Alagood, Robert Kyle

From: Malgor, Manuel C. [mcmalgor@mdpd.com]
Sent: Thursday, March 01, 2012 10:30 AM
To: Alagood, Robert Kyle
Cc: Varela, Margarita J.
Subject: MDPD Homeland Security SOP
Attachments: HSB SOP (redactedl).pdf

Good morning Mr. Alagood,

Attached is our (Homeland Security Bureau) SOP. I apologize for the delay but we had to run it by our chain of command and our Legal Bureau. I hope you find the information you are looking for. If I can be of any further assistance feel free to contact me.

Manuel Malgor, Sergeant
Miami-Dade Police Department
Homeland Security Bureau
9105 NW 25 Street
Miami, FL 33172
305.470.3908 - Office
mmalgor@mdpd.com
"Delivering Excellence Everyday"

MIAMI-DADE POLICE DEPARTMENT
Homeland Security Bureau

Standard Operating Procedure (SOP)

The **Miami-Dade Police Department's Homeland Security Bureau** is a Fusion Center herein referenced to as Homeland Security Bureau (HSB) or Southeast Florida Fusion Center (SEFFC). Our goal is to address the Miami-Dade Police Department's (MDPD) continuously growing homeland security initiatives through the below mission statement.

Mission Statement: To gather and analyze information in furtherance of disseminating criminal intelligence products within the Department, as well as to local, state and federal partners in an effort to identify and track homeland security and terrorism related activities and crimes; and to provide situational awareness in civic activities to include labor or community causes that may compromise the public safety of the citizens of Miami-Dade County (MDC).

The HSB/SEFFC reports directly to the MDPD Director.

The HSB/SEFFC is divided into three investigative components, the Intelligence Section, the Infrastructure Protection Section and the Operations Coordination Section, in conjunction with the Southeast Regional Domestic Security Task Force (SERDSTF) and the Department of Emergency Management.

The purpose of this SOP is to guide HSB/SEFFC employees in the accomplishment of their daily goals and responsibilities, in augmentation of the Departmental SOP.

All Bureau personnel will become familiar with the procedures established herein and acknowledge acceptance and agreement to the HSB/SEFFC Security and Nondisclosure Policy, via their signature on an acknowledgment log.

All procedures and mandates outlined herein have the force of departmental policies and/or rules. Any conflicts with federal or state law, MDC regulations, or the Department Manual (DM) will be resolved in favor of the higher authority. Any conflicts contained herein, which is adjudged to be illegal, incorrect or inapplicable shall not affect the validity of the remaining content. It is the responsibility of the revealing party to bring any conflict to the HSB/SEFFC Major's attention, via their respective Chain of Command.

APPROVED BY:

_____ _____
Glenn Stolzenberg, Major — Date
Homeland Security Bureau

_____ _____
James K. Loftus, Director — Date
Miami-Dade Police Department

TABLE OF CONTENTS

Page(s)

TABLE OF CONTENTS

Page(s)

TABLE OF CONTENTS

Page(s)

SECTION A – MAJOR'S OFFICE

BACKGROUND: The complex nature of the activities of the HSB/SEFFC requires written procedures to ensure proper management of assigned personnel and their activities.

ACTION: Standard Operating Procedures, which set forth Bureau methods, have been prepared. The contents enumerate those procedures, which are unique to the Bureau and used for accomplishing routine and recurring actions. New procedures and changes to existing procedures will be documented in this SOP annually.

OPERATIONS OVERVIEW: The HSB/SEFFC has the primary responsibility of coordinating, monitoring and overseeing all homeland security related incidents within the Miami-Dade Police Department's (MDPD) jurisdiction. In addition, the HSB/SEFFC is responsible for initiating proactive homeland security related investigations and may assume control of any MDPD correlating incident, as it deems appropriate.

SEFFC was initiated in response to the increase need for timely information sharing and exchange of crime related information among members of the law enforcement community. One component of HSB/SEFFC focuses on the development and exchange of criminal intelligence. This component focuses on the criminal intelligence process where information is collected, integrated, evaluated, analyzed and disseminated. The Mission of the HSB/SEFFC is to enhance partnerships, which foster a connection between every facet of the law enforcement community. HSB/SEFFC will afford the men and women, who are dedicated to protecting the public and addressing violence, with all available intelligence resources and communications capabilities. Unless readily shared, critical information is without value.

The HSB/SEFFC is also charged with maintaining communication, and/or cooperative liaison regarding subversive, militia and extremist activities, as well as civic, labor and community activist/causes that may adversely impact the safety of the citizens of Miami-Dade County (MDC) and/or result in civil disorder.

In furtherance of our domestic security mission, the HSB/SEFFC is also assigned to identify MDC's critical infrastructures and key resources, and initiate or recommend vulnerability assessments, where appropriate, maintain liaisons with the public and private sectors, and promotes the Department's Homeland Security Awareness Campaign.

Lastly, while the Bureau's primary jurisdictional responsibility is the unincorporated areas of MDC; HSB/SEFFC personnel provide homeland security and criminal intelligence gathering and dissemination assistance to law enforcement agencies at the local, regional, state, federal and international levels.

REVOCATION: HSB/SEFFC Standard Operating Procedure dated, 2010.

EFFECTIVE DATE: As reflected on Authentication Page.

JOB DESCRIPTIONS

The below job descriptions detail general responsibilities as listed and/or as outlined by the Miami-Dade County Employee Relations Department Job Descriptions listings. Additional responsibilities for each classification are listed under their corresponding area of assignment.

MAJOR

Illustrative Tasks:

Direct, through subordinates, the work of homeland security initiatives, criminal intelligence, police operations, including the pursuit, apprehension and arrest of law violators. Serve as the departmental liaison to the Department's Homeland Security Coordinator, and is a panel and voting member of the Urban Area Security Initiative (UASI) and Urban Area Work Group (UAWG) of matters on behalf of the Department's interests. Liaison with federal, state and local law enforcement partners as well as the Joint Terrorism Task Force (JTTF) and Field Intelligence Group (FIG) of the Federal Bureau of Investigation (FBI) to address homeland security concerns. Reviews and evaluates reports prepared by subordinates and ensures that departmental orders and procedures are being followed within the HSB in accordance with the Departmental Manual. Directs and coordinates the activities of HSB/SEFFC the use of enforcement and administrative processes; reviews established goals and objectives and monitors achievements. Reviews and evaluates the development of the Homeland Security Bureau policy and procedures and ensures the bureau is operated in full compliance with all applicable laws and statutory mandates for Miami-Dade County and State of Florida. Prepares and submits preliminary budget estimates; reviews requisitions for supplies and equipment; evaluates subordinate staff and recommends reassignment, training and disciplinary actions within unit of assignment. Presents oral reports on crime statistics and deploys resources of the Department to impact reductions. Reports to the Office of the Director and performs related work as required; inclusive of relaying all homeland security and important Bureau matters.

CAPTAIN

Illustrative Tasks:

Plans, assigns, and reviews homeland security related work, which includes criminal investigations and intelligence, responds to letters from the public, reviews reports prepared by subordinates, ensure that subordinates are complying with issued orders and directives.

Commands major offense sections of the HSB/SEFFC; responsible for homeland security related investigations, which occur within numerous municipalities. Cooperates with municipal law enforcement agencies in suppressing criminal activities and apprehending suspected offenders.

CAPTAIN (Continued)

Conducts operational inspections of the HSB/SEFFC; reviews compliance with departmental regulations and policies; submits recommendations for the modification of existing orders, operational plans and the development of new procedures for all phases of public safety. Reviews reports prepared by subordinate officers; recommends techniques for special investigations; makes recommendations for changes in procedures or policies to increase effectiveness. Prepares and submits preliminary budget estimates; reviews requisitions for supplies and equipment; evaluates subordinate staff and recommends promotion, reassignment, training and disciplinary actions within unit of assignment; work consistent with organizational placement is performed as required. Serves as executive officer of the Bureau; coordinates the activities of lieutenants; ensures Bureau administrative functions are carried out consistent with policy and procedure. Coordinates the activities of elements involved in the training function; such as in-service, out-service, firearms, specialized and others. Supervises a major element involved in investigation of organized criminal activity or intelligence. Responsible for investigation of employee misconduct or investigation of criminal offenses by departmental members. Performs related work as required.

POLICE LIEUTENANT

Illustrative Tasks:

Plans, assigns, and reviews the work of a shift of police officers and sergeants, organized into groups of squads, and engaged in various law enforcement and crime prevention activities and other investigations of alleged criminal activities. Supervises and participates in a variety of special criminal investigative units or specialized support activities, including staff training and criminal intelligence investigations. Conducts roll call and inspects personal appearance and their equipment; determines courses of action to be taken during shift, emergencies or complex law enforcement situations; discusses activities in area of assignment with subordinate supervisors and provides assistance to subordinates. Reviews a variety of reports, correspondence, memoranda and files prepared by subordinates and other departmental personnel for adequacy and completeness, to comply with departmental directives, ascertain trends, detect unusual cases, determine cases to be investigated and identify problem areas.

Prepares various correspondence and statistical reports, studies and budgets to present findings, provide information, justify and project needs, recommend solutions and document work activities, equipment utilization and operations. Receives verbal and written complaints and inquiries from the public, media, other government agencies and department personnel and provides information on departmental regulations and procedures, explains courses of action that will or have taken place, and refers complaints to other departmental authorities. Accounts for all equipment, materials, supplies and vehicles assigned to the specific operating unit to ensure proper inventory levels and operational readiness.

POLICE LIEUTENANT (Continued)

Performs duties of superior in order to provide continuity of operations, as necessary. Attends various departmental and non-departmental meetings and training courses; reads materials pertinent to the law enforcement field to keep abreast of current developments; identifies training needs, prepares lesson plans and conducts formal training sessions. Testifies in court, before grand juries, and hearings concerning police activities, to provide information from evidence gained through investigations and assist in case prosecutions. Makes recommendations regarding hiring, discipline and promotion of subordinates; authorizes leave and overtime; reviews performance reports prepared by subordinates and rates employee performance. Performs related work as required.

POLICE SERGEANT

Illustrative Tasks:

Plans, assigns, and reviews the work of a squad of subordinate police officers engaged in a variety of law enforcement activities, such as criminal and intelligence investigations; determines proper course of action to be taken in day-to-day activities, emergencies or complex law enforcement situations. Conducts roll call, inspects subordinate's personal appearance and their equipment, makes work and equipment assignments, conducts informal training sessions, discusses activities in area of assignment. Accounts for all equipment, materials, supplies and vehicles assigned to the specific operating unit to ensure proper inventory levels and operational readiness. Assists subordinates with the performance of duties in order to supplement the staff accordingly, to enforce laws and ordinances and make arrests; acts in the absence of superiors as required to provide continuity of operations. Reviews a variety of reports prepared by subordinates and other departmental personnel for adequacy and completeness, in order to comply with departmental directives, ascertain trends, detect unusual cases and identify problem areas. Prepares various operational and administrative documents, as well as statistical reports, to present findings, recommend solutions, provide information, and document work activities. Additionally, identifies specific actions to be taken to address investigative operations. Receives verbal and written complaints and inquiries from the public and other government agencies and provides information on departmental regulations and procedures, explains courses of action that will or have taken place, and refers complaints to other departmental authorities. Investigates individuals involved in alleged crimes; gathers information and evidence, makes arrests, provides police protection and determines if criminal activities are or have taken place.

Interviews or interrogates witnesses, informants, suspects, prisoners and others to obtain and gather information and to determine the nature and extent of individual involvement with specific criminal activities. Testifies in court, before grand juries and hearings concerning police activities, to provide information from evidence gained through investigations and assist in case prosecutions. Attends various training courses and reads materials pertinent to the law enforcement field to keep abreast of current

POLICE SERGEANT (Continued)

developments; identifies training needs, prepares lesson plans and conducts formal training sessions.

Makes verbal presentations to schools, the media, community groups and other organizations to improve the public awareness of police activities. Makes recommendations regarding hiring, discipline and promotion of subordinates; authorizes leave and overtime; evaluates and rates employee performance. Performs related work as required.

POLICE OFFICERS (Detectives)

Illustrative Tasks:

Investigates criminal activities related to the HSB within the unincorporated area of MDC. Testify in court concerning work activities. Serves criminal court orders, conducts search and surveillance to determine whereabouts of person to be served, arrests fugitives and returns person to proper authority. Assists in departmental programs and cooperates with other agencies in matters related to homeland security; threat, criticality and vulnerability assessments and various criminal intelligence investigations. Participate in undercover surveillance, civil defense exercises, rescue operations, and criminal intelligence collection. Assist in the presentation of departmental training programs. Perform related work as required.

INTELLIGENCE ANALYST SUPERVISOR (IAS)

Illustrative Tasks:

Responsibilities include supervising and coordinating specific operational law enforcement activities inclusive of investigative, tactical, and specialized analytical activities. Monitor the progress of assignments and give guidance on the completion of analytical projects, as well as evaluate the quality and resourcefulness of investigative tools used for the desired results. Review and assess all requests for assistance and make appropriate assignments to ensure accuracy. Provide research and technical expertise on complex criminal and financial investigations. Attend meetings and act as the Bureau's liaison with other investigative support entities. Perform related work as required.

POLICE FINANCIAL INVESTIGATOR (PFI)

Illustrative Tasks:

Examine confiscated wagering and related financial records, including tax returns. Establishes gross sales and net profits of persons arrested to determine amount of fine

POLICE FINANCIAL INVESTIGATOR (PFI) (Continued)

recommended, provide information to the Internal Revenue Service (IRS) when violations of tax and wagering laws are uncovered, determine possible relationships with other cases, and determine if illegal profits were used to purchase assets, which are subject to seizure. Examines police records to determine expenses incurred during investigations. Testify in court proceedings, pre-trial conferences, and depositions as an expert witness. Examines financial records provided by the MDPD, Legal Bureau to determine the disposition of funds seized during narcotics investigations. Examine tax and business records of employees under investigation by the IRS. Provide interviews for the media. Perform related work as required.

INTELLIGENCE ANALYST (IA)

Illustrative Tasks:

Reviews, extracts, and analyzes reports and other information and compiles data into logical form to provide general or specific intelligence for use in investigative and planning decisions. Reviews data from various reports and graphically links specific intelligence information relating to association of individuals and establishments by developing charts and graphs; graphically charts specific events obtained from data to provide chronological presentations. Analyze financial data from various reports to provide specific accounting information to be used in conducting investigations. Exchanges intelligence information with other law enforcement partners to complete projects assigned; assists investigative personnel in special projects by conducting the necessary research in agency files, obtaining corporate records or other information. Keep abreast of significant organized crime activity within the jurisdiction of the Department, Bureau, and nearby areas by means of reviewing reports and media articles. Attends scheduled departmental meetings, as assigned, to present briefings or obtain pertinent information relating to investigations and planning. Perform related work as required.

POLICE CRIME ANALYST SPECIALIST 1 (PCAS 1)

Illustrative Tasks:

Reviews daily police reports concerning targeted crimes; including robbery, burglary, sexual battery, carrying concealed firearm, loitering and prowling, suspicious persons, vehicle, incident and information reports; identifies ad hoc and specific data elements and codes data for entry into automated files or for manual review and verifies entered data for accuracy.

Prepares information reports from automated, manual or feedback sources in an attempt to identify known criminal offenders who are active outside the geographical boundaries in which they live or work; responds to specific requests for assistance from investigative elements by searching for subject and/or vehicle descriptions, preparing

POLICE CRIME ANALYST SPECIALIST 1 (PCAS 1) (Continued)

association matrices, or charts, and appropriate investigative lead reports. Tracks targeted crimes such as burglaries, robberies, and sex offenses on pin/spot/overlay maps to accurately portray current geographical locations and time frames. Reviews daily field interview reports and identifies data elements; extracts report data and ensures entry into the district automated files using standardized formats and assures sufficient detail to permit collation and extrapolation of information pertinent to the users needs.

Prepares and disseminates bulletins to the appropriate user groups concerning each district's targeted crimes and provides interpretive information or notes special concerns as needs are identified or requested. Meets regularly with uniformed, investigative and other analytical personnel for the purpose of exchanging information or developing ad hoc reports; attends scheduled meetings with municipal investigative units for the dissemination and exchange of information. Monitors and ensures appropriate action is taken regarding habitual or career criminals as defined in Florida State Statutes through personal feedback or formalized follow-up mechanisms. Perform related work as required.

POLICE RECORDS SPECIALIST 1 (PRS 1)

Illustrative Tasks:

Operate a computer terminal to make inquiries, recoveries, modifications, cancellations and entries on wanted, missing/runaway subjects, articles, guns and securities, into local, state, and national criminal justice information systems for the MDPD and other municipal police agencies without computer terminals. Sends and receives messages from local, state, and Florida Crime Information Center (FCIC) terminals; verifies messages and bench warrants in the FCIC to other police agencies. Receives telephone calls from police officers; verifies information and enters data concerning stolen and recovered passenger vehicles, trucks, trailers, and other vehicles into computer terminals. Provides counter services to the public, processes correspondence, researches general records, files, and operates microfiche equipment. Assists jail booking personnel, via telephone, in the handling and processing of current arrests. Perform minor maintenance to computer terminals and microfilm readers. Maintains appropriate work records and logs. Perform related work as required.

DATA ENTRY SPECIALIST 1 (DES 1)

Illustrative Tasks:

Performs data entry including researching, verifying, and correcting information to be entered into a database; creates simple forms, formats, and or statistical charts; runs and prints reports, and performs disk backups.

DATA ENTRY SPECIALIST 1 (DES 1) (Continued)

Operates standard office equipment, such as personal computer, copy or facsimile machine, and calculator; screens telephone calls and refers caller to appropriate party or take telephone message; opens, sorts, and distributes mail; sorts and files correspondence, reports, or other materials. Processes documents requiring various procedural knowledge specific to area of assignment; reviews documents for sufficiency, obtains necessary signatures and routes appropriately, maintaining follow-up; provides information to other divisions and the public, applying significant knowledge of departmental rules, regulations and procedures to interpretations made; may supervise a small group of employees engaged in routine clerical duties. Perform related work as required.

ADMINISTRATIVE SECRETARY

Illustrative Tasks:

Performs secretarial and clerical duties for an executive official; commits supervisors' time in making appointments and maintains calendar; maintains supervisors itinerary and makes travel and hotel arrangements as required. Arranges for and attends various conferences and meetings; informs participants and provides background information; serves as recording secretary at conferences, board meetings and staff consultations; takes official minutes and prepares reports of proceedings; follows through on actions required as a result of conferences. Takes and transcribes dictation, which may vary by subject matter including legal, technical, financial or other specialized terminology; takes verbatim transcript from telephone calls or in conferences as requested. Opens, screens and distributes mail; marks important parts of instructions, orders and regulations for executive, and organizes mail according to priorities; maintains control of correspondence flow through office; insures that report deadlines are met and that all information distributed is complete. Composes correspondence from verbal instructions of superior, and independently drafts replies to inquiries; reviews correspondence prepared by others for superior's signature to ensure correct grammar, format and completeness. Receives and screens telephone calls and visitors; responds to requests for information by answering questions where there are established policies or regulations, or precedent actions taken by supervisor. Plans, assigns and reviews the work of subordinate clerical employees engaged in typing reports, correspondence and other documents, filing, and performing a variety of other clerical duties; provides training in procedures and methods in the organization of assignment.

Researches and compiles data from a variety of sources in connection with special reports, budget preparation and other matters; assembles material for supervisors reply to correspondence demanding superiors' personal attention. Keeps various activity and production records; types various activity reports, requisitions, work orders and personnel forms; composes reports on caseloads, workloads or other subjects as delegated; authorizes expenditures from petty cash; requisitions office supplies; performs arithmetic calculations for budget requests and other matters.

ADMINISTRATIVE SECRETARY (Continued)

Establishes and maintains office filing systems and reorganizes files as required; establishes subject matter files for superior; purges files of unnecessary items according to established policies and procedures. Makes recommendations regarding hiring, discipline and promotion of subordinates; authorizes leave and overtime; evaluates and rates employee performance. Perform related work as required.

SECTION SECRETARY

Illustrative Tasks:

Performs advanced secretarial duties for an administrator who is located organizationally directly underneath the Major; makes appointments and maintains calendar; arranges for conferences and meetings; attends meetings and conferences taking minutes or summary notes. Opens and distributes mail; maintains control of correspondence flow through section and assures that response deadlines are met; composes correspondence or selects standardized formats; prepares a variety of reports, correspondence, documents, forms, and requisitions. Receives visitors and screens telephone callers; acts as receptionist and answers requests for information involving department, division or section activities and established policies and procedures. Operates word processing, micro-computer or advanced typewriting equipment to prepare and create report, generate correspondence or other documents, and complete forms, requisitions and other similar standardized records. Assigns and reviews the work of subordinate clerical employees engaged in typing, filing, and other clerical activities; provides advice and assistance as questions arise concerning work tasks and section procedures. Retrieves and assembles material from files; authorizes expenditures from petty cash funds; requisitions office supplies; performs arithmetic calculations as needed. Takes and transcribes dictation as required, involving technical or specialized terminology. Perform related work as required.

ORGANIZATION

The HSB/SEFFC is divided into four operational sections commanded by the Bureau captain under the office of the major. Each section carries clearly defined areas of responsibilities and individual subsections as follows:

1. **OPERATIONS COORDINATION SECTION**
   A. Intelligence Operations Center
   B. Administrative Operations and Support Unit

2. **INTELLIGENCE SECTION**
   A. Intelligence Squad 1
   B. Intelligence Squad 2
   C. Technical Operations Unit

ORGANIZATION (Continued)

3. **INFRASTRUCTURE PROTECTION SECTION**
   A. Infrastructure Protection Squad 1
   B. Infrastructure Protection Squad 2
   C. Special Projects Squad

4. **SOUTHEAST REGIONAL DOMESTIC TASK FORCE**

5. **DEPARTMENT OF EMERGENCY MANAGEMENT**

MAJOR'S OFFICE OVERVIEW

Major's Office

A. Major
B. Captain

A. The Major reports directly to the Office of the Director. In addition to the previously described job illustration, the Major will report intelligence information and homeland security-related issues, which directly impacts the Department or community to the Director as required [CALEA 43.1.7]. The Major has the responsibility to command, coordinate, direct and control all activities of the Bureau. He reviews work productivity for evaluation and improvement, and initiates all memoranda emanating from the Bureau.

The Major maintains the efficiency, productivity, welfare, and discipline directing of subordinates and maintaining a constant evaluation of community concerns and directs subordinate personnel in effective manpower distribution.

The Major reports to the Director who is the departmental Homeland Security Coordinator (HSC) and shall serve as the departmental liaison with all MDC departments, as well as local, state and federal agencies dealing with terrorist and homeland security matters. The HSC shall also coordinate with MDPD entities on strengthening the domestic security measures of the Department, which include prevention, preparedness, protection, response and recovery capabilities.

CAPTAIN'S OFFICE OVERVIEW

B. The HSB/SEFFC captain commands the Bureau's daily function, reports directly to the Bureau Major and is responsible for the command and control of the Bureau's four investigative sections, Infrastructure Protection, Intelligence, Operations Coordination, and Southeast Regional Domestic Task Force.

SECTION B – BUREAU ADMINISTRATION

SECURITY AND NONDISCLOSURE AGREEMENT

In consideration of being granted access to certain sensitive information, all personnel assigned to the HSB/SEFFC are bound and must hereby accept the obligation contained herein.

Sensitive Information includes:

- Active Criminal Intelligence - Information that relates to an identifiable person or group of persons collected in an effort to anticipate, prevent, or monitor possible criminal activity.

- Active Criminal Investigation - Information gathered by a criminal justice agency in the course of conducting an investigation of a specific act or omission.

- Law Enforcement Sensitive - Information that could adversely affect on-going investigations, create safety hazards for officers, divulge sources of information, and or compromise their identities.

- For Official Use Only - or sensitive but unclassified – Information, which warrants a degree of protection and administrative control.

HSB/SEFFC personnel acknowledge and understand that their assignment to the HSB/SEFFC places them in a position of special confidence and trust.

HSB/SEFFC personnel acknowledge and understand that any and all information is considered sensitive and that they have been given a briefing on the need for maintaining the security of such sensitive information, and the procedures to be followed in any authorized release or dissemination of such information.

HSB/SEFFC personnel acknowledge and understand that the unauthorized disclosure to unauthorized personnel or the negligent handling of sensitive information could jeopardize sources of information, damage or irreparably injure ongoing or future investigations or place persons at risk.

Accordingly, HSB/SEFFC personnel agree that they will not disclose, publish, release, transfer, copy (whole or in part), or otherwise make available any information obtained in the scope of their HSB/SEFFC function, except as provided by in this agreement, and will keep all relevant information made available in confidence and prevent its unauthorized disclosure.

HSB/SEFFC personnel acknowledge and understand that they will only release sensitive information to bona fide law enforcement/criminal justice personnel with an established NEED and RIGHT to know the information and to such other persons, as directed by an authorized HSB/SEFFC supervisor. An authorized HSB/SEFFC supervisor is defined as a lieutenant or higher within the HSB/SEFFC.

SECURITY AND NONDISCLOSURE AGREEMENT (Continued)

This restriction does not apply to information that was in the public domain at the time it was disclosed, or that is disclosed pursuant to the provisions of a court order.

However, HSB/SEFFC personnel acknowledge that any information obtained from the public domain will not be disseminated if in its dissemination, relevant and sensitive information regarding a criminal or intelligence investigation maybe compromised or plans pertaining to the mobilization, deployment, or tactical operations involved in responding to emergencies.

HSB/SEFFC personnel acknowledge and understand that any other unauthorized dissemination of HSB/SEFFC sensitive information is prohibited and understand that if they are uncertain as to the appropriateness of a particular release of information, they must first confirm that the release is proper with their immediate supervisor (acting supervisors are not authorized to permit release for this provision).

HSB/SEFFC personnel acknowledge and understand that any unauthorized release of sensitive information may result in their HSB/SEFFC assignment removal, as well as possible disciplinary action. In addition, any unauthorized release of sensitive information may result in criminal prosecution under applicable law.

HSB/SEFFC personnel acknowledge and understand that all conditions and obligations under this agreement are binding throughout their participation with the HSB/SEFFC and at all times thereafter, unless otherwise confirmed in writing by a HSB/SEFFC supervisor.

OFFICE SECURITY PROCEDURES

The HSB/SEFFC carries security procedures [redacted]. All HSB/SEFFC personnel and visitors must adhere to the below procedures, without exception.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

SYSTEM/FILE SECURITY [CALEA 43.1.2]

Administrative and Security Issues

Security of the systems is the responsibility of the Bureau's Designated Security Officer (Intelligence Section Lieutenant) in collaboration with an IOC sergeant to prevent unauthorized access to the information.

The Bureau Security Officer will oversee a process for audit and inspection of backup documentation supporting participating agency submittals to the database. This process can be conducted by mail, utilizing a random sample of submittals and requesting the participating agency head certify compliance of the entry.

In order to protect the integrity of the system, access, modifications, removal, and retrieval of information will be limited to individuals who:

- Have signed a MDPD HSB/SEFFC, SERDSTF - 7 User's Agreement and Access Control for Use of the Secure Work Space and HSDN
- And whose clearance has been verified by the Bureau Security Officer in concert with DHS

All correspondence, briefs and reports prepared or obtained by Bureau personnel will be stored within areas or containers designated by the Bureau Security Officer. Release and/or destruction of material will be done following the appropriate records retention schedule.

All classified, sensitive or official use documents will only be discarded after being approved by the Bureau Security Officer, via one of the Bureau's shredders or incineration. Personnel must remain cognizant of their respective assignment and the sensitive nature of the material being handled or processed and follow all applicable local, state and federal laws/guidelines.

[redacted]

BUREAU ADMINISTRATIVE PROCEDURES

The following administrative procedures have been instituted to ensure that the Bureau complies with departmental procedures and applies to all Bureau personnel. It should be noted that, with the exception of headers, any text that is bolded would be a direct reference to the **DM.**

BUREAU CORRESPONDENCE

- All correspondence prepared for distribution outside of the Bureau will be prepared under the Major's name unless otherwise directed.

- Correspondence for the Major's signature will be routed to the Administrative Secretary for forwarding to the Captain, prior to the Major's final review and approval.

TRAVEL PROCEDURES

- Bureau personnel wishing to travel must do so in accordance with the provisions of **Administration (DM Chapter 3, Part 2)**.

- Personnel will be responsible for preparing and submitting the appropriate paperwork in a timely manner.

- Training related travel requests must relate to traveler's assigned duties and/or responsibilities in order to be approved and forwarded.

- Investigative travel requests will be reviewed and approved as they relate to continuing an investigation or corroborating intelligence information.

VEHICLE ASSIGNMENT AND USAGE

All employees operating a policy or County assigned vehicle will be responsible for the care, maintenance, etc., of the vehicle as described in **Vehicles** under **(DM Chapter 5, Part 1)**.

VEHICLE ASSIGNMENT AND USAGE (Continued)

The OCS Supervisor will designate a unit member to serve as the liaison with the Fiscal Administration Bureau's (FAB) Fleet Management Section and the County vendor regarding rental vehicles.

All routine exchanges, involving rental or policy vehicles will be documented utilizing the Vehicle Exchange Information Form.

The form shall be prepared by the concerned employee, approved by the section lieutenant and forwarded to the Administrative Sergeant. The fleet Administrative Sergeant (AS) shall prepare the notification of exchange memorandum to the FAB for the Bureau Major's signature, and revise the Bureau's Vehicle Assignment Roster.

Section supervisors will ensure that all emergency after-hours rental vehicle exchanges are properly documented on the following business day and information forwarded to the AS.

GSA SUPPLIES

AS will coordinate all requests for GSA supplies to ensure the following:

- Check the request against existing supplies, to avoid overstocking.
- Upon receipt of supplies, check the order against the invoice for completeness.
- Notify the person or section that ordered the supplies that the supplies have been received.

All supply storage areas will remain locked at all times.

Keys will be limited to Bureau command staff, section supervisors, each section's supply coordinator, and concerned AS personnel.

Each section supervisor will anticipate their supply needs and be responsible for submitting a completed GSA Supply Request form to the AS:

A. The top portion of the form indicating address and contact person will contain the Bureau suite number and the contact name of the AS supervisor.

B. The person or section requesting the supplies will print their name or section in the lower, left-hand corner of the form.

SECURITY CARDS AND KEYS

The OCS will serve as liaison with the FAB's Building Maintenance Section and the HIDTA Building Security Office on all matters of card/key access issuance and control.The OCS will prepare the necessary forms for initial request for keys and/or cards, return or transfer of keys/cards, and report of stolen or lost keys/cards. Completed forms will be forwarded to the Bureau Major for his signature.

PETTY CASH PROCEDURES [CALEA 17.4.2c]

AS will serve as the liaison with FAB for all cash transaction procedures.

The following procedures will be adhered to when making Petty Cash purchases:

- OCS should be contacted to establish the proper index code and sub-object budget code to be used.
- The completed request is returned to the OCS for processing.
- The request will be forwarded to the Bureau Major for approval.
- Upon approval by the Bureau Major, the OCS will issue cash to the requesting employee.
- When purchase is complete, the original receipt must be affixed to the approved request form and forwarded to the OCS to initiate the repayment process.

PAYROLL AND ATTENDANCE RECORDS (PAR)

- OCS will serve as the liaison with the Personnel Management Bureau (PMB) in all matters concerning employee payroll and attendance.
- ePAR and payroll documents will be submitted to the designated OCS staff member no later than 8:00 a.m., on Friday of the non pay-week, and 7:00 a.m., on Monday, respectively, excluding holidays.
- Sections will incorporate all their personnel records into one PAR form.
- Change Forms should also encompass their entire section's changes into one continuous form, and when possible, the employee identification numbers will be listed in sequential order.
- Completed PAR forms must be reviewed and initialed by the responsible supervisor.

PAYROLL AND ATTENDANCE RECORDS (PAR) (Continued)

- Completed payroll documents must be reviewed and initialed by two individual supervisors.

- Any concerns regarding payroll or attendance issues will be directed to the AS for resolution.

BUREAU REPORTS

Weekly Report:

- The Weekly Report will be submitted to the Captain and the Bureau Major by 8:00 a.m., Friday for review.

- Copies will be distributed as required, with the approval of the Captain and/or Major.

Activity Reports:

- Unit supervisors will ensure their respective personnel prepare and submit Daily/Weekly Activity Reports.

- Reports will be as detailed as the subject confidentiality permits.

- Unit supervisors will enter report information into the HSB/SEFFC Monthly Performance Report spread sheet database.

Bi-Weekly Sector/Assignments Report:

- Unit supervisors will ensure that respective personnel complete Sector and Assignment Brief Reports and that they are forwarded to the IOC for appropriate analysis, via chain of command, no later than every pay week Friday.

- The reports will be reviewed by the appropriate supervisors and received within the IOC by the following Tuesday.

- An electronic version of the report will be saved by the assigned sector and assignment lead investigator in the designated folder on the HSB/SEFFC secure network drive.

MONTHLY REPORT

Bureau Monthly Report:

- Section supervisors will submit their monthly statistical report to the AS on the first working day of each month.
- The OCS will prepare the consolidated Bureau Budget Monthly Report.
- The OCS will submit the compiled report to the Bureau Major for review, via chain of command, no later than the fifth working day of each month

Vehicle Inventory Report:

- AS will complete the Vehicle Inventory Report, which is to be submitted electronically to FAB, Fleet Management Section and Professional Compliance Bureau on the first working day of the month. A hard copy will be filed in the administrative files.
- Section supervisors will ensure that Vehicle Exchange Information Forms (Annex A) are forwarded to the AS immediately upon any change in vehicle assignments for inclusion in the Vehicle Inventory Report.
- AS will compile the Vehicle Exchange Information Forms and forward them to the Bureau Major.

Vehicle Inspection Report:

- Section supervisors will have **Vehicle Inspection Forms (DM Chapter 5, Part 1, Annex A)** completed and forwarded to the Administrative Secretary
- No later than the fifth working day of the month.
- The report will be maintained in the Bureau's administrative files.

Cash Fund Report:

- Section Cash Fund Custodians will submit to the AS a report of cash transactions by the fifth working day of the month.
- AS will prepare a consolidated Bureau monthly statement.
- The monthly statement of all cash transactions (petty cash and investigative funds) will be submitted to the Director no later than the fifth working day of the month **(DM Chapter 4, Part 1, Section I, IV., C.).**

SEMI-ANNUAL REPORTS

Formal Personnel Inspections:

- Formal personnel inspections, which include document and equipment inspections, will be conducted semi-annually, in May and November, and documented, utilizing the **Personnel Inspection Report Form (DM Chapter 2, Part 4, Annex H)**

- AS will compile and forward the reports to the Captain for review and inclusion in the Bureau personnel inspection files.

- AS will forward a consolidated copy of reports, which disclose any discrepancies along with corrective action taken to the Professional Compliance Bureau, Staff Inspections Section.

- As directed by the Departmental Manual, the HSB/SEFFC Intelligence Section Lieutenant will complete the Semi-Annual Informant Report of active Confidential Informants (CI) in April and October.

- The report will contain the control number of all active CI(s), any change in the information included on the Department Control Card, and the total amount of monies paid to each informant, (this report will be forwarded to the Professional Compliance Bureau, Criminal Conspiracy Section).

Facilities and Operations Inspections:

- AS personnel will conduct inspections of facilities and operations semi-annually, in June and December, using the Operations Inspection Report and Facilities Inspection Report.

- The AS Supervisor will prepare a report of findings and recommendations to the Captain.

- The completed forms and report will be maintained in the Bureau's administrative files.

ANNUAL REPORTS

HSB/SEFFC supervisors will ensure that an annual report that details the investigative expenditures of the sections is completed by October 1 of each year.

Annual Investigative Expenditure Report:

- The Section Cash Fund Custodians will submit a reconciled, balanced and properly documented **Annual Investigative Expenditure Report (DM Chapter 4, Part 1, Annex P)** to AS by the first working day of October.

Annual Investigative Expenditure Report: (Continued)

- AS will prepare the Bureau's Annual Investigative Expenditure Report, based upon the submission of each Section's supervisor, for review by the Captain.

- The approved report will be forwarded to the FAB, with a copy to the MDPD Internal Auditor, by October 10, of each year.

Files, Systems, and Equipment Inspections:

- The AS will be responsible for conducting inspections of Bureau files systems and equipment.

- The inspections will be conducted annually, during January, using the Files and Systems Check List and General Equipment Inspection Data Form **(DM Chapter 2, Part 4 Annexes E and F)** for inclusion in the Bureau administrative file.

EMERGENCY OPERATIONS

MDPD has established an Emergency Operations Plan, which describes the overall operation of the Department and individual employees' responsibilities during any large scale event, which threatens the public safety. The HSB/SEFFC has established a Hurricane Operations Plan, which is updated annually and outlines the responsibilities of HSB/SEFFC employees when the hurricane conditions are considered imminent or in the ensuing aftermath if a hurricane does hit MDC.
Procedures and Responsibilities: In addition, all HSB/SEFFC employees will complete the Emergency Management Daily Activity Report when appropriate and authorized during a declared state of emergency.

Personnel Assignments: When a hurricane watch is announced, the following will be accomplished: Assignment of sworn Bureau employees shall be divided between the Alpha shift and the Bravo shift. Sworn Bureau employees who are off-duty will be placed on standby. The County Manager's Office will announce when County employees without hurricane assignments will be excused from duty and employees will be released at the discretion of the MDPD Director.

On-duty Bureau employees will be relieved to secure homes and families as operating strength permit. Bureau employees may be reassigned as the need arises during hurricane operations.

Computer System Procedures: Prior to Bureau employees leaving their work place because of a pending hurricane, the following will be accomplished:

- Ensure all computer information has been backed-up
- Remove diskettes from floppy drives
- Store all back-up disks in a safe location

EMERGENCY OPERATIONS (Continued)

Turn off the following computer equipment:

- Central processing unit (CPU)
- Monitor
- Printer
- Any other peripheral or auxiliary components
- Mini-uninterruptible power supply
- Remove all electrical cables and plugs from electrical outlets
- Disconnect and remove cables from all PC components, if appropriate
- Wrap heavy-gauge plastic around all PC equipment
- All equipment should be picked up off the floor and placed on tables, chairs, or cabinets, in case of flooding.

Upon returning to work, Bureau employees will:

- Inspect all components for signs of wind or water damage

- Contact the Information Technology Services Bureau to report damage and for assistance to reconnect equipment

- Prior to powering up the equipment, ensure that all cables, plugs, and sockets, are dry and clear of debris

- Do not power up any equipment that has sustained water immersion or intrusion

Emergency Contact: After a storm, and within eight hours upon the storm's completion, employees should contact their immediate supervisor. The contact person will initiate telephone calls to employees, in their respective area, who did not contact them. The contact person will then contact the Captain or Major with a status report regarding Bureau employees. The emergency contact roster will be updated periodically throughout the year. The roster will include the address and telephone number where Bureau employees will be located if a hurricane were to strike the greater MDC and Broward County area.

Mobilization Procedures/Mobilization Assignments: Upon a departmental mobilization, all Bureau employees shall comply with the following:

Sworn Employees: Assignments shall be divided between the Alpha shift and the Bravo shift. Report to the location designated and in uniform to perform their assigned duties.

Civilian Employees: Civilian employees shall work such hours as specified by their supervisor and report to the Bureau or other location as specified to perform their assigned duties.

COMPUTER PROCEDURES

Personal Computers (PC) and Laptops – Personal Computers are used for word processing, small database applications and to access network resources. All county assigned PC and issued laptops will be password protected at all times. The departmental approved programs are:

- Microsoft Office Word (Word-processing)
- Microsoft Office Excel (Spreadsheet)
- Microsoft Office PowerPoint (Presentation)
- Microsoft Office SharePoint (Sharing information with Fusion Centers)
- Microsoft Office InfoPath (Document creation tool)
- Microsoft Office Access (Small Database)

MDPD Network: The MDPD Network is available through the local area network and provides the following application:

- Microsoft Office Outlook (E-Mail Department wide)
- Employee Roster (listing all departmental employees)
- Available Training Information
- Departmental Manual with search capabilities
- Florida Statutes
- Right Fax (ability to fax from any PC connected to the network)
- Connection to MDC Main Frame
- Microsoft Office

The following applications are used for investigative purposes:

- **ACISS** is the internal report writing and filing system is the ACISS client-server computer system. An in-house case management system, which houses HSB/SEFFC case reports, Interpol and intelligence information. This system is often used to extract, analyze, and produce homeland security products.

- **AutoTrackXP** has powerful search capabilities, allows one to easily browse, via the internet, through billions of current and historical records on individuals and businesses. Whether investigating fraud, conducting criminal and civil

investigations, locating witnesses, finding missing children or locating and verifying assets, AutoTrackXP can deliver comprehensive information right to your desktop.

- **Caribbean Heat** this web-base program was developed by the MDPD over 20 years ago to monitor Caribbean Criminals. To date, the database contains approximately 400,000 criminals from the Caribbean.

- **Consolidated Lead Evaluation and Reporting (CLEAR)** is a completely new user interface system, which is easy to use, allows for intuitive searching, and intelligence reporting.

- **Crime Analysis System (CAS)** MDPD case management/reporting system.

- **Distributed Factual Analysis Criminal Threat Solution (dFacts)** implements factual data analysis from existing data sources and integrating disparate data from many types of web-enabled storage systems.

- **Driver And Vehicle Information Database (D.A.V.I.D)** provides digital photographs, vehicle, subject, and lien information. If no digital photograph is available, the Florida Investigative Support Center or the Florida Fusion Center can request a manual retrieval of a photograph from the Department of Highway Safety and Motor Vehicles.

- **Department of Corrections (DC) – Career Offender Information Network** provides inmates, parole and probation information, to include photographs, based on name or DC number. Queries can be made on absconders, fugitive and escapees.

- **eAgent** this web-based system is utilized to conduct complete background checks, and is also compatible with National Crime Information Center (NCIC) 2000 and National Law Enforcement Telecommunications System.

- **Electronic Field Interview Report (eFIR)** the eFIR system is an on-line web application developed to capture field interview information and to provide real time investigative search.

- **Entersect** Supports law enforcement and government research efforts across the nation to locate subjects, develop background information, and secure information from a cellular or unlisted number.

- **Financial Crimes Enforcement Network (FinCEN)** provides information on any Currency Transaction Reports, Suspicious Activity Reports (SARs), or any other type of financial report that may be filed on a subject possibly involved in

suspicious activity. This resource is only available between the hours of 8:00 a.m. and 5:00 p.m.

- **Florida Crime Information Center II (FCIC II)** criminal justice information collected by criminal justice agencies that is needed for the performance of their legally authorized, required functions.

- **Florida Criminal Justice Network (CJNet)** provides access to Florida databases; such as the Registered Sex Offenders and Predators Database, the Department of Corrections online search system, the DAVID database, FDLE's Office of Statewide Intelligence, CJIS testing online and many other specialty data links.

- **Florida Division of Corporations (Sunbiz)** provides information for corporations, limited liability companies, limited partnerships, general partnerships, trade marks, fictitious name registrations, and liens. Images of most documents can be accessed. This is a public website and can be accessed at www.sunbiz.org.

- **ESRI Geography Information System (GIS)** a geographic information system integrates hardware, software, and data for capturing, managing, analyzing, and displaying all forms of geographically referenced information. GIS allows us to view, understand, question, interpret, and visualize data in many ways that reveal relationships, patterns, and trends in the form of maps, globes, reports, and charts.

- **GuideSTAR Technologies (GS/1)** is a powerful new tool for the national law enforcement community to facilitate collaboration in detecting and interdicting potential threats and investigating and resolving sophisticated criminal events.

- **Homeland Security Information Network (HSIN)** is a web based encrypted network providing for delivery of real time interactive information exchange among members of the intelligence community. There are currently over 600 communities of interest on the HSIN. HSB/SEFFC is currently accessing HSIN intelligence, Florida, and government portals, as well as posting SEFFC products.

- **Homeland Secure Data Network (HSDN)** is a DHS enterprise-wide solution designed and implemented to provide standardized, secure transport, with desktop applications, to enable a consistent classified capability in support of the DHS mission. HSDN provides the exchange of secret data for DHS and other federal, state and selected local agencies.

- **InfraGard** collaboration for National Infrastructure Protection. InfraGard provide government and law enforcement agencies with subject matter experts, assisting in protecting critical infrastructures.

COMPUTER PROCEDURES (Continued)

- **Law Enforcement Online (LEO)** an official U.S. Government system for authorized use only by authorized members of the law enforcement community. Information presented in this system is considered sensitive, but not classified, and for official law enforcement use only. The SEFFC has created a LEO Special Interest Groups page to provide secure information exchange and sharing for federal, state, local and tribal law enforcement agencies nationwide.

- **I2 Analyst Notebook** provides analysis and visualization capabilities that support IOC analytical ability to turn large sets of data into actionable intelligence.

- **LexisNexis** offers authoritative legal, news, public records, and business information, tailored applications, advanced technology solutions and premium research tools that seamlessly integrate into agency or department work flows.

- **Miami Dade County Mainframe** through the Criminal Justice Information Services (CJIS) Network, County employees are able to research court records, traffic, Miami Dade criminal histories, property records, occupational licenses, warrants, field interview reports, etc.

- **National Crime Information Center (NCIC)** maintains stolen, abandoned, and recovered property and wanted and missing person files in NCIC 200 for all fifty states, Canada, US Virgin Islands, Commonwealth of Puerto Rico and District of Columbia.

- **Pen Link** supports investigators with phone toll records and pen registers to generate a link analysis report for court presentation

- **SAR Vetting Tool (SVT)** designed to improve SAR quality and accuracy as suspicious activity reports are entered into the system. The SVT provides an automated framework to standardize and manage SAR business processes. It also allows other law enforcement agencies to participate in and benefit from the ISE Share Spaces.

- **South Florida Virtual Fusion Center (SVFC)** is a unique model, as it relates to fusion centers. Although virtual in nature, the center leverages information and intelligence from its regional partners to produce a comprehensive view of the situational awareness of the region.

- **Transaction Archive Reporting (TAR) System** is a sub-system of the FCIC II and is used to store and retrieve all FCIC II/NCIC 2000 transactions. The information contained in this file is used for criminal investigations, investigations of suspected misuse, as well as compliance of FCIC II, public record requests, and administrative purposes.

COMPUTER PROCEDURES (Continued)

- **U.S. National Central Bureau Interpol (USNCB)** the HSB/SEFFC serves as the point of contact for all Interpol related issues within MDC. The SEFFC staff has access to both the Interpol Website and Database – one of only five such local agencies in the country.

- **Water and Sewer System** is a database that provides account information on individuals at a particular residence.

Computer Security:

Each user in the Bureau is responsible to protect information from disclosure, tampering and destruction. Access to applications is controlled through the use of passwords and physical security.

Each user's authorized-access to the network is through their ID number and an individual password. Currently, each user has the ability and is responsible for changing their password.

Each authorized person is granted access to the highest level required to meet his or her respective need.

Users will logoff the network and turn off the monitors when away from their workstations for an extended period of time and at the end of each shift.

PCs are to be shutdown and turned off, via the UPS back-up box, at the end of each workweek.

Bureau assigned laptops will not be left unattended unless properly secured in a locked container; e.g., desk within the office, room in the Bureau, or trunk of a vehicle while conducting an investigation. Laptops and electronic media devices will not be left in vehicles or maintained without a password.

All sensitive and classified electronic material will only be stored on the Bureau's secure network server or approved and issued device that meets national security standards.

Computer Usage:

Back-ups should be made daily for all PCs, via the Bureau's secure server "H" Drive.

Printing of data should be limited and unneeded copies will be shredded.

Disks used in PCs will be scanned for virus, prior to being opened in a PC.

Any and all media being transferred or surveyed out of the Bureau for resale or destruction should first be sanitized using a data wiping application, which meets the standards set forth by the United States Department of Defense (DOD5220.22-M). This includes copiers, computers, printers, and electronic media storage devices.

Computer Usage: (Continued)

Bureau personnel are encouraged to become proficient in the use of all computer equipment.

The Miami-Dade Police Safety Training Institute provides training while additional training is available through other Bureau sources.

Most programs are menu driven. Selecting the number or letter corresponding to the desired application allows access to a particular application. Once the application is running, the application dictates what type of entry is required for each task.

Any questions as to the operation of a particular program or function should be referred to the Intelligence Analyst.

E-mail provides a tool that allows communications over the entire Department network. Messages can be sent or received and the information stored and printed. Each person has a mailbox specific to them that is controlled by their sign on.

Documents stored on PCs, attached to the network and running in Windows, can be faxed utilizing Right Fax. This is accomplished by selecting the Right Fax from the printer selection file in the respective word-processing program.

Computer Legal Issues:

Software residing on Bureau computers must be approved and comply with all federal copyright laws.

Personal software should be reviewed by the OCS to ensure that it meets the licensing requirements and is compatible with Bureau operations.

The person presenting personal software must show purchase receipt or documentation reflecting proof of ownership meeting licensing requirements.

Documentation must be provided detailing the operational requirements of the program and the program functions.

SOUTH FLORIDA VIRTUAL FUSION CENTER

The South Florida Virtual Fusion Center (SFVFC) www.sfrfc.org incorporates the information sharing aspect of traditional fusion centers with the accessibility of virtual connectivity using a SharePoint platform. The SFVFC brings relevant partners together to maximize the ability to prevent and respond to terrorism and criminal acts. By embracing this all crimes, all hazards concept, the SFVFC will be able to effectively and efficiently safeguard our region and maximize anticrime efforts. The following is a list of partners:

SOUTH FLORIDA VIRTUAL FUSION CENTER (Continued)

- FBI Field Intelligence Group
- FDLE
- Other federal and state law enforcement
- Law Enforcement in:
    - Monroe County
    - MDC
    - Broward County
    - Palm Beach County
- Regional partners in:
    - Fire/Rescue
    - Emergency Management
    - Health
    - Private Partners

SFVFC is a unique model, as it relates to fusion centers. Although virtual in nature, the center leverages information and intelligence from its regional partners to produce a comprehensive view of the situational awareness of the region.

SFVFC goals are to establish, enhance, and maintain collaborative relationships with all information sharing entities in the region to create and maintain a seamless flow of communication. By reaching out to disciplines, other than law enforcement, a level of cooperation and coordination is created that will assist in the protection of our citizens, visitors, and critical infrastructure. Additionally, the SFVFC will have the ability to leverage all possible sources of information and technology for partners, while ensuring the constitutional rights, civil liberties, civil rights, and privacy of the citizenry are protected.

The SFVFC mission is to protect South Florida by providing information and knowledge, in the form of actionable information, to policy and decision makers. The SFVFC will collect, analyze, produce, and disseminate information in order to support regional efforts to detect, deter, disrupt and deny terrorist and/or criminal activity.

The core functions of the SFVFC are to compile and make available information and intelligence from all relevant sources, and to analyze information and intelligence from all sources to anticipate, identify, prevent and/or monitor criminal and terrorist activity. Distribute intelligence products. through the SFVFC by:

- Posted alerts
- Regional announcements
- Applications
- Document library
- Calendar of events
- Links of interest
- News feeds
- Discussion groups

SOUTH FLORIDA VIRTUAL FUSION CENTER (Continued)

Users are able to post their own alerts to provide situational awareness to other members of the community or to specialized work groups. These alerts can be customized by the user so that information can be disseminated in a timely and accurate manner. Information can range from finished products where all information has been checked and verified for accuracy.

SECTION C - OPERATIONS COORDINATION SECTION (OCS)

STAFFING OVERVIEW

The OCS is comprised of the IOC and the Administrative Operations Support Unit. The OCS is overseen by a Police Lieutenant and encompasses Police Sergeants, Intelligence Analyst Supervisors, Police Officers, Intelligence Analysts, Police Crime Analysis Specialists, Police Records Specialists (PRS), Police Financial Investigators, Data Entry Specialists and Secretary.

The OCS provides administrative, operational, Intelligence and analytical support to all Sections, to facilitate the carrying out of Bureau functions. In addition to the general responsibilities stated above, the below outline depicts specific responsibilities performed by the individual OCS units.

ADMINISTRATIVE OPERATIONS and SUPPORT UNIT

The Administrative Operations Support Unit's goal is to ensure the Bureau's administrative functions comply with departmental policies and procedures.

- Ensure the scheduling and coordination of Bureau roll calls, held once a month, on the second Thursday of each month at 10am.
- Serve as coordinator of the **E-Notify System and ensure that** Bureau members are complying with witness subpoena procedures as specified in **Court Activities (DM Chapter 7, Part 1) accordingly.**
- Conduct inspections of line personnel and vehicles as outlined in **Inspections (DM Chapter 2, Part 4).**
- Perform as the unit inventory representative to coordinate and assist with the preparation of the Capital Asset Inventory for the Bureau.
- Coordinate key and access card assignment and return for all Bureau personnel.
- Prepare requests for Telecommunication Service Forms for telephone, modem and data lines.
- Act as liaison with FAB as requested.
- Maintain the Bureau records in the Personnel Profile System database and prepare reports as requested.
- Perform other assignments as directed by the Section Lieutenant, Captain and Bureau Major
- PRS is responsible for maintaining the Intelligence files [CALEA 51.1.1d]

ADMINISTRATIVE OPERATIONS and SUPPORT UNIT (Continued)

- Prepare Monthly stats
- Maintain the Bureau's equipment and inventory supplies
- Pay monthly Bureau expenses
- Supervise clerical staff
- Coordinate the administrative functions of Bureau personnel enumerated herein
- Keep Bureau personnel informed of changes to departmental policies and procedures
- To ensure that the Bureau procedures comply with departmental guidelines and to modify those procedures as necessary
- To coordinate and monitor the Bureau's budget allocation and spending
- Conduct a background check of businesses, corporations, corporate officers, or firms, and/or persons under the following conditions:

    1. Off-Regular-Duty Police Service Permit Application
    2. A full-time employee submits an Outside Employment Request Form, pursuant to a request from the Director or his designee for:

        a. Taxi permits

        b. Stevedore permits (Port of Miami)

        c. County vendors (Parks Department)

        d. Positions with other County Departments where the nature of the position or assignment is sensitive

INTELLIGENCE OPERATIONS CENTER (IOC)

The IOC serves as the fusing point of sensitive criminal information and has the primary functions of collecting, verifying, analyzing and disseminating criminal intelligence information relating to homeland security issues from local, state and federal agencies. The IOC also has a vital role of being the liaison between multiple partnered agencies that includes local, state, federal and tribal agencies, as well as private entities.

INTELLIGENCE OPERATIONS CENTER (IOC) (Continued)

Additional responsibilities include:

- Responsible for supervising and coordinating specific operational law enforcement activities; inclusive of investigative, tactical, and specialized analytical activities.

- Monitor the progress of assignments and give guidance on the completion of analytical projects, as well as evaluate the quality and resourcefulness of investigative tools used for the desired results.

- Review and assess all requests for assistance and make appropriate assignments to ensure accuracy and legal sufficiency.

- Maintain constant liaison with individuals from other departmental entities and county or state agencies, i.e. representatives from law enforcement, government buildings, transit systems, power plants and other critical infrastructures, processing a homeland security nexus.

- Respond and/or coordinate meetings, conferences, training and critical incidents in order to increase the Department's awareness of potential domestic and foreign threats.

- Record, analyze, evaluating and collect, information to produce all-source intelligence that answers the commander's priority intelligence requirements and information requirements.

- Conduct investigations and coordinate intelligence by recommending areas of interest, and describing possible effects of extremist groups.

- Integrate input to HSB/SEFFC intelligence products for planning, decision making, and investigations.

- Participate in investigations and analyze group or individual capabilities that may pose a public safety risk or impede police and emergency responders or jeopardize long-term objectives.

- Gather and analyze information related to Bureau sector and assignments and then collaborate with the assigned investigator.

- Assess any vulnerabilities and or threats that may arise.

- Create intelligence, information, and officer safety bulletins that relate to analyst assigned sector and assignments.

INTELLIGENCE OPERATIONS CENTER (IOC) (Continued)

- Research different databases for local, national and international intelligence/information to capture homeland related issues to produce bulletins for awareness.

- Read all Homeland Security related emails locally, nationally and internationally for trends, as well as accessing various related internet sites; e.g., HSDN and LEO

- Manage and track requests from the following:

  1. USNCB Interpol
  2. Crime Stoppers Tip
  3. Tips from citizen tip line, emails, and anonymous
  4. Foreign background checks for employment
  5. SAR

- Send out Alert messages from the IOC mainframe to keep HSB/SEFFC staff updated on major event that may affect the citizens of MDC.

- The SFVFC should be updated with regular and situational awareness.

- Enter all SARs into the SVT, so that information can be pushed to the shared space to be shared nationwide.

- Assist HSB/SEFFC investigators that are assigned to their responsible sectors and assignments; which may include using varied database systems; such as FCIC/NCIC, ACISS, D.A.V.I.D., Insite, dFacts, I2 Analyst Notebook, CAS, HSIN, E-agent, AutoTrack XP, Criminal Justice Network, e-Police, SVT, SAR-ISE shared space, Investigative Intranet, LEO, LexisNexis, Interpol I-247, HSIN – Intelligence, public records, SERDSTF Virtual Fusion Database.

- Process phone requests from other law enforcement agencies.

- Attend meetings that relate to specific sectors or assignments.

- Provide research and technical expertise on complex criminal and financial investigations.

- Attend meetings and act as the Bureau's liaison with other investigative support entities.

- Analyst and detective liaisons for the FBI, Miami Joint Analytical Center (JAC) responsibilities are researching, producing and disseminating intelligence products to prevent terrorist acts and to facilitate complete and successful investigations.

HSB/SEFFC EQUIPMENT CONTROL

All personnel are responsible and held accountable for issued equipment.

Exchange or loaning of equipment between personnel is prohibited. All equipment exchanges will be accomplished and recorded through the OCS.

Upon transfer out of the Bureau, or reassignment within the Bureau, all equipment must be returned to the OCS for inspection and reissue.

Supervisors are responsible to ensure that transferred or reassigned personnel report to the OCS with issued equipment prior to transfer or within one week of reassignment.

All stolen, lost, damaged, or destroyed equipment must be immediately reported in accordance with **Logistics (DM Chapter 6, Part 2**).

The person the equipment was issued to, or the first person discovering the loss of or damage to the equipment, must initiate an Offense-Incident Report (OIR) and Report of Missing Property form, which will be forwarded to the Bureau Major for appropriate action.

The person shall forward two copies of the OIR and the Report of Missing Property form to the OCS Supervisor for inventory purposes.

Damaged equipment must be turned in as soon as damage is discovered to minimize further damage and to safeguard employee welfare.

The equipment must be accompanied with a memorandum, approved by the concerned person's supervisor, detailing the damage and containing a statement explaining how the damage occurred.

Personnel will be held responsible for the security of equipment in their possession. Equipment will not be loaned, photographed, copied, sketched, tampered with, reproduced, or unnecessarily displayed without prior authorization of the OCS.

Any violation of the security of Bureau equipment will be immediately reported to the OCS.

Equipment will not be left unattended without exercising reasonable security measures:

1. Equipment in unattended vehicles will be secured in the vehicle's trunk.

2. With the exception of chargers and batteries, equipment will be secured in file cabinets or desk drawers when left unattended in work areas.

Supervisors are to designate secure storage facilities for equipment, within work areas under their control, and are responsible to conduct periodic inspections to ensure that equipment is not left unattended, except as indicated previously.

HSB/SEFFC EQUIPMENT CONTROL (Continued)

The OCS is responsible for control of all Bureau technical and special equipment, and has the authority to recall equipment for preventive maintenance and inspection.

Equipment recall may be verbal, or by memorandum.

Any investigator who feels that relinquishing the recalled item will endanger the successful completion of an ongoing investigation will advise the supervisor of this belief.

Any conflict, which cannot be resolved at the supervisory level will be referred to the Bureau Major, via chain of command, for a final decision and assignment of priorities.

SECTION D - INTELLIGENCE SECTION

STAFFING OVERVIEW

The Intelligence section is comprised of two Intelligence Squads and a Technical Operations Unit (TOU). The intelligence section encompasses a Lieutenant, Police Sergeants, Police Officers, Secretary and Data Entry Specialists.

INTELLIGENCE SQUADS

The Intelligence Squads are the primary departmental and Bureau representatives on all criminal intelligence matters. However, all HSB/SEFFC Sections and personnel share equal responsibilities in coordinating, monitoring and overseeing homeland security related incidents within the MDPD's jurisdiction.

The Section will not ordinarily perform enforcement activities, but shall be a source of intelligence and investigative assistance for operational units [CALEA 51.1.1d].

Additionally, the below listed details encompass responsibilities and assignments that parallel and/or interlink to all HSB/SEFFC Sections:

- Initiate proactive homeland security related investigations.
- Assume control of any MDPD homeland security related incident, as deemed appropriate.
- Gather, analyze, disseminate and maintain corresponding criminal intelligence.
- Maintain communication, information, and/or cooperative liaison regarding subversive, militia and extremist activities, as well as civic, labor and community activist/causes that may adversely impact the citizens of MDC and/or result in civil disorder.
- Identify MDC's critical infrastructures and key assets.
- Initiate or recommend vulnerability assessments.
- Maintain liaisons with the public and private sectors.
- Promote homeland security awareness.
- Provide homeland security related assistance to law enforcement agencies at the local, state, federal and international levels.
- Attend and contribute to law enforcement intelligence groups, task forces and law enforcement committees.

FORENSIC VIDEO UNIT (FVU)

The FVU provides video forensics services to Bureau and departmental personnel, as well as other local, state and federal agencies requiring this service.

Services provided:

- Recover all video evidence for departmental investigative units as requested.
- Transcode video evidence from captured media format to DVR or other requested format.
- Conduct comparison analysis.
- Provide images from video for subject identification.
- Prepare media releases to provide the media for identification purposes.
- Provide peer review of high profile cases for requesting agencies prior to case presentation in court.
- Provide expert testimony.
- Prepare proper reports on procedures and findings for administrative or court presentation.
- Provide proper care and preventive maintenance of specialized equipment assigned to the unit.
- Provide equipment and operational expertise for all entities of the Department and outside agencies, as required [CALEA 51.1.1d].

EVIDENCE CONTROL

All evidence received by FVU must be accompanied by a Property Receipt, and entered into the Property and Evidence Tracking System. The person(s) receiving the evidence are responsible for the evidence being properly secured in the evidence storage locker.

Upon completion of required analysis process, FVU will notify the requesting entity. It is the responsibility of the requesting detective to take possession of the property within 72 hours of being notified.

FVU EQUIPMENT PROCEDURES [CALEAA 51.1.1d]

The VFU will make every effort to acquire and provide the most appropriate equipment available to suit the requirements of the investigation.

FVU EQUIPMENT CONTROL

All personnel are responsible and held accountable for issued equipment.

Upon transfer out of the Bureau, or reassignment within the Bureau, all equipment must be returned to the OCS for inspection and reissue.

Supervisors are responsible to ensure that transferred or reassigned personnel report to the OCS with issued equipment, prior to transfer or within one week of reassignment.

All stolen, lost, damaged, or destroyed equipment must be immediately reported in accordance with **Logistics (DM Chapter 6, Part 2**). The person the equipment was issued to, or the first person discovering the loss of or damage to the equipment, must initiate an Offense-Incident Report (OIR) and Report of Missing Property form, which will be forwarded to the Bureau Major for appropriate action.

The person shall forward two copies of the OIR and the Report of Missing Property form to the OCS for inventory purposes.

Damaged equipment must be turned in as soon as damage is discovered to minimize further damage and to safeguard employee welfare.

The equipment must be accompanied with a memorandum, approved by the concerned person's supervisor, detailing the damage and containing a statement explaining how the damage occurred.

Personnel will be held responsible for the security of equipment in their possession. Equipment will not be loaned, photographed, copied, sketched, tampered with, reproduced, or unnecessarily displayed without prior authorization of the OCS.

Any violation of the security of Bureau equipment will be immediately reported to the OCS.

Equipment will not be left unattended without exercising reasonable security measures:

1. Equipment in unattended vehicles will be secured in the vehicle's trunk.

Supervisors are to designate secure storage facilities for equipment, within work areas under their control, and are responsible to conduct periodic inspections to ensure that equipment is not left unattended, except as indicated previously.

The OCS is responsible for control of all Bureau technical and special equipment, and has the authority to recall equipment for preventive maintenance and inspection.

TECHNICAL OPERATIONS UNIT (TOU)

The TOU squads assist, Section Bureau and departmental personnel with specialized equipment use and technical expertise.

Additionally, they perform the below listed details.

- Prepare proper reports on intelligence gathering activities resulting from use of specialized equipment.
- Conduct surveillances as directed.
- Provide proper care and preventative maintenance of all specialized equipment.
- Comply with vehicle maintenance.
- The Unit also provides technical support in the form of sophisticated electronics.
- Equipment and operational expertise for all entities of the Department and outside agencies, as required [CALEA 51.1.1b].

The following procedures for the TOU will apply:

TOU EQUIPMENT PROCEDURES [CALEA 51.1.1d]

The TOU will make every effort to acquire and provide the most appropriate equipment available to suit the requirements of investigators.

TOU EQUIPMENT DESCRIPTION

The basis for issuance of equipment will vary with equipment type. Equipment has been separated into four general groups:

Regular Investigative Aids; including, but not limited to, tape recorders, camera kits, tripods, binoculars, night scopes, etc.

Specialty Equipment: including, but not limited to, transmitter tracking devices, vehicle tracking equipment, miniature transmitters and kits, telephone decoders, room amplifiers and associated equipment.

This equipment will only be issued in accordance with **Investigations (DM Chapter 25, Part 1)**. As a general rule, any covert recording and transmitting equipment that is subject to legal guidelines, pertaining to the interception of oral or wire communication, falls into this category.

TOU EQUIPMENT DESCRIPTION (Continued)

This equipment is only issued to personnel that have demonstrated the ability to utilize it properly. The TOU supervisor will determine the extent of experience or training necessary in order to establish the proficiency necessary to successfully utilize the equipment.

Technical Equipment: can be highly specialized, expensive, or sensitive, including: video cameras; recorders and associated items; audio recorders; night vision devices or cameras; testing and diagnostic equipment; audio and video processing equipment; specialty tools; and other equipment as determined by the TOU Supervisor.

TOU personnel are available to install and operate the equipment. In some instances, after the initial installation, investigators may be trained to operate the equipment. After demonstrating their ability, it may be issued to them on a per case basis at the discretion of the TOU Supervisor.

TOU EQUIPMENT CONTROL

All personnel are responsible and held accountable for issued equipment.

Exchange or loaning of equipment between personnel is prohibited. All equipment exchanges will be accomplished and recorded through the OCS.

Upon transfer out of the Bureau, or reassignment within the Bureau, all equipment must be returned to the OCS for inspection and reissue.

Supervisors are responsible to ensure that transferred or reassigned personnel report to the OCS with issued equipment, prior to transfer or within one week of reassignment.

All stolen, lost, damaged, or destroyed equipment must be immediately reported in accordance with **Logistics (DM Chapter 6, Part 2**). The person the equipment was issued to, or the first person discovering the loss or damage to the equipment, must initiate an OIR and Report of Missing Property form, which will be forwarded to the Bureau Major for appropriate action.

The person shall forward two copies of the OIR and the Report of Missing Property form to the OCS for inventory purposes.

Damaged equipment must be turned in as soon as damage is discovered to minimize further damage and to safeguard employee welfare.

The equipment must be accompanied with a memorandum, approved by the concerned person's supervisor, detailing the damage and containing a statement explaining how the damage occurred.

TOU EQUIPMENT CONTROL (Continued)

Personnel will be held responsible for the security of equipment in their possession. Equipment will not be loaned, photographed, copied, sketched, tampered with, reproduced, or unnecessarily displayed without prior authorization of the OCS.

Any violation of the security of Bureau equipment will be immediately reported to the OCS.

Equipment will not be left unattended without exercising reasonable security measures:

2. Equipment in unattended vehicles will be secured in the vehicle's trunk.

3. With the exception of chargers and batteries, equipment will be secured in file cabinets or desk drawers when left unattended in work areas.

Supervisors are to designate secure storage facilities for equipment, within work areas under their control, and are responsible to conduct periodic inspections to ensure that equipment is not left unattended, except as indicated previously.

The OCS is responsible for control of all Bureau technical and special equipment, and has the authority to recall equipment for preventive maintenance and inspection.

Equipment recall may be verbal, or by memorandum.

Any investigator who feels that relinquishing the recalled item will endanger the successful completion of an ongoing investigation will advise the supervisor of this belief.

Any conflict, which cannot be resolved at the supervisory level, will be referred to the Bureau Major, via chain of command, for a final decision and assignment of priorities.

ISSUE PROCEDURES

Prior to issue, the following steps will be completed:

1. Equipment availability and serviceability will be determined.

2. Special equipment items as detailed in Investigations (**DM Chapter 25, Part 1**), require that a Special Equipment Form, be completed.

3. The investigator that will actually be utilizing the equipment will receive instructions and be involved in a simulated test of the equipment.

TOU personnel will provide instructions to the users to ensure that equipment is to be utilized within the legal parameters and technical limitations of the equipment issued.

Issued equipment is the exclusive responsibility of the person signing for it.

ISSUE PROCEDURES (Continued)

The Equipment Assignment History Log (Annex D) recording the transaction will be prepared by TOU personnel.

The completed Equipment Assignment Log and the form will be placed in the equipment-out tray for processing in the TOU Inventory Control System computer program and filing into the TOU badge number file of the concerned employee.

RETURN PROCEDURES

Equipment signed out by an individual will be returned by that individual.

In the absence of the concerned employee, the equipment will be accepted by TOU from the supervisor of the individual to whom the equipment was issued.

To ensure full utilization of available resources, investigators will be required to return equipment as soon as the task for which the equipment was checked out for is completed.

If the equipment will be held longer than 24 hours, prior approval of the TOU Supervisor is required.

Upon return, the following steps will be completed by TOU personnel:

a. Equipment will receive perfunctory inspection.

b. The Equipment Assignment History Log in the concerned employee's badge file will be updated to reflect the return.

c. A photocopy of the update will be made available to the person returning equipment, if requested.

d. The completed form will be placed in the Inventory Control Officer's in-basket for computer processing.

INVENTORY RESPONSIBILITIES

The TOU supervisor will insure that equipment inventory records are maintained. Inventory records will include:

A. An equipment file listing all equipment on the Bureau inventory.

INVENTORY RESPONSIBILITIES (Continued)

1. Periodic Inventories:

   a. Departmental policy requires that a complete physical inventory of all capital equipment shall be taken annually. This inventory is in response to notification by the departmental inventory officer.

   b. All communications equipment must be inventoried annually, during the month of January, documented on an inventory worksheet and forwarded to the Communications Bureau by January 31 of each year.

EQUIPMENT REPAIR

Repair or alteration of issued equipment by someone other than TOU personnel is strictly prohibited.

Radios in need of repair may be taken to the County Radio Shop by the person having custody of the device.

All other equipment shall be returned to the TOU for repair.

ELECTRONIC INTERCEPT PROCEDURES

All electronic telephone intercepts dialed number recorders (DNR's), and oral intercepts will be conducted in accordance with **Investigations (DM Chapter 25, Part 1).**

Prior to applying for a court order to conduct any electronic telephone intercepts, the concerned investigator will complete the following steps:

1. Check with the TOU for availability of equipment.

2. Obtain approval of the Bureau Major, via the chain of command. This also applies to disconnecting an intercept.

3. Prepare the intercept application and affidavits in consultation with a departmental legal advisor, if applicable.

4. Deliver the application and affidavit to the State Attorney's Office for authorization, pursuant to making application to a judge

5. The court order must bear the judge's typed or printed name, as well as his signature and be certified or notarized by a clerk of the court. Two copies of the order are to be delivered to TOU.

6. A lead technician will be assigned to the case. The technician will initiate and follow through with the technical aspect of the intercept. In the event of an

7. absence of the lead technician, an alternate may be assigned by the TOU supervisor. The lead technician will complete the following steps:

    a. Initiate an intercept case file containing one copy of the court order and all subsequent paperwork.
    b. Prepare the proper form letter requesting assistance from the telephone company and deliver the letter, with a copy of the court order, to the telephone company.

    c. Check subscriber information, obtain current appearance point information, and order appropriate services.

    d. Verify the appearance points and request a 1FB Business service line.

SECURITY

The TOU will normally be attended between 8:00 a.m. and 6:00 p.m., Monday through Friday, excluding holidays. The TOU's shop and special equipment storage room will be locked when not attended. Regular on-call procedures will be utilized when the TOU shop is unattended.

Access to the shop will only be granted by TOU personnel, the TOU Supervisor, and/or the Bureau Major.

Keys to the TOU shop will only be in the possession of TOU personnel, the TOU Supervisor and the Bureau Major.

[redacted]

SECTION E - INFRASTRUCTURE PROTECTION SECTION

STAFFING OVERVIEW

The Infrastructure Protection Section (IPS) is comprised of two Infrastructure Protection Squads and a Special Projects Squad. The IPS encompasses a Lieutenant, Police Sergeants, Police Officers and Secretary.

INFRASTRUCTURE PROTECTION SQUADS

The IPS squads are the primary departmental and Bureau representatives on all infrastructure protection matters. However, all HSB/SEFFC Sections and personnel share equal responsibilities in coordinating, monitoring and overseeing homeland security related incidents within the MDPD's jurisdiction.

Additionally, the below listed details encompasses responsibilities and assignments that parallel and/or interlink to all HSB/SEFFC Sections:

- Initiate proactive homeland security related investigations.
- Assume control of any MDPD homeland security related incident, as deemed appropriate.
- Gather, analyze, disseminate and maintain corresponding criminal intelligence.
- Maintain communication, information, and/or cooperative liaison regarding subversive, militia and extremist activities, as well as civic, labor and community.
- Monitor activist/causes that may adversely impact the citizens of MDC and/or result in civil disorder.
- Identify MDC's critical infrastructures and key assets.
- Initiate or recommend vulnerability assessments.
- Maintain liaisons with critical infrastructure and key resource partners within both the public and private sectors.
- Promote homeland security awareness.
- Provide homeland security related assistance to law enforcement agencies at the local, state, federal and international levels.
- Attend and contribute to law enforcement intelligence groups, task forces and law enforcement committees

SPECIAL PROJECTS SQUAD

The Special Projects Squad is responsible for handling, coordinating, monitoring and overseeing homeland security related projects that are deemed special by the Bureau command staff, as well as assisting with the aforementioned Bureau personnel responsibilities.

SECTION F - SOUTHEAST REGIONAL DOMESTIC SECURITY TASK FORCE

The Southeast Regional Domestic Security Task Force (SERDSTF) was established to address preparation and response efforts by federal, state, and local law enforcement agencies, fire and rescue departments, first responder personnel and others in dealing with potential or actual terrorist acts within or affecting this state. The task force administration is comprised of personnel from MDPD and the Florida Department of Law Enforcement (FDLE); they include a police lieutenant who serves as the Functional Work Group (FWG) supervisor, and who works in conjunction with a group supervisor from FDLE. Three sergeants support the mission of the SERDSTF as FWG liaisons to the 11 FWGs, and are supported by three civilian analysts from FDLE.

SERDSTF Goals and Objectives:

PREPARE for all hazards, natural or man-made, to include terrorism.
PREVENT, preempt, and deter acts of terrorism.
PROTECT Florida's citizens, visitors, and critical infrastructure.
RESPOND in an immediate, effective, and coordinated manner, focused on the victims of the attack.
RECOVER quickly and restore our way of life following a terrorist attack.

The goal of Florida's Domestic Security Strategy is to strengthen our domestic security prevention, preparedness, protection, response and recovery capabilities through interdisciplinary and interagency consensus and commitment and to build and rely on a strong regional mutual aid response capability. The SERDSTF plays an integral role by representing the interests and needs of Region 7 and assists in coordinating disaster and emergency response within the region, or to an adversely affected region somewhere else within the state.

Responsibilities of the SERDSTF also include: improving Florida's ability to identify potential terrorist threats; collect and disseminate intelligence and investigative information; facilitate and conduct ongoing security audits and vulnerability assessments to protect critical infrastructure; promote public awareness of how suspicious incidents should be reported; coordinate tabletop exercises and drills to further develop the skills of first responders and disaster response teams, should an emergency related to a terrorist threat develop and coordinate and facilitate response operations involving Regional Domestic Security Team assets, in accordance with the State Terrorism Response Plan.

The SERDSTF represents the operational component of Florida's domestic security structure within Region 7, as is tasked with the following:

- Bringing regional partners together- emergency management, fire rescue, health, education, law enforcement, communications, and the private sector.
- Provides the forum for open communications among partners.
- Builds cooperation, understanding and appreciation for each other's role in protecting and securing our citizens and visitors.
- Provides essential link between the community and the state – acts as a conduit for information exchange, coordination (training, equipment, exercises) to ensure a community focus, statewide consistency, and redundancy in strategy, operations and protocols.

The SERDSTF is also tasked with the coordination of the regional statewide grant submission process. These responsibilities include:

SECTION F - SOUTHEAST REGIONAL DOMESTIC SECURITY TASK FORCE (Continued)

- Facilitate regional capability reviews, which are submitted to the FDLE Office of Domestic Security for use in future funding consideration.
- Coordinate regional committees that conduct project development, based upon the review.
- Identify regional projects and requested funding, and coordinate submission to the Office of Domestic Security.
- Coordinate the regions participation in the Peer Review process, which scores each project submission. (Accounts for 30% of final project score.)
- Represent the region in the funding committees, to prioritize and present projects to voting members. (55 voting members, representing regions and state vote. Voting accounts for 70% of final ranking. The prioritized list presented to SWG Executive Board and DSOC for final approval.)

SECTION G - Department of Emergency Management and Homeland Security

As part of the MDPD, HSB has assigned a contingent of police personnel to the Department of Emergency Management (DEM) in order to act as liaisons to the emergency management community.

Police personnel include:

- (1) Police Lieutenant
- (1) Police Sergeant
- (2) Police Detectives

As homeland security liaisons to the DEM, these officers perform the following functions as part of their duties:

- Serve as DEM and HSB liaison with municipal police departments, County, state and federal law enforcement agencies; including the FBI and FDLE.
- Provide law enforcement subject matter expertise to better ensure DEM and HSB is actively engaged in effective planning, training and exercises within the law enforcement community. Write plans and procedures as assigned. Coordinate and participate in training and exercise events as assigned.
- Analyze and review police and homeland security intelligence reports and briefs Command Staff personnel and other appropriate DEM and homeland security personnel on potential security threats and emerging issues, as allowed in accordance to their respective clearances.
- Assist the DEM and Homeland Security Watch Center personnel with reviewing and analyzing homeland security information as necessary. Provide a linkage into the police intelligence community, as necessary, to verify and validate information for alerts and warnings.
- In cooperation with MDPD, assist DEM and homeland security personnel in obtaining risk assessments for fixed facilities, transportation and critical infrastructure.
- Participates in Emergency Operation Center activations as appropriate.
- Participates in community outreach activities, town hall meetings, community events and other public education activities.
- Serves as Emergency Management Liaison to Miami-Dade Fire Rescue Grants Bureau for Urban Area Security Initiative and State Homeland Security Grants Program.
- Participate in homeland security grant projects, grant funding meetings, grant application management activities, etc.
- Manages program budgets and resources as assigned
- Represent DEM and HSB on homeland security committees as assigned.
- Upon request, assist the MDPD Director with special assignments and projects.
- Prepares reports, maintains documentation and records.

SECTION H – ARREST and SEARCH WARRANT PROCEDURES

ARREST and SEARCH WARRANT and CONFIDENTIAL INFORMANT PROCEDURES

OVERVIEW

HSB/SEFFC personnel will ensure that when obtaining or executing any warrant or handling and processing confidential informants, that they abide by the procedures set forth in the MDPD Departmental Manual.

SECTION I – SOURCE DEVELOPMENT and RECRUITMENT

SOURCE DEVELOPMENT and HANDLING PROCEDURES

OVERVIEW

Listed below are the Bureau's source development and handling procedures. Bureau lieutenants will ensure that each corresponding responsibility is adhered to by their personnel.

HSB/SEFFC personnel will ensure that their implementation of source development and handling procedures augments the already existing confidential informant procedures, as outlined in the Departmental Manual.

Glossary:

- Domain - sector, assignments or groups that have an impact to MDC.
- Source - refers to a person who is knowledgeable in a field of interest and is not handled by any one detective.
- Informant - implies a criminal nexus and procedures governing such will be in accordance with the Department's Standard Operating Procedures.
- Levy - tasking of source, every contact should end with a tasking.

Source Management:

- HSB/SEFFC personnel will review and comply with departmental policies and procedures, as related to confidential informants and sources, prior to working with sources.
- Bi-annual assessments are conducted on current domains to determine resource allocation for source and intelligence development.
- Staff will utilize domain assessments provided by IOC sector analysts, current local and international events/changes affecting the domain, detective assessment/opinion, and other pertinent data to make proper adjustments of resource allocation.
- The Bureau's Intelligence Section lieutenant and one IOC detective will conduct source report deconfliction, on a routine/continual basis.
- Source deconflicters will review reporting, and deconflict reporting with other agencies within the MDPD area of responsibility.

Source Management: (Continued)

- Source deconflicters will be tasked with meeting to discuss source reporting and meeting with other agencies to ensure efforts are not duplicated. This will maximize the effective utilization of our resources.

- The IOC analysts will create and maintain fluid domain assessments to ensure accurate and effective data as it pertains to the domain.

- Data will be comprised of all available resources of information and will be noted along with the deriving source, date acquired, location and name of originating source.

- IOC analysts will identify intelligence gaps within domains and create target packages by providing all pertinent data to assist detectives in filling the gap.

- Domain assessments should remain fluid and will be reviewed every 14 days to ensure the data is current, and pertinent information is updated.

- Domain assessment changes will be noted in detail and all prior information will be retained in order to document continuity.

- Domain assessment will be utilized to brief Bureau Commanders at and other MDPD command staff personnel as warranted, as well as to assist in investigations and intelligence gathering capabilities.

- Domain assessments are sensitive documents and must be treated as such, following existing procedures and protocols. Release of the assessments outside of the HSB/SEFFC will require approval of a lieutenant or higher and will be documented.

- Assessments are to be treated as sensitive material and hand carried during any transmission.

- Under no circumstance will assessments be transmitted via electronic correspondence.

Open Source Reporting:

- Detectives will utilize Sector Bi-Weekly Brief Reports to document open source reporting.

- Detectives should identify open sources by name and provide basic contact information for the open source. Other biographical information is helpful, but not required.

Open Source Reporting: (Continued)

- IOC analysts will review sector contact reports, and utilize information provided to update domain assessments. Further inquiries for information or information deconfliction should be redirected to sector detective.

- IOC sergeant, or cleared designee, will maintain a listing of HSB/SEFFC open sources to maximize effective utilization of available information resources.

- The Intelligence Section Lieutenant is the Confidential Source Manager (CSM).

- The CSM will be responsible for overall source and source dossier management.

- The CSM will ensure confidential sources are being utilized properly and contact is being maintained by managing detectives.

- Use of written documentation and appropriate database tracking will be retained in a secure environment that is only accessible to the CSM, the HSB/SEFFC Captain or the HSB/SEFFC Major (this allows an effective means to manage sources and reduces duplication efforts).

- Command staff will have a clear picture of HSB/SEFFC source capabilities and network. In the event a detective needs a source in a certain community or has access to a certain job, field or group, the CSM can help identify a possible match, and guide the detective towards the handling detective.

- The CSM will identify sources by source number, and basic demographic information to include:

    - Sex
    - Age Range (Ex 20-25)
    - Ethnicity
    - Physical Characteristics
    - Access (what do they do, what domain they have access to, member of specific group, etc.)
    - Educational Level
    - Languages Spoken
    - Handling Detective

- The CSM will be responsible for maintaining a dossier sample and keeping the format up to date.

- Follow MDPD guidelines in source dossier procedures, and amend the following source bio to include:

    1. Level of education
    2. Languages spoken
    3. Membership in organizations

Open Source Reporting: (Continued)

4. Hobbies
5. Extended family relationships
6. Detective inquiries into source biases, motivations, training progress, effectiveness, and personal opinion to facilitate source use by another detective
7. Religious and political affiliations
8. Personality assessment

Confidential Source Management and Reporting:

- The IOC analysts will utilize confidential source reporting to update domain assessments.

- The IOC analysts will identify confidential sources by source number in reporting. Any inquiries to source information will be referred to the handling agent.

- HSB/SEFFC personnel will ensure that MDPD Confidential Informant guidelines are followed, during the recruitment and/or handling of a confidential source (see MDPD Departmental Manual for specifics).

- Sources will be developed to meet the needs of intelligence gaps in HSB/SEFFC domains.

- Sources will be identified as an open and confidential source.

- Open source:

    1. Human source that routinely provides information of value to the law enforcement community
    2. Source requires little or no anonymity and low level of protection
    3. Confidential source
    4. Source requires high level of anonymity and protection

- HSB/SEFFC detectives will focus resources in recruiting sources that will assist in filling intelligence gaps, which are fluid, in assigned domains.

Open and confidential sector sources should be contacted minimally every 14 days (telephonic or personal).

- All contacts will be documented in a source dossier or sector weekly contact reports should include type of contact, times, and synopsis of conversation.

- All information will be reported, regardless of investigative value.

Confidential Source Management and Reporting: (Continued)

- Detectives should continue to test, train, evaluate and levy their source during every contact.

- A proper turnover of sources will be conducted upon a handling detectives' retirement or Bureau transfer.

SECTION J – INVESTIGATIVE and REPORTING PROCEDURCES

INVESTIGATIVE and REPORTING PROCEDURES

The below procedures should be implemented <u>when applicable</u>, in all Bureau cases and investigations, and <u>will</u> always comply with CALEA standards:

Notifications (prior to, upon arrival and post scene investigations):

- Immediate Supervisor
- IOC
- JTTF
- Other Affected HSB/SEFFC sector detectives
- Appropriate sector point of contact
- HSB/SEFFC sector analyst

Documentation:

- All notification dates and times should be maintained for investigative/case file timeline purposes.
- Homeland Security Report- to be utilized by all investigators to document every investigative effort and noteworthy event. This report is an HSB/SEFFC internal report, similar to an offense incident report and/or any other type of redline investigative report. It serves as both an original and a supplemental report.
- Subject Data Entry Worksheet- to request the appropriate type(s) of subject background checks, allowing for either an independent/stand-alone background check or as a supplement to the assigned investigator's independently conducted checks.
- Timeline Sheet- tracks the dates and times of all notifications, investigative steps, leads, follow-up actions, document preparations and submittal/return dates.
- Case File Coversheet- to be appropriately titled and placed over each section of the case file.

Reporting Procedures:

- All Incidents/cases will be reported **<u>immediately</u>** to the chain of command, via the first line supervisor (supervisor notifies the chain of command telephonically or via e-mail).

Reporting Procedures: (Continued)

- The **respective sergeant, all Bureau lieutenants and the IOC** will **immediately be notified during and/or following the initial investigation**.

This summary will serve as a draft for the command staff incident notification. The IOC will also utilize this draft to originate any paperwork and correspondence, as needed. A full report of the incident will then be completed, using the Homeland Security Report **within 24 hours of the incident**. A hard copy of this report will then be submitted to the respective sergeant for review and approval. The final draft of the Homeland Security Report **must** be completed, reviewed and approved by the supervisory chain, within three working days of the event. Once final approval of a report is obtained, the **signed hard copy, along with the corresponding electronic copy will be forwarded to the IOC** for appropriate entry **(*note-detectives must ensure that they index all pertinent information pertaining to the report, to secure appropriate cross references).**

- The IOC will assign and maintain all homeland security reports' case numbers including any supplemental report numbers. Case numbers generated as a result of an after hours incident will be assigned on the following work day. In either event, the lead detective on each case is responsible for generating the corresponding case numbers from the IOC.

- All after hour called out detectives will be assigned lead investigator status for their responding incident and will remain with the assigned case throughout its entirety.

- The appropriate sector detective will be notified of all investigations involving their sector and may be assigned co-lead responsibilities on the next regular work day.

- All subsequent case actions regarding an incident or event will be identified by the appropriate supplemental report case number i.e., HSB/SEFFC 2006-1.1, HSB/SEFFC 2006-1.2, HSB/SEFFC 2006-1.3 etc.

- All reports **must be** submitted along with the original master case file for review and approval by lead detective's immediate sergeant and lieutenant (see case file content for further instructions).

- Case files will then be returned to lead detective for appropriate filing/securing.

- All master case files will be centrally stored and secured within the HSB/SEFFC through the designated records custodian in the IOC.

- Lead investigators may maintain individually stored and secured working case files and **under no circumstance will these files be left in any vehicle or unsecured area.**

Follow-Up:

- Investigators will continuously liaison with the JTTF, sector point of contacts and other affected sector detectives.

- Detectives will maintain timelines for all follow-up contacts, notifications and investigative activities.

Case File Content:

- Each case file must be maintained in a red, two partition folder divided into six categories (non-pertinent or continual events and/or assigned tips may be kept in smaller red partition folders). The tabs must be uniformly labeled as follows; (1) Timeline, (2) HSB/SEFFC Reports, (3) MDPD Reports, (4) Other Agency Reports and Miscellaneous Documents, (5) Subject Profile (6) Photographs. The dividers will be prefaced by a titled HSB/SEFFC Coversheet that also contains bullets for each type of document within its category (i.e., the wording HSB/SEFFC Reports on the coversheet and bullets beneath it stating the specific reports, etc.) **Case File Coversheet-** to be appropriately titled and placed over each section of the case file **(Annex D).**

File content includes:

- Homeland security report(s) with supervisory signatures
- Subject Data Worksheet(s)
- All subsequent documentation returned by IOC
- MDPD reports (Offense Incident Reports, Filed Interview Cards, etc.)
- JTTF reports
- Supervisor case summary reports
- Reports from outside police agencies, municipalities,
- Public and private sector reports (i.e., Miami-Dade Water and Sewer Department, Miami-Dade Transit)
- Security agencies' reports (i.e., Wackenhut Incident Reports)
- Timeline Report
- Subject profiles/photographs
- Scene/evidentiary photographs

File content includes: (Continued)

- Investigations directed at a person or group of persons for the purpose of identifying a criminal activity or gathering intelligence information to anticipate, prevent, or monitor.

- Investigators will obtain prior approval from the unit supervisors to initiate an intelligence case.

- The unit supervisor will determine that there is reasonable suspicion of criminality to initiate an intelligence case.

- The gathering of data for political or other purposes unrelated to criminal activity is prohibited.

- The unit supervisor will closely monitor the progress of the intelligence case to insure concurrence with state law and departmental rules, policies, and directives.

- Criminal intelligence information received from anonymous sources will be carefully scrutinized and evaluated by investigators and the unit supervisor. The information must be verified by an independent source prior to initiating an intelligence case.

- Intelligence cases will have a six-month suspense date, during which it must be demonstrated that criminal activity exists [CALEA 51.1.1c].

- Intelligence cases failing to meet requirements as aforementioned or cases that are not updated or supplemented for a period of six months, will be considered a closed investigation subject to disclosure pursuant to the Public Records Law [CALEA 51.1.1c].

- Exception - intelligence information documented prior to January 25, 1979, is not covered under the public records law; therefore, it is not subject to disclosure [CALEA 51.1.1c].

REPORTS AND RECORDS [CALEA 51.1.2]

General

The HSB/SEFFC follows and observes, as warranted, national references pertaining to information gathering and intelligence sharing of such material and data (i.e., GIWG, NCISP, 28 CFR, Fusion Center guidelines, etc.). The aforementioned is done in concert with applicable state and local laws.

REPORTS AND RECORDS [CALEA 51.1.2] (Continued)

Information can be received at HSB/SEFFC from numerous sources; some of these sources can be:

- Private citizens
- Anonymous telephone call or written correspondence
- News media reports (open source)
- Other county, state, or federal agencies/departments
- SARs

The HSB/SEFFC has established an internal investigative report writing and filing system that is designed to record and protect complex and sensitive investigative intelligence information, which requires strict confidentiality. These reports were created in Microsoft InfoPath.

SUSPICIOUS ACTIVITY REPORT (SAR)

SARs is gathering of information regarding behaviors and incidents associated with crime and establishing a process, whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism.

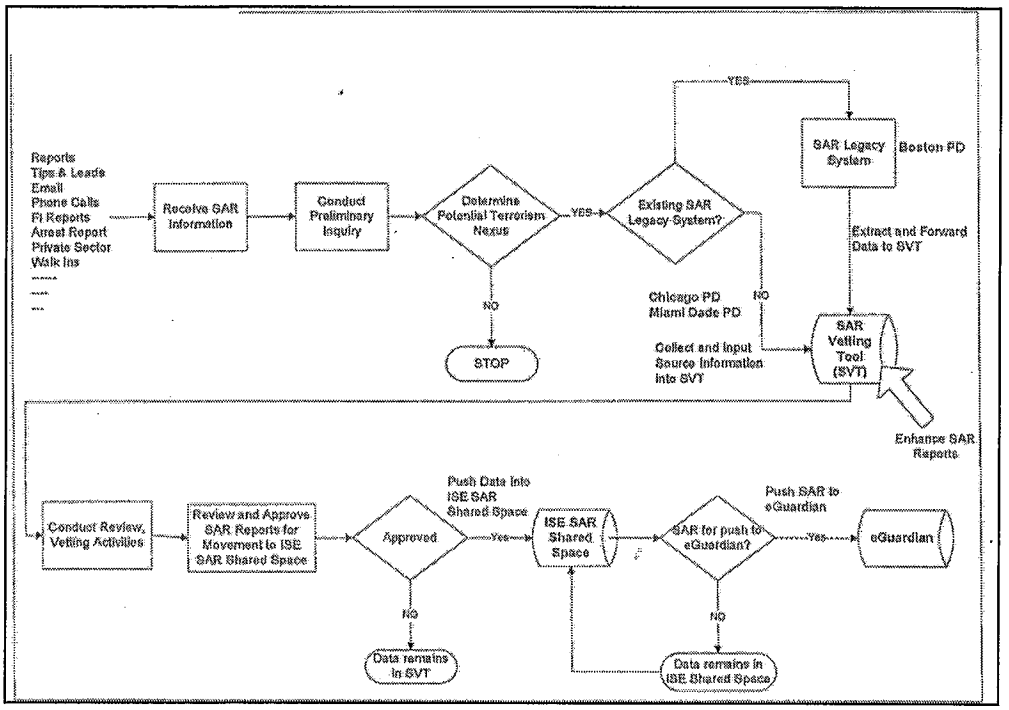
Directive 08-14, was created and distributed to all MDPD personnel and was incorporated into the Departmental Manual. This Directive explains how we all play a vital role in identifying and reporting suspicious activity that may be indicative of behavioral traits or patterns related to homeland security threats, as well as give detailed information of how, what, when, where, regarding suspicious reporting.

SAR reports are vetted and identified through user roles and functionality; analyst, supervisor and administrator, before being pushed to the ISE-Shared Space.

The SVT was designed to improve SAR quality and accuracy as suspicious activity reports are entered into the system. The SVT provides an automated framework to standardize and manage SAR business processes. It also allows other law enforcement agencies to participate in and benefit from the ISE Share Spaces.

SUSPICIOUS ACTIVITY REPORT (SAR) (Continued)

- **SVT Workflow:**



NATIONAL OPERATION CENTER (NOC)

The National Operations Center (NOC) provides real-time situational awareness and monitoring of the homeland; coordinates incidents and response activities; and, in conjunction with the DHS Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The NOC, which operates 24 hours a day, 7 days a week, 365 days a year, coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

The SEFFC provides the NOC with real time local situational awareness, as well as regional demographics and cultural awareness that they would not normally have available to them. The Southeast Florida area desk also provides the fusion center with a liaison that is able to reach out to other participating state, local and federal law enforcement agencies in the sharing of information.

REQUIREMENT of 28 CODE OF FEDERAL REGULATIONS (CFR) Part 23

28 CFR Part 23 is a *guideline* for law enforcement agencies and is followed by the HSB/SEFFC staff. It contains implementing standards for operating federally funded multi-jurisdictional criminal intelligence systems. It applies to systems operating through federal funding under the Omnibus Crime Control and Safe Streets Act of 1968, as amended.

It provides guidelines for:

- Submission/entry of criminal intelligence information
- Security
- Inquiry
- Dissemination
- Review and purge

Single agency databases, where no information is disseminated or shared outside the agency, do not have to comply with 28 CFR Part 23 requirements. Agencies may collect information through their normal agency investigative processes and maintain that information in their agency files.

As long as that information is only used within the agency, 28 CFR Part 23 does not apply. However, if the information is elevated to a multi-jurisdictional intelligence database where it will be shared with multiple agencies, then it must meet 28 CFR Part 23 requirements.

Entering Names of Individuals and Organizations in the Database

- The officer submitting the information must have enough information from sources, observations, or other investigative efforts to believe the named subject, (individual, organization, group, or business) is involved in criminal activity.
- The subject does not have to be the target of an investigation.
- The subject does not have to have been arrested.
- Officials of the Office of Justice Programs and the Bureau of Justice Assistance have interpreted this provision to apply to all names for which a record or file is created in the database:
- Individuals
- Associates
- Relatives
- Employers

Entering Names of Individuals and Organizations in the Database (Continued)

- Telephone subscribers

- Organizations, groups, or gangs, including extremist groups
- Businesses
- Corporations
- Names of organizations, groups, and businesses, which are part of a criminal enterprise or are a front for criminal activity, can be entered.
- The suspected criminal activity of the subject (individual, organization, group, or business) should be listed in the database.
- Backup documentation supporting the determination of the suspected criminal activity of the subject must be kept in the submitting agency files.
- If an organization, group, or business is documented as a criminal enterprise or front, the members are considered to be reasonably suspected of involvement in the specified criminal activity and can be entered in the database.

Non-criminal Identifying Information

- Under the following circumstances, names of individuals, organizations, groups, or businesses that are not suspected of criminal involvement, but that provide descriptive, identifying information regarding the criminal suspect, may be entered as "noncriminal identifying information."

- The information must be labeled or contain a disclaimer that it is non-criminal identifying information.

- The criminal suspect identified by this information must meet all requirements of 28 CFR Part 23.

- The identifying information cannot be used independently to meet the reasonable-suspicion requirement needed to create a record or file in the database.

What NOT to Enter

- Do not automatically enter names of all individual members of organizations, groups, or businesses without a determination that the organization, group, or business is a criminal enterprise or front.

- Do not create and maintain a record or file on an individual unless the individual is suspected of criminal activity.

- Do not enter names of individuals, organizations, groups, etc., not suspected of criminal activity unless clearly labeled as "noncriminal identifying information."

What NOT to Enter (Continued)

- No information about political, religious, or social views, associations, or activities can be entered unless the information relates to criminal activity and the subject is suspected of criminal activity.
- Information obtained in violation of federal, state, or local laws cannot be entered.

Database Operation

- Provide for the following information to be listed for each criminal suspect (individual or organization) entered in the database:
- Source reliability (reliable; usually reliable; unreliable; unknown)
- Content validity (confirmed; probable; doubtful; cannot be judged) NOTE: Entering the combination of "Unknown Source" and "Content Cannot be Judged" would not meet 28 CFR Part 23 requirements and should be blocked from entry.
- Submitting agency name.
- Submitting officer name.
- Provide for all names (individuals and organizations) entered in the database as criminal suspects to be linked to a criminal activity. NCIC offenses are recommended as a standard, but may not be all inclusive for agency needs. The Office of the General Counsel, Office of Justice Programs, has approved use of the following criminal activity descriptions in addition to the NCIC offenses:
    1. Terrorism
    2. Narcotics
    3. Criminal gang
    4. Street gang
    5. Prison gang
    6. [redacted]
    7. Labor racketeering
    8. Organized crime

- Provide for sufficient data to be entered to identify the subject (date of birth, race, sex, etc.)
- Provide the capability to label or add appropriate disclaimers for each name (individual, organization, group, or business) entered in the database as strictly identifying information, carrying no criminal connotation. Noncriminal identifying information may only be entered as an addition to a criminal suspect's record existing in the database. It is permissible for these names to be searchable.

Database Operation (Continued)

Upon retrieval, it must be clear to the user that the information is noncriminal identifying information relevant to the criminal suspect, activity, or enterprise.

- Provide for entry of the submittal date or the purge date (or both) so that a determination can be made of how long the information has been in the system and when it is due for purge.
- Provide for capturing an audit trail of dissemination of information from the database. A record must be kept of who received the information, the date disseminated, and the reason for release of the information.

Purging Data

- The IOC lieutenant will ensure that the database is continually reviewed and that they provide for purging data in the database, prior to the expiration of the retention period (no longer than five years).
- The purge date of a record may be updated (extended), based on validation by the submitting agency or officer that the subject continues to be suspected of criminal activity.
- Agencies or officers in different jurisdictions may have information on and interest in the same subject(s). Each of the agencies may submit its own entry of the subject to the database. This would result in creating duplicate subject records that show different purge dates. Maintaining duplicate records would prevent the purge of subject information, which may be of interest to agencies in more than one jurisdiction. Prior to purging, the IOC lieutenant will ensure that the other agency or officer has been contacted to verify any duplication of efforts.
- General "tip" information will be immediately reviewed for validity and continually pursued in good-faith for up to 120 days. Should the information not be supportive or related to a criminal case, the appropriate supervisor will review and determine whether the information shall be purged from the database.

Administrative and Security Issues

Security of the systems is the responsibility of the IOC lieutenant, including user identification, passwords, audit trails, or other security hardware and software, to prevent unauthorized access to the information.

IOC lieutenant will oversee a process for audit and inspection of backup documentation supporting participating agency submittals to the database. This process can be conducted by mail utilizing a random sample of submittals and requesting the participating agency head certify compliance of the entry.

All secret or sensitive documents will be destroyed in the appropriate level shredding machine.

Administrative and Security Issues (Continued)

The intelligence report narratives, prepared by investigative unit detectives are the only medium by which criminal intelligence information may be entered into the investigative unit reporting system. It should be prepared when it serves one or more of the following purposes:

a. To record details of proactive investigations into the activities of identifiable criminal groups, individuals, or their associates that lead an experienced police officer to believe that criminality is the objective of their acts or behavior.

b. To record details of criminal investigations or criminal court cases over which the Department does not exercise primary investigative jurisdiction and which relate to individuals or groups participating in, witnessing, or victimized by organized criminal activity.

c. The intelligence report may be used to record the information or to serve as a "cover sheet" conveying a copy of another law enforcement entity's report into the Section's intelligence files.

d. To record details of civil litigation, business transactions, or source of confidential informant reports pertaining to identifiable criminal groups or individuals and/or their associates.

e. The intelligence report is the primary document used to record a onetime intelligence event, a series of such events, or to document the conduct of an extensive intelligence investigation.

IOC shall serve as the central receiving and storage point for intelligence data.

Intelligence information will be provided to the concerned departmental entity by the investigative unit through preparation of an Intelligence Update Report (Annex C).

Evaluated data is cross-referenced to reflect relationships and to ensure complete retrieval in order to provide authorized personnel with the most up-to-date information on criminal activity.

FILE SECURITY [CALEA 43.1.2]

Due to the highly sensitive nature of intelligence files, a separate and secure manual file system is utilized to store intelligence records.

In order to protect the integrity of the system, retrieval of information will be limited to individuals approved by the investigative section supervisor, captain and the Bureau Major.

FILE SECURITY [CALEA 43.1.2] (Continued)

a. Dissemination of information will adhere to the limitations and requirements of Florida Statutes (FSS) 119, Public Records Law.

b. Exceptions to these procedures require the approval of the intelligence section supervisor, captain or Bureau Major.

All original case files and documents will be maintained and secured in the HSB/SEFFC central file system. Investigators may maintain "working copies" of case files, but they shall remain secured.

All sensitive, confidential or secret level material will be stamped accordingly and have the appropriate cover page attached to avoid accidental disclosure.

CASE TRACKING

A case tracking and management system have been developed, in order to establish procedures that appropriately account for all HSB/SEFFC investigations.