

SEMINOLE COUNTY SHERIFF'S OFFICE GENERAL ORDER	NUMBER: G-55
	RESCINDS:
SUBJECT: Domestic Security	
EFFECTIVE: April 12, 1995	
REVISED: March 12, 2024	

Table of Contents:

- I. Purpose
- II. Scope
- III. Definitions
- IV. Responsibilities of All Employees
- V. Dissemination of Intelligence Information
- VI. Division Responsibilities
- VII. Homeland Security
- VIII. Crime Analysis Units
- IX. Planning and Forecasting
- X. Crime Reporting
- XI. Public Safety Camera Network
- XII. Annual Review of Procedures and Processes

I. PURPOSE:

This directive describes the functions of the Domestic Security Division and its role in supporting Sheriff's Office operations and homeland security, which includes the following responsibilities:

- A. Crime Analysis and Research,
- B. Counterterrorism/Homeland Security,
- C. Gang Intelligence and Suppression,
- D. Offender Management,
- E. Inmate Telephone Monitoring,
- F. Comp Stat,
- G. Warrants Administration
- I. Public Safety Camera Network

II. SCOPE:

The Domestic Security Division is responsible for the Sheriff's Office function of collecting, analyzing, and disseminating data concerning criminal activity and suspicious incidents, and intelligence relating to homeland security. The Division gathers criminal intelligence information for the purpose of tracking and identifying emerging crime patterns, and to provide personnel with a central agency intelligence repository. The Division may also be used as a resource to develop personnel (workload) allocation studies.

III. DEFINITIONS:

- A. *Criminal Intelligence Information:*
Intelligence information relates to an identifiable person or group of persons that is collected by the Sheriff's Office to anticipate, prevent, or monitor possible/potential criminal activity. Examples of criminal activity may include information relating (but not limited) to:
1. Domestic or international terrorist groups,
 2. Potential terrorism related activities,
 3. Robbery and burglary rings,
 4. Organized criminal activities,
 5. Criminal gangs,
 6. Outlaw motorcycle gangs,
 7. Sexual offenders.
- B. *Domestic Security Division Intelligence Records Custodian:*
The Domestic Security Division Captain (or designee) is responsible for overseeing the security, maintenance, and purging (destruction) of all written and electronic intelligence reports, records, and files, in accordance with state law and guided by the Federal Code of Regulations related to criminal intelligence information under 28 CFR, Part 23. A Detective and an Analyst will be tasked with the annual purging process.
- C. *Automated Face Recognition:*
The automated search of a facial image in a biometric database, which typically results in a group of facial images ranked by computer-evaluated similarity.
- D. *Public Safety Cameras Network (PSCN):*
Is a system that combines various camera systems and information sources and places it on one platform so the end-user can rapidly identify crimes, safety issues, or any other form of information that can make the community and first responders safer.
- E. *Real Time Crime Center (RTCC):*
A crime analyst unit that can respond rapidly to in-progress events, and utilize various forms of information and intelligence, to provide real time assistance to first responders to improve public safety and situational awareness, enhancing our ability to respond effectively.

IV. RESPONSIBILITIES OF ALL EMPLOYEES:

- A. *Prohibition:*
The collection of criminal intelligence about individuals, groups, or enterprises is limited to criminal conduct and will relate to activities that presents a threat to the community.
1. Information may be collected and maintained only under the following circumstances:
 - a. If reasonable suspicion exists connecting persons with known or suspected criminal activity; and
 - b. The information is relevant to that criminal activity.
 2. Information will not be collected or maintained by the Sheriff's Office based solely on a person's:
 - a. Support of unpopular causes,
 - b. Race, ethnicity, or
 - c. Religious and/or political affiliations.

- B. Employees will not knowingly engage in any illegal activity in the collection of intelligence data, nor shall they direct any other person to engage in the collection of intelligence data through illegal means.
- C. Dissemination of criminal intelligence information is the responsibility of the Domestic Security Division.
- D. Supervisors will routinely inspect collected intelligence information to ensure that it meets the requirements of this chapter.

V. *DISSEMINATION OF INTELLIGENCE INFORMATION:*

- A. Strict control over this process ensures compliance with confidentiality to protect a person's privacy rights, sources of information, and any potential ongoing criminal investigation.
- B. The release of any intelligence information will follow Section 119.071, Florida Statutes, or other safeguards or requirements of law.
- C. Intelligence information will only be released after a complete review is conducted, and it is determined that the release will not jeopardize any ongoing or potential criminal investigation. The release of any information will be in accordance with applicable Florida Statutes.
- D. The Domestic Security Division distributes law enforcement sensitive (LES) information to law enforcement personnel and law enforcement organizations with a need and right to know. Non-LES portions of the information may be shared with the public to generate community support and inform citizens of criminal activity in their communities.
- E. If requested, the Domestic Security Division can conduct certain extensive analyses for the public at a cost (fee) determined by the Sheriff's Office. These analyses are performed by the division as a secondary duty to regular Sheriff's Office business.

VI. *DIVISION RESPONSIBILITIES:*

- A. The Domestic Security Division ensures the Sheriff, and his command staff are briefed on crime patterns, crime trends, or other information in a timely manner. Briefings may be verbal, delivered at a scheduled meeting (if not urgent), or in written form.
- B. The Division produces a weekly and monthly crime report which is disseminated throughout the Sheriff's Office (it may also be distributed to other law enforcement agencies that request it).
- C. The Captain (or designee) will attend crime analysis or intelligence meetings and will participate in related task forces as approved by the Sheriff. As necessary, and as approved by the Domestic Security Division Captain, participation in these task forces will include the collection, processing and sharing of information and intelligence as it relates to criminal investigations and homeland security.
- D. Reporting, collecting and/or documenting information will be accomplished using the Café Program and other supporting systems. Intelligence information will be maintained in other systems as required in 28 CFR, Part 23.
- E. Procedures for Using Intelligence Personnel or Techniques:
 - 1. The Domestic Security Division can provide information to help operational personnel address tactical, crime control, and prevention objectives by identifying and analyzing a criminal's methods of operation, providing crime pattern recognition, and furnishing

analyses of data from field interrogations and arrests.

2. The Division may also assist the agency in long-term planning efforts by enhancing the technology of the Sheriff's Office improving methods of information sharing, and through identifying Prolific Offenders in the community.
3. Crime analysis or intelligence studies conducted by the Domestic Security Division may be requested by operations personnel by completing a *Crime Analysis Request Form* on the Sheriff's Office intranet.

F. Procedures for Using Facial Recognition Programs:

1. SCSO may utilize facial recognition for law enforcement investigations requiring identification or verification of subjects where a digital image is available. Facial recognition searches and comparisons may be performed through a web-based browser and is to be used to assist in law enforcement investigations. Information found through a facial recognition search is to be considered a "lead" for further investigation.
 - a. Sheriff's Office users may access approved facial recognition programs from SCSO or approved websites.
 - b. All users are required to complete the online training modules prior to gaining access to programs utilized by the Sheriff's Office, and the end user must demonstrate competency with the facial recognition process.
 - c. All users must adhere to the requirements set forth in the training provided to the user and outlined by the vendor. Users must also comply with the CJIS Security Policy to include the security of the data and information as well as the exchange of any such data or information.
 - d. Users shall include a reason for search. This reason shall be the associated case number for the subject of the facial recognition search.
 - f. Facial Recognition is an investigative tool and any law enforcement action taken based on a submission shall be based on the requesters own identity determination and not solely the results of a search. Any information found through facial recognition search is for "lead" purposes only. Once a "lead" is developed, it is the responsibility of the requester conducting the investigation to confirm the identity of the subject in the image and take law enforcement action only upon their own independent identification.
 - g. All facial recognition platforms are subject to audit for statistical reporting and to confirm the use follows agency policy. All user activity is logged.
 - h. If a user receives a potential match and requires facial verification of the match, the user shall contact their supervisor and / or another experienced user for assistance. If no match is found, the user shall utilize other investigative methods to determine identity.
2. General Guidelines:
 - a. Facial Recognition will only be used for official law enforcement investigations.

- b. Crime Analysts and Detectives of the Seminole County Sheriff's Office may utilize their assigned cellular phone or digital camera to capture face imagery of a subjects of interest.
- c. Submission of facial images to facial recognition programs for comparison (probes) may be in JPG, BMP, and PNG file Formats. Images can be obtained through the following means:
 - i. The subject is in a public area;
 - ii. The subject is lawfully detained; or
 - iii. Consent.
- d. Individuals will not be physically detained and physical force will not be used for the purpose of taking a photograph for facial recognition. Deputies should ask for consent; this does not preclude a deputy taking the photograph of a person in a public place provided the deputy has not hindered the movement of the person.
- e. All photographs, and search activity submitted to facial recognition programs are logged and subject to audit.
- f. All Facial recognition investigations will be documented in the corresponding CAFÉ report as an investigator note.

3. Use of Facial Recognition:

- a. Crime Analysts and Detectives of the Seminole County Sheriff's Office may utilize facial recognition solely for law enforcement purposes and these programs are not to be used for public use or dissemination.
- b. All Crime Analysts and Detectives are required to use their personal log in credentials when utilizing a facial recognition program.
- c. All image submissions and comparisons must meet the following criteria:
 - i. Reasonable suspicion that the subject being searched is in fact a suspect, person of interest, witness, or victim of a crime;
 - ii. To intervene in life-threatening emergencies.
 - iii. To locate a missing person (there must be an associated Agency Case Number);
 - iv. To determine the identity of individuals who are unable to communicate their identity; or
 - v. To prevent or investigate the crime of terrorism as defined by 18 U.S. §2332b or Florida Statutes Section 775.30.
- d. Any information found through facial recognition search is for investigative lead purposes only, and this information may not be shared to an unauthorized entity, agency, or person.

- e. Information that is obtained through a search will be maintained in accordance with the Sheriff's Office open investigation policy and our intelligence management policy.
 - f. Searches cannot be conducted to track or identify individuals engaging in political, religious, or other protected forms of free speech or expression.
4. Maintaining and updating status of submitted photographs to facial recognition programs
- a. The Records Section is responsible for ensuring that records which have been ordered sealed or expunged have been removed from facial recognition programs.
5. Auditing
- a. The Analyst Supervisor will be appointed to maintain user access and authorizations in accordance with the agreement between Seminole County Sheriff's Office and any authorized Facial Recognition Program vendors.
 - b. The Analyst Supervisor will perform audits that consist of reviews for user access and proper use. The audit logs will be stored on site for a minimum of 1 year.
 - c. The Analyst Supervisor will notify the Facial Recognition Vendors if required by the Agreement with said Vendor within 10 business days if audit findings include, but are not limited to:
 - i. Unauthorized access
 - ii. Searches that do not comply with the constraints of the law and the agreement between the Seminole County Sheriff's Office and Facial Recognition Vendors.
 - iii. Other items that are deemed unusual activity
 - iv. Any notification of non-compliance should include the username, date, time, and case number.
6. Violations of Agreement
- a. Any violation of these guidelines will result in immediate revocation of the offending user's access to Facial Recognition programs. Additionally, all violations of these guidelines shall be reported to the Captain of the Domestic Security Division as soon as the violation is discovered.

G. Pawn Compliance and Property Recovery responsibilities:

- 1. The goal of ensuring pawn brokers and secondhand dealers comply with the law is to ultimately reduce the likelihood of stolen property transitioning through such businesses

and to increase the likelihood that stolen property is recovered by law enforcement.

2. The Domestic Security Division and SNP Region Detectives will provide the following to SNP and other law enforcement agencies:
 - a. Familiarization training on PAWN records systems, applicable Florida Statute, and investigative techniques as it relates to pawn shops and second-hand dealers.
 - b. Analytical support necessary to identify frequent or suspicious pawns.
 - c. Detectives to support inspection and compliance operations.
 - d. Analytical support to link suspects involved in dealing in stolen property cases.
 - e. Crime, intelligence, and trend reports as it relates to pawn shops and secondhand dealers.
3. SNP Region Detectives will organize, conduct, and document all inspections related to Pawn Shops and Secondhand Dealers.
4. Scheduled meetings will be held between Sheriff's Office Detectives and municipal detectives within Seminole County to develop a systematic approach to PAWN shop/Secondhand Dealer inspections.
5. Inspections of PAWN shops/Secondhand Dealers in unincorporated Seminole County is primarily the responsibility of SNP Region Detectives, but can be conducted by trained SWORN Sheriff's Office employees.
6. Inspections of pawn shops/second-hand dealers in municipalities are the responsibility of that specific jurisdiction, but if assistance is requested or needed, the sheriff's office will provide such assistance.
7. If through an inspection a pawn ticket is determined to have errors, it is the responsibility of the pawn shop/second-hand dealer to immediately correct the ticket and resubmit.
8. Sheriff's Office employee who discovered the error with the ticket will review the corrected ticket to ensure the proper corrections have been made.
9. Continuous ticket errors from the same pawn shops/second-hand dealer should be documented and could result in enforcement action.

