

TITLE: INTELLIGENCE CENTER PROCEDURES

CODIFIED:
69.4

EFFECTIVE:
09/15/17

RESCINDS/AMENDS: 0

PAGES:
12

PURPOSE

This document is designed to provide an outline and protocols for personnel staffing the Intelligence Center and to the analysts that assist Intelligence Center personnel during operational or critical incidents in the Criminal Intelligence Center.

DISCUSSION

As a critical section of the Criminal Intelligence Center, the Intelligence Center's mission is to provide our law enforcement personnel in the city and our other law enforcement partners throughout the nation with timely and accurate information and intelligence regarding critical incidents and significant public safety events. The Intelligence Center is the eyes and ears of the Santa Fe Police Department; the most critical operational element within the center. It is responsible for recognizing significant public safety events locally, nationally, and globally. It plays a key role in helping the center achieve its goal to prevent, reduce, and disrupt crime and terrorism through the early warning of all-crimes, all-hazards, and all-threats. The Intelligence Center also assists in the support of critical incidents, emergency responses, and

investigations. The Intelligence Center is where real time analysis begins; therefore, it is critical that personnel assigned to the Intelligence Center are actively engaged in monitoring events and activities locally, regionally, and throughout the nation and the world. The personnel staffing the positions in the Intelligence Center have the following responsibilities:

- (1) Maintaining situation awareness of events locally and throughout the world;
- (2) completing time sensitive requests from our vetted partners;
- and, (3) coordinating the dissemination of information, as delineated in this document.

The Santa Fe Police Department Intelligence Center does not engage in the collection or storage of information or intelligence unless there is reasonable suspicion to believe that a person, or a group, is engaging in or is about to engage in criminal activity. 28 CFR Part 23 is a guiding document for all law enforcement agencies pertaining to criminal intelligence systems.

Adherence to 28 CFR Part 23 is of utmost importance to the center, as is the protection of privacy, civil liberties, and the right of persons or groups to engage in constitutionally protected activities.

DEFINITIONS

The following words and concepts are important to note:

Intelligence – The product of an analytic process that evaluates information collected from diverse sources, integrates the relevant information into a cohesive package, and produces a conclusion or an estimate.

Critical Incident – Situations that present a risk of significant bodily harm, property damage, or

are unusual in nature, and a law enforcement agency is involved in some capacity.

Significant Public Safety Event – Events that cause or could cause serious injury or loss of life. Events that have a major impact on quality of life, negatively impacts a business community, or affects critical infrastructure. Law enforcement may or may not be involved.

PROCEDURE

A. General Duties and Responsibilities – Intelligence Center Personnel

1. Coverage of phone calls: The Intelligence Officer phone line is **505-955-5219**. The general Intelligence Center phone number is 505-955-5038. These phones must be answered at all times; there is no margin for error.
2. TIPS: This service/application is to be monitored and responded to at all times in the Intelligence Center during operating hours;
3. Monitor the Computer Aided Dispatch (CAD) for all priority 1 and 4 incidents.
4. Monitor CAD for additional calls (non-priority 1 and 4).
5. Monitor police and emergency response radio channels.
6. Notify the CID Captain or his/her designee when required (see section D)
7. Notify the OIC & CID Captain by email (see section D)
8. Notify the appropriate school district security agency when a police call occurs within the agency's jurisdiction (e.g. SFPS, CHS, SFHS, SMHS, SFCC, St. Johns, etc.) or occurs in the

immediate vicinity and the call will have an impact on normal school or facility operations.

9. Disseminate non-emergency requests (i.e., not requiring immediate attention) to appropriate personnel (e.g., analyst, investigators, supervisor, etc.)
10. Disseminate emergency requests (i.e., immediate attention type) that require a Tactical workup to an analyst. Record in the Intelligence Tracking System as a Tactical workup request (See Tactical Workup below).
11. Disseminate/update law enforcement personnel on-scene of events with information, either requested or obtained.
12. Disseminate Alerts, Advisories, and Notifications of officer safety information, critical incidents or significant public safety events generated or received.
13. Coordinate with the 911 Communications Supervisor, via phone (505-428-3710), and OIC, if necessary.
14. Document incoming intelligence, notifications, and other information in the appropriate log.
15. Monitor local and global events via media sources available (e.g., local channels, Internet, CNN, Fox News, etc.)
16. Brief in-coming supervisors and relieving personnel on specific and/or active incidents, or when breaking.

B. Crime Analyst Duties and Responsibilities (Assisting the Intelligence Center)

1. Receive directed assignments and requests for workups from the CID Commander, including Tactical workups (see below).
2. All available Intelligence Center personnel are required to assist with the requirements of the Tactical workup.
3. Disseminate to the Intelligence Center information on unusual events, including major crimes (e.g., shootings, aggravated robberies) in order to ensure that the Intelligence Center is aware of events and trends occurring throughout the region.
4. Provide results of workups to Intelligence Center personnel for dissemination or directly to the requestor. Provide relief to the Intelligence Center, when necessary.
5. Maintain situational awareness as an aid to Intelligence Center personnel.

C. Notifications

1. The communication of officer and public safety information, and major crimes and events are to be made to all members of the center, operational personnel and our partners within the County of Santa Fe and State of New Mexico.
2. Notifications are to be made via the current email distribution groups and telephone lists; and
3. Members should be aware that not all law enforcement personnel have smartphones; i.e., Blackberries, Droids, iPhones, etc.; therefore, in addition to the e-mail, you are to phone the on-duty Shift Lieutenants and pass on any information to him or her, if necessary.
4. In the event of an incident that requires notification to multiple persons and dissemination of information will be

communicated in accordance with the Department's policies and procedures.

D. Intelligence Unit (CIU) Notifications

1. The CID Captain, OIC, and CIU must be immediately notified, by phone 24/7, of the following incidents:
 - a) Confirmed "hits" on the Violent Gang / Criminal Organization subjects (see Section K),
 - b) Suspicious subjects in custody or are being detained, or cannot be identified,
 - c) A bomb threat to any public facility,
 - d) A bomb threat to an area school or a plot to harm or injure students (e.g., Columbine),
 - e) Any Suspicious Activity situations
 - f) Any situation involving a person(s) conducting surveillance at any location to include critical infrastructure.
 - g) Unattended bags or suspicious packages.
 - h) Any threat to national security.
 - i) Any situation involving suspicious activity indicating a potential narcotics or terrorism nexus.
2. In addition, the CID Commander & OIC must be emailed, of the following incidents:
 - a) Any of the above phone notifications, as a follow-up,
 - b) Arrest of any person identified by CIU,
 - c) Arrest of any person identified as an employee of a law enforcement agency, or
 - d) Any time when directed by a supervisor.

Note: Any email will be copied to All SFPD personnel, to include Supervisors & Analysts.

E. Documentation of Phone Calls/Notifications/Responses/Requests

1. All activity in the Intelligence Center shall be documented in the Intelligence Tracking System with no exceptions, including but not limited to:

- a) All calls coming into the Intelligence Center on any phone, cellular or landline, requesting support or information, will be the subject of an entry in the Intelligence Tracking System,
- b) Phone notifications that the Intelligence Center makes to any other agencies will be entered in the Intelligence Tracking System,
- c) All email requests and responses for support or information will be the subject of an entry in the Intelