); U.S. Department of State (DOS/Office of Diplomatic Security); Internal Revenue Service (IRS); U.S. Marshals Service (USMS); U.S. Postal Inspection Service (USPIS); U.S. Secret Service (USSS); and various State police agencies.

(e) USNCB Divisions. Special agents from participating agencies are assigned to duty in one of four INTERPOL-USNCB Investigative Divisions. The divisions correspond to the types of criminal cases typically conducted under the statutory authority of the respective member agencies staffing the USNCB. The four INTERPOL-USNCB divisions are: Alien/Fugitive, Criminal, Drugs, and Financial Fraud. The CBP representatives are assigned in the Alien/Fugitive division.

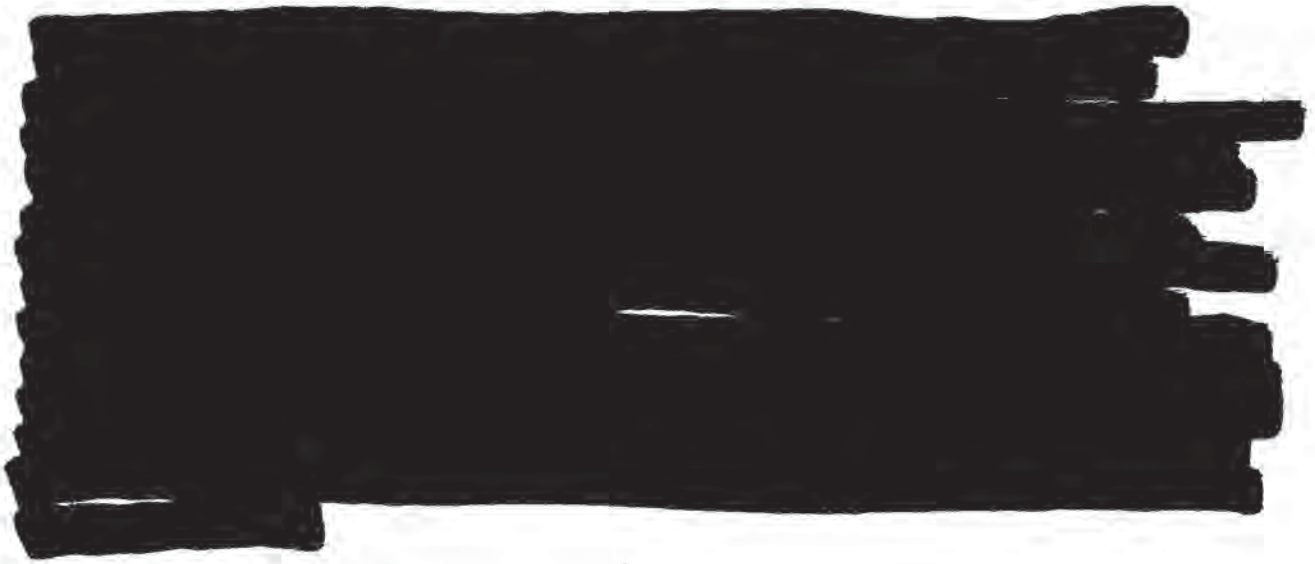
The USNCB-INTERPOL organizational scheme is intentionally broad. By nature, many foreign and domestic inquires have overlapping areas of investigative interest. Requests for investigative assistance received by the USNCB cover a wide range of offenses - from murder and violent crimes, narcotics and robbery violations, large-scale economic fraud and counterfeiting, to the location and apprehension of international fugitives and immigration-related offenses, such as document and visa fraud, and human smuggling.

Some limitations exist, however: Article 3 of the INTERPOL Constitution states, "It is strictly forbidden for the Organization to undertake any activities of a political, military, religious, or racial character." Requests for information placed through INTERPOL are thus evaluated against an agreed standard of operation. Similarly, member countries restrict processing requests to areas of investigative interest, which are recognized violations of their criminal statutes.

(f) CBP Requests Via Interpol. The USNCB's statistics reflect that CBP has consistently made the greatest number of requests among participating U.S. agencies using INTERPOL's communication channels to conduct foreign inquiries. This occurs for good reason, as CBP officers routinely encounter foreign nationals in the course of their assignments. Many of these foreign nationals will either have violated their immigration status, be unlawfully seeking entry or some benefit under the INA, or are under investigation by law enforcement agencies for other reasons.

The USNCB facilitates CBP requests for foreign criminal histories, records of conviction and outstanding warrants, and assists in the positive identification of foreign nationals, as well as procurement of travel documents. In addition,
INTERPOL has recently provided its cache of fingerprints to US-VISIT, which will in turn

lead to more interdictions of transnational criminals at our ports of entry. Often, the USNCB is the sole means available to CBP officers to obtain the information required to proceed in pending criminal or administrative investigations. CBP officers are encouraged to take advantage of the facilities available to them through the USNCB.



The INTERPOL - USNCB is accessible 24 hours a day/seven-days-a-week, by telecommunications (via NLETS and JUST), telefax, letter, DHS e-Mail, and telephone.

Communications references are listed below. When requesting or providing information, please follow the guidance listed below.

Plainly state the reason for your request (e.g., TECS/US-VISIT Hits, criminal investigation, unlawful application for benefits, visa/passport fraud), and indicate where you want your inquiry directed (i.e., to which countries).

Refer to the INTERPOL -USNCB case file number assigned, if applicable, to your inquiry, as this is the method by which INTERPOL matters are referenced.

Provide CBP file references (alien file number, I-94 admission number, naturalization number, etc.) and provide the following information, if known, for each subject of inquiry: name, aka(s), D/POB, COB, passport number, country of issue, visa information, last foreign residence, and parent names, together with any additional lead information which would assist foreign police in responding.

Telephone contacts - identify yourself as a CBP officer and ask for the CBP - INTERPOL representative (your request will be processed whether or not CBP representatives are available).

Please note that countries receiving requests for information typically request fingerprints and photos to assist in confirming a subject's identity and the record information they provide. Information supplied by member countries for individuals in the absence of fingerprints is subject to caveat.

Please note that your request for information will likely require your office to provide a disposition in the matter for forwarding to the responding country (e.g., deportation information, U.S. criminal convictions, etc.). Failure to reciprocate with the responding countries severely jeopardizes future CBP requests.

(g) INTERPOL Communications.

- Telephone: (202) 616-9000
- Telefax: (202) 616-8400
- NLETS address: DCINTEROO
- JUST address: JIPOL
- CBP e-Mail address: [redacted]

Mailing Address: INTERPOL- USNCB
U.S. Department of Justice
1301 New York Ave. N.W., 3rd Floor
Washington, DC 20530

# Chapter 33: Multi-Agency Automated Systems (Added INS - TM2)

33.1 Interagency Border Inspection System (IBIS)
33.2 National Crime Information Center (NCIC)
33.3 National Law Enforcement Telecommunications System, Inc. (NLETS)
33.4 The California Law Enforcement Telecommunication System (CLETS)

## 33.1 Interagency Border Inspection System (IBIS). (Revised by CBP 3-04)

(a) Background. The Interagency Border Inspection System (IBIS), a multi-agency database of lookout information, was initiated in 1989 to improve border enforcement and facilitate inspection of individuals applying for admission to the United States at ports-of-entry and preinspection facilities. The IBIS initiative began in response to both legislative and administrative mandates, as well as to evolving agency needs for a more efficient primary inspection at land, air and sea ports-of-entry.

IBIS resides on the Treasury Enforcement Communication Systems (TECS) at the CBP Data Center. Field level access is provided by an IBIS network with more than 24,000 computer terminals located at air, land, and sea ports of entry. A portable system using CD ROM drives is referred to as the Portable Automated Lookout System (PALS) and is discussed in Chapter 31.4(b).

IBIS provides the law enforcement community with access to computer-based enforcement files of common interest. IBIS contains information on suspect individuals, businesses, vehicles, aircraft, and vessels. It also provides access to the FBI's National Criminal Information Center (NCIC) and allows its users to interface with all fifty states via the National Law Enforcement Telecommunications Systems (NLETS). NCIC access includes records on wanted persons, stolen vehicles, license information, criminal histories, and previous Federal inspections.

CBP also has the authority to collect passenger name record information on all travelers entering or leaving the United States. This information is strictly used for preventing and combating terrorism and serious criminal offenses, with the principal purpose of facilitating CBP's mission to protect the borders through threat analysis to identify and interdict persons who have committed or may potentially commit a terrorist act.

In addition to CBP, law enforcement and regulatory personnel from 20 other federal agencies or bureaus use IBIS, including the FBI, Interpol, DEA, ATF, IRS, the Coast Guard, FAA, and Secret Service, among others. [See MOU in Appendix 33-1.]

Because of the multi-agency participation, as well as the system requirements to

provide, in addition to its basic lookout capability, a wide range of other special user requirements such as intelligence, investigative and other law enforcement activities, IBIS has evolved to provide a wide range of special features, including:

- Imagery
- Electronic Mail
- On-line Help
- Query Notifications
- Commercial Directories
- Primary Query History
- On-Line User Manual
- Machine-Readable Documents
- Biometric ID Technology

(b) IBIS Policy. Data in IBIS is "Law Enforcement Sensitive." Access to data is granted on a need-to-know basis for official use only. All IBIS users must be certified through an on-line security certification test and must be certified every two years. Abuse of misuse of IBIS could result in loss of access, termination of employment, and may include criminal prosecution.

(1) The restrictions in the use of IBIS are as follows:
Never leave your terminal unattended. If you must step away, log off completely.

(A) Do not leave IBIS materials unattended in unprotected places.
(B) Ensure that IBIS printouts are secured or destroyed.
(C) Never confirm or deny the existence of an IBIS record to the public or unauthorized user. This includes oral, handwritten and printout information.
(D) Only use IBIS to perform official duties required by your job. Browsing is not permitted. Never access IBIS information out of curiosity. Do not query your friends or members of your family.
(E) Information released outside of DHS must be accompanied by a Customs Form 191 (CF 191) and must be approved by a supervisor. Mark IBIS information "Law Enforcement Sensitive" when releasing to an authorized use outside of DHS.
(F) Do not disclose your password.
(G) Do not store IBIS information or records on the hard drive.
(H) If any IBIS data is stored on diskettes, label diskettes with "Law Enforcement Sensitive" and secure the diskettes while not in use.
(I) Report violations to your supervisor or to the Office of the Inspector General (OIG).

(2) Policy regarding IBIS equipment at a POE is as follows:

(A) POE and field office technical support staff will follow the guidelines outlined in memorandum entitled "IBIS Technical Support Guidelines at POE's" dated March 2, 2001.

(B) Internet access at a POE is to be restricted to one or two workstations that do not have access to IBIS. Designated Internet access workstations should be labeled appropriately, including a warning not to configure or provide access to IBIS from these workstations. All workstations at a POE, where practical, are required to have access to the intranet. Only approved browser software is permitted on designated internet workstations.

(C) All workstations' Virtual Terminal Access Module (VTAM) identification (ID) addresses and Internet Protocol (IP) addresses will be statically assigned and coordinated with IBIS personnel prior to installation or changes.

(c) Planned IBIS Enhancements. [reserved]

(d) Availability of IBIS training. PHOENIX is the computer-based training system which resides on the TECS mainframe computer. It is used to administer self-guided specialized training to field users. All TECS/IBIS users have the capability of accessing PHOENIX and taking courses offered. Many of the TECS/IBIS courses are optional. However, if you are a TECS/IBIS user, you must take the TECS Security Certification Test and, if you are an NCIC/NLETS user, you must take the NCIC Certification test. Your local Systems Control Officer has been issued a manual which will show you how to access and use the PHOENIX system. Additionally, a training region of the mainframe applications is available to simulate real-time events at ports-of-entry.

(e) Procedures for Computer System Failures

This section clarifies and documents the standard operating procedures to be followed in circumstances where the primary system, Interagency Border Inspection System (IBIS) becomes unavailable at ports of entry (POEs). All officers performing inspectional duties are required to be proficient with IBIS, to include the Advance Passenger Information System (APIS), and all other systems available, e.g., National Automated Immigration Lookout System (NAILS) and Portable Automated Lookout System (PALS), which support the inspectional process. These procedures must be followed in sequential order when access to the IBIS database is unavailable.

All system problems and outages must be reported to the Customs and Border Protection (CBP) Help Desk at [redacted]

(1) IBIS/APIS Failure at Air Ports of Entries (POEs):

If IBIS/APIS becomes unavailable at an individual air POE, inspectors must query all arriving passengers in NAILS. Directors, Field Operations (or Port Directors) should

ensure that all officers performing inspectional duties have access to NAILS and are proficient in the use of NAILS. If for any reason APIS is unavailable, port managers should obtain the APIS manifest and the "short list" (this list will consist of all primary, secondary and National Crime Information Center (NCIC) possible matches) of possible APIS matches for these arriving flights. [redacted] Regardless of the manner in which the APIS information is received, officers conducting inspections must confirm that each passenger's APIS data is complete and accurate. If the data is not complete and accurate, the data must be modified and queried through the available systems.

(2) IBIS and NAILS Failures at Air POEs:

In situations where both IBIS and NAILS become unavailable, inspectors must query arriving passengers in PALS. Ports are directed to immediately identify how PALS can be made accessible, either by the local area network or on stand-alone computers. Steps must be in place so that PALS may be accessed rapidly and correctly when required.

[redacted]

(3) IBIS Failure at Land POEs:

[redacted]

(4) IBIS and NAILS Failure at Land POEs:

[redacted]

[redacted]

(5) IBIS/APIS Failure at Sea (cruise or non-cruise) POEs:

[redacted]

## 33.2 National Crime Information Center (NCIC).

(a) General. The National Crime Information Center (NCIC) is a nationwide computerized information system established as a service to all criminal justice agencies--local, state, and federal. The goal of NCIC is to assist the criminal justice community in the performance of its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information readily available to as many criminal justice agencies as possible. For NCIC purposes, "criminal justice information" is defined as: "information collected by criminal justice agencies that is needed for the performance of their legally authorized, required function. This includes: wanted person information, stolen property information; criminal history information; information compiled in the course of investigation of crimes that are known or believed on reasonable grounds to have occurred, including information on identifiable individuals; and information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity."

General policy concerning the philosophy, concept, and operational principles of the system is based upon the recommendations of the NCIC Advisory Policy board to the Director of the FBI. The Board is composed of the top administrators from local, state, and Federal criminal justice agencies throughout the United States. Through Board input, changes in current file applications, the addition of new files, and new procedures (edits, codes, validations, etc.) are coordinated with all NCIC participants.

Through the use of computer equipment located at FBI Headquarters in Washington DC, the NCIC System stores vast amounts of criminal justice information which can be instantly retrieved and furnished through an NCIC terminal to any authorized agency. The NCIC data bank can best be described as a computerized index of documented criminal justice information concerning crimes and criminals of nationwide interest and a locator-type file for missing persons.

The NCIC serves criminal justice agencies in the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the US Virgin Islands and Canada.

(b) Use of NCIC information. The data stored in the NCIC is documented criminal justice information and this information must be protected to ensure correct, legal, and efficient dissemination and use. The individual receiving a request for criminal justice information must ensure that the person requesting the information is authorized to receive the data. The stored data in NCIC is sensitive and should be treated accordingly, and unauthorized request or receipt of NCIC material could result in criminal proceedings.

A Secondary Dissemination Log must be kept if a criminal report is ever given to a second party. If a criminal history report is requested, the attention field in the query is "filled in" with the requesting party. If the report is given to someone other than what was entered in the attention field, an entry in a secondary dissemination log must be entered providing the date, the name of the person to whom the report is given, signature and which criminal history was disseminated. A safe policy to adopt is to give a party just enough information to run the report themselves so that there is no need to maintain a dissemination log. But, just in case the day comes and a criminal history is given to someone other than the requesting party the log will be available and on site.

## 33.3 National Law Enforcement Telecommunications System, Inc. (NLETS).

The National Law Enforcement Telecommunications System, Inc. (NLETS) is made up of representatives of law enforcement agencies from each of the 50 states, District of Columbia, Puerto Rico and several Federal law enforcement agencies. The purpose of the organization is to provide for an improved interstate law enforcement and criminal justice communications system.

The NLETS system provides a communications link to law enforcement systems across the US, through a switching computer located in Phoenix, Arizona. NLETS queries may be made on state criminal history, vehicle registration, and drivers license information. Administrative messages are also supported.

NLETS is comprised of eight regions representing six or seven states that are grouped together to represent a regional community of interest. The Board of Directors meets at least once each year to conduct the organization's business. All policy decisions are made by the Board of Directors. The policy decisions range from how the system is to be operated to how the Corporation's general business will be handled. The offices phone number is (602)-224-0744.

Authorized INS personnel may access NLETS through IBIS.

## 33.4 The California Law Enforcement Telecommunication System (CLETS).

The California Law Enforcement Telecommunication System (CLETS) allows California IBIS

users direct access to California state motor vehicle information and other California criminal justice systems information.

# Chapter 34: Tools and Equipment (Added INS - TM2)


34.1 General
34.2 Firearms and Other Defensive Equipment
34.3 Ultraviolet and Infrared Viewing Equipment
34.4 Magnifying Devices
34.5 3-M Verification System Device
34.6 High-Intensity Light
34.7 Photophones
34.8 Machine-Readable Document Readers
34.9 CU-5 Camera Equipment
34.10 Admission Stamps and Security Ink
34.12 Government Vehicles
34.13 Audio-Visual Equipment


**References:**

AM 2.2.100, AM 1.5.215

## 34.1 General.

As an inspector, you will have available a wide variety of tools and equipment essential to the effective performance of your job. As new technologies are developed, you will have to continue to upgrade your inspectional skills to fully make use of them. Each new device which the Service purchases for use by its officers requires training in proper operation and maintenance. Much of this equipment requires special precautions to insure its security.

## 34.2 Firearms and Other Defensive Equipment.

(a) Firearms. There is one Servicewide policy relating to firearms. This policy encompasses a wide range of topics including such things as:

- authorization to carry weapons
- issuance and control of weapons
- use of firearms (deadly force policy)
- firearms training and qualification
- acquisition of firearms and ammunition
- reporting and investigating shooting incidents

The entire firearms policy is included as Appendix 34-1 of this manual. (IN99-24)[ See I-LINK

(b) Oleoresin Capsicum (OC) Spray Devices. Extreme caution shall be exercised in the use of OC spray, a form of less than lethal force, which immigration inspectors may have to use under certain circumstances. Authorization to be issued and to use OC devices shall be granted only to immigration officers, including immigration inspectors, who have received appropriate INS training and certification on the use, maintenance, and safeguarding of these devices. All OC spray devices made available to INS employees shall be INS-issued and shall be properly safeguarded at all times. If used, OC spray devices shall be utilized only after less invasive less than lethal use of force options have been considered and/or used. The use of OC spray devices shall be in conformity with policies and/or procedures established by INS governing their use.

(c) Batons. Immigration Inspectors may be authorized to carry one or more types of batons which may need to be used in specific instances while in the performance of official duties. Authorization to be issued and to use batons shall be granted only to immigration officers, including immigration inspectors, who have received appropriate INS training and certification in their use. All batons made available to INS employees shall be INS-issued and shall be properly safeguarded at all times. As an impact weapon and because its improper use can result in serious bodily injury and/or death, the decision to use a baton requires careful judgment. An affirmative decision to use a baton should be based on articulable facts which, if considered by any reasonable person, would support the use of this type of less than lethal force.

(d) Body Armor. The use of bullet-resistant body armor is a personal choice issue left to the discretion of individual immigration inspectors. While Inspections Program officers are not administratively mandated to use this type of equipment, the INS has nevertheless encouraged its use by making units of bullet-resistant body armor available to immigration inspectors on a funds-available basis. The INS is also evaluating the practicality and feasibility of including bullet-resistant body armor as an optional purchase item which uniformed INS officers can obtain under the INS Uniform Contract.

(e) Other Tools and Equipment. The INS will also consider making other equipment available to Inspections Program personnel on an as-needed basis. Examples of such equipment include, but are not limited to, flashlights, buoyant life preservers, and special purpose footwear.

## 34.3 Ultraviolet and Infrared Viewing Equipment.

## 34.8 Machine-Readable Document Readers.

I-LINK

A growing number of countries are now issuing machine-readable passports or visas. Most documents use an international standard established by the International Civil Aviation Organization (ICAO) and are readable by a standard electronic scanning device. In most locations, these devices are connected to the IBIS system. The reader serves to automate the lookout name query.

## 34.9 CU-5 Camera Equipment.

The CU-5 camera and accessories are used to make copies of documents for port records, for intelligence collection and for posting lookouts. The camera can also enlarge a document or fingerprint image. With the use of a filter, the camera can be used to examine glossy finishes. The camera can also be used to make 35mm slides for slide presentations.

## 34.10 Admission Stamps and Security Ink.

a) Admission Stamps

Historically the Service has permitted individual ports-of-entry (POE) to acquire and maintain inspector admission stamps. This policy and procedure has led to numerous versions and styles of admission stamps that are susceptible to fraud.

In May 2001, the Service replaced all admission stamps utilized by its inspection staff with a standardized admission stamp. Additionally, the Service centralized the issuance of replacement stamps, and provided for maintenance of the stamps. The design of the standardized admission stamp incorporates several security features.

These features are described in the Forensic Document Laboratory (FDL) Document Intelligence Alert #2001A-45 illustrated this new stamp design. For additional information pertaining to the new INS admission stamp contact the Intelligence staff at the FDL.

The Service has contracted with the vendor for the maintenance of the stamps. This includes the mechanical condition of the stamping unit (carrier) as well as the quality of the plate text and the digits within the rotating head. Admission stamps can be returned to the vendor for maintenance and/or replacement of the plate text, rotating dater or carrier. There is no expense to the Service for maintenance of the admission stamps (except for costs of shipping the stamp to the contractor). The shipping of stamps to the vendor for repair should be done through a mail system that permits tracking of the package (i.e., FEDEX, UPS, certified mail/return receipt). A brief memorandum that

includes the return mailing address and the point of contact must be included in the container used to ship the stamp to the vendor. The memorandum must also provide a description of what repairs are required or the reason for return.

b) Security Ink

All stamps used to endorse documents that show evidence of status or immigration benefits must use security ink. Examples include admission stamps, "temporary I-551" stamps, line stamps, I-95 stamps, parole stamps, voluntary departure stamps, refugee stamps and office 3-letter code stamps.

[redacted]

c) Control of Admission Stamps

1. Tracking.

A record of each Service admission/approval stamp must be kept on an individual Form G-570, Record Receipt-Property Issued to Employee, and maintained numerically according to the stamp number. The Form G-570 must be executed upon receipt of each new stamp by the office controlling the stamp.

2. Distribution:

In offices where stamps are procured centrally and distributed to more than one location, the office controlling the stamp, or the procurement/ordering official, must maintain either individually or by block of numbers a record indicating the controlling location and date of shipment. The receiving station must then create an individual Form G-570.

3. Tracking Requirements:

The Form G-570 for each stamp must contain the following information:

a) Stamp type and number

(e.g., line date NYC-1 or admission stamp NYC-1);

b) Date received at POE or controlling location;

c) Date issued to officer;

d) Receiving officers name, typed or printed, and signature;

e) Date returned to Property Custodian;

f) Date of destruction, loss, theft, or withdrawal from use, if any; and

g) Supervisor's name, typed or printed, and signature.

d) Lost, Stolen or Compromised Admission Stamps or other Secure Property

Every effort must be made to ensure that admission stamps and other secure property are guarded from being lost, stolen or compromised. Guidance on handling secure property can be found in Chapter 10 of the Security Officers Handbook. If an admission stamp or other secure property item --such as security ink or a pad-- is lost, stolen or compromised, it will be immediately reported orally to supervisory personnel, and reported in writing to supervisory personnel within 24 hours of the incident. Port Directors are responsible for ensuring that the actions in subparagraph "e" below, and in the Security Officers Handbook for reporting lost or stolen equipment, are initiated as expeditiously as possible. The Security Officers Handbook is available on INSERTS.

e) Preparation of Intelligence Report Concerning Loss, Theft, or Compromise of Secure Property

1. A Form G-392 Intelligence report on each incident involving a lost, stolen, compromised admission stamp, and stamps that have been permanently removed from use is to be prepared and routed to the Offices of Intelligence, Internal Audit, Investigations and the INS FDL within 24 hours of the detection of the loss, or theft, or the discovery of a compromised admission stamp or other secure property such as ink pads or security ink.

2. The INS FDL will maintain a listing of all lost, stolen, compromised stamps or stamps that have been permanently removed from use.

3. The report on a lost, stolen, or compromised admission stamp, or related security property, must include all pertinent data, such as the date, time, and place of the loss, theft, or the discovery of the compromised admission stamp, the name of the officer to whom the stamp was assigned, what efforts where made to recover the lost stamp, or the circumstances surrounding the discovery of the compromised stamp and any other pertinent facts relating to the incident.

## 34.12 Government Vehicles.

Inspectors may be assigned to use a govenrment vehicle (or they may use their privately owned vehicle) to perform inspections or inspections-related activities. Service polices governing vehicle use are included in AM 2.2.101 and the Personal Property Handbook (M-429).

## 34.13 Audio-Visual Equipment.

Some ports-of-entry use either tape recorders or video cameras to record certain activities such as sworn statements or secondary interrogations. Use of such equipment may provide evidence to support a case and may also be helpful to defend Service employees against allegations of improper conduct. Service policy governing use of audio-visual equipment is included in AM03.400.

# Chapter 41: Liaison Activities; Facilities (Added INS - TM2)

41.1 Liaison with Federal Inspection Agencies
41.2 International Border Liaison
41.3 Liaison with International Air and Sea Carriers and Foreign Governments
41.4 Liaison with Other Federal Agencies
41.5 Liaison with Port Authorities; Inspectional Facilities

**References:**

**INA:** Section 239.

**Regulations:** 8 CFR 239.

## 41.1 Liaison with Federal Inspection Agencies.

(a) General. Several Federal agencies share responsibility for inspection of international passengers and the items in their possession at the time of arrival. Besides INS, the Customs Service, Animal and Plant Health Inspection Service and Public Health Service all have responsibilities for the inspection of international travelers. These agencies are referred to collectively as the Federal Inspectional Services (FIS). In recent years, the roles of these agencies have evolved from each agency operating relatively independently to a more cooperative, joint effort. This joint effort has resulted in more efficient and effective inspectional procedures. The Interagency Border Inspection System (IBIS) is a prime example of this cooperative effort.

(b) Port Quality Improvement Committees. In June and July of 1995, the Federal Inspection Services (FIS), consisting of the Immigration and Naturalization Service (INS), the United States Customs Service (USCS), the Animal and Plant Health Inspection Service (APHIS), and the Bureau of Consular Affairs of the Department of State (DOS), participated in a National Performance Review (NPR) Border Process Reengineering conference with a common purpose of reengineering the primary inspection process at air and land border Ports-of-Entry (POEs). Three teams convened to develop recommendations to improve efficiency, effectiveness, and cycle times of primary travelers and vehicle processing through integrated inspection processes at airports and at both land borders.

In the Fall of 1995, the Executive Oversight Committee, comprised of agency representatives at the Deputy Commissioner/Administrator level of each FIS, and the Senior Implementation Group , comprised of agency representatives from the national unions as well as executive level managers, were formed to monitor and evaluate the testing of BPR recommendations.

In January 1996, nine pilot sites were selected to further test the NPR recommendations and five additional sites were identified shortly thereafter. A total of eight airport and six land border sites were chosen. In addition, Miami was designated a NPR Reinvention Lab.