VII. HOMELAND SECURITY:

- A. In addition to its other functions, the Counter Terrorism Unit of the Domestic Security Division is the Sheriff's liaison to law enforcement agencies, task forces, and other organizations for the exchange of intelligence information regarding foreign and domestic terrorism. Association with these entities facilitates information sharing and assists in the multi-jurisdictional preemption of terrorist acts or events.
- B. The Counter-Terrorism Unit:
 1. Collects and compiles terrorism related intelligence information from various sources within the Sheriff's Office, such as confidential sources and from the community.
 2. Reports and relays terrorism intelligence to task forces in which it participates, that include:

- a. Joint Terrorism Task Force (JTTF) and Safe Streets, (overseen by the Federal Bureau of Investigation), and/or
 - b. Central Florida Intelligence Exchange (CFIX) (overseen by the Florida Department of Law Enforcement):
 - (1) Deputies and/or civilian support staff are assigned to assist task forces.
 - (2) Information gathered and/or distributed by task forces may be expanded as necessary to address on-going crime trends that affect multiple jurisdictions.
- C. As necessary, the Counter Terrorism Unit compiles and distributes confidential homeland security reports. These reports may be distributed by protected email, regular mail, or if they contain information of an exigent or sensitive nature, personally delivered (hand-carried).
- D. Information will be vetted to ensure facts are objectively and accurately reported. Supporting data should be included, if necessary, to the report, and if it does not threaten an on-going or potential investigation.
- E. The Sheriff's Office public website will be used to provide terrorism awareness information to the public and the media. As necessary, the Counter Terrorism Unit will advise the Public Information Officer to issue a public awareness release to the media and the community.
- F. The Domestic Security Division Captain will keep the Sheriff informed, through the chain of command, of all pertinent information relating to current or potential terrorist activity in the Central Florida area. The captain may bypass the chain of command to inform the Sheriff of emergency situations; however, the captain will inform the chain of command as soon as practical.
- G. Employees having information that might affect Sheriff's Office homeland security initiatives should report it to the Counter Terrorism Unit as soon as possible.

VIII. CRIME ANALYSIS UNITS:

- A. The Domestic Security Division is staffed with four (4) Crime & Intelligence Analyst Units: Crime Analysis, Warrant Analysis, Corrections Intelligence Analysis, and Real Time Crime Center (RTCC – Staffed when work assignments and schedules allow).
 - 1. The Crime Analyst Units use specialized computer software to provide for the secure collection and analysis of crime data and information.
- B. The Crime Analyst Units process and examine data to identify and interpret criminal activity to enable the development of strategies that enhance law enforcement service activities, link suspects to crimes, and support command staff functions.
- C. Information is used to pinpoint potential problem areas and identify suspects. The Crime Analyst Units document the temporal and geographic distribution of selected crimes and analyses may include, but are not limited to:
 - 1. Frequency by type of crime,
 - 2. Geographic factors,
 - 3. Chronological (temporal) factors,

4. Victim and target descriptors,
 5. Suspect descriptors,
 6. Suspect vehicle descriptors,
 7. Modus operandi factors,
 8. Physical evidence information, and
 9. Community policing strategies and problem oriented policing initiatives (SARA), or to develop community policing crime suppression strategies.
- D. In addition to the above, the Crime Analyst Units attempt to:
1. Identify developing crime patterns or trends.
 2. Aid in the assembly and comparison of specific crimes to those committed by suspects already in custody.
 3. Identify similarities among different offenses and reveal commonalities and patterns in the characteristics of current crime problems.
 4. Produce computer generated printouts (including graphs, maps, and other visual displays) indicating the location of crimes by types and times, which may include modus operandi factors, suspect information, victim, target descriptions, and property loss information.
 5. As needed, generate a consolidated report containing known information to develop and provide guidelines and/or direction to prevent future crimes and apprehend suspects.
- E. Data Collection
1. Crime Analysts will use the following resources to collect information to include, but not limited to:
 - a. Official agency reports (arrests, offenses, intelligence, field contacts, traffic violations),
 - b. CAD data,
 - c. Internal databases,
 - d. Intelligence databases,
 - e. Outside Law Enforcement intelligence reports or bulletins,
 - f. Open internet sources, and
 - g. Social media.

IV. PLANNING AND FORECASTING:

- A. By identifying crime patterns or trends through statistical analysis the Crime Analyst Units may be able to determine the optimum strategy, tactics, and number of personnel necessary to deal with a problem or situation.

- B. Intelligence led policing and/or crime analysis information may be used to develop problem oriented or community policing crime suppression strategies and provide staffing and resource projections for multi-year periods.
- C. The Domestic Security Division assists in developing long-term planning efforts in tactical strategies, budgeting, and other administrative activities. Factors that may be considered include the analysis of crime trend data by type of crime, offender characteristics, and time and geographic location.

X. CRIME REPORTING:

- A. Crime reports may include information such as Comp Stat, Snapshot, current crime trends, prolific offenders, hot spot areas and divisional progress as it relates to ongoing annual goals and projects addressing crime and crime prevention.
- B. Comp Stat Reports provide crime analysis information and other specified data to agency components and command personnel. The report encompasses activities of all organizational components to aid in planning or forecasting long-range agency needs.

XI. PUBLIC SAFETY CAMERA NETWORK

- A. The Domestic Security Division will utilize a Public Safety Camera Network (PSCN) to enhance the safety of the community and first responders. The PSCN platform will enable connectivity with other forms of data to enable a faster information sharing from the Crime Analyst Units to first responders.
- B. Access to the Public Safety Camera Network (PSCN) will be made available to various first responders to include Law Enforcement, Fire Rescue, and Emergency Management. The Domestic Security Division will provide access to the PSCN through administrators and in various permission levels. Permission levels will be created by the Domestic Security Division, and they will be adjusted as needed for the event that is being addressed. Administrative access will be maintained by the Domestic Security. The Domestic Security Division will manage employee access to the PSCN for the Sheriff's Office, The Domestic Security Division can suspend or cancel access to Sheriff's Office personnel if misuse is suspected or occurs.
- C. Users will be given access to the Public Safety Camera Network (PSCN) through both the web and mobile applications, giving them access to numerous information sharing features. All users of the PSCN can utilize the PSCN for legitimate public safety purposes only, and only while on duty. Users can send and receive direct messages (text, images, and video) with other users, the Crime Analyst Units and other first responder that are participating in an event. The user can activate GPS monitoring from their mobile phone, allow other users, and the RTCC to monitor their location and other first responders. Members of Domestic Security Division can utilize the PSCN for demonstrations or training.

All accounts may be audited at any time. Any misuse of the PSCN either on a PC, Laptop, or Mobile Phone will result in revocation of access privileges and discipline.

Camera Registry and Camera Integration is the process of utilization of community cameras to enhance the PSCN. Camera Registry and Camera Integration will be managed through the Domestic Security Division and the connectseminolecounty.com page.

Camera Registry is registering your camera with the Sheriff's Office and other law enforcement agencies within Seminole County. This registry allows Detectives to know the locations of cameras,

and that the owner of that camera has indicated that they will share the information with law enforcement.

Camera Integration permits the owner of the cameras (businesses, government) to integrate their cameras' feed into the PSCN. The cameras can be integrated into the PSCN through various methods and the donor of the camera feeds can chose the way they are integrated (active all the time or call driven with three priority levels.)

- D. Training will be conducted by or organized by the Domestic Security Division.
- E. Video evidence that is recorded from a camera on the PSCN platform can be stored in evidence.com directly through the PSCN platform. Any video not identified as evidence will be held for thirty (30) days and then deleted from the PSCN platform.

XII. ANNUAL REVIEW OF PROCEDURES AND PROCESSES:

- A. Based upon input from division personnel, the Division Captain will continuously review operational processes and procedures to ensure effectiveness and consistency in operations, including the quality and quantity of information being received and/or disseminated by the Division.
- B. Annually, the Division Captain will report on the current status of Division goals, objectives, and related procedures and processes in its annual goals and objectives statements. In addition, the captain will review this directive and require it to be revised, if necessary, to reflect any changes in procedures or processes. This annual policy review will be automated through PowerDMS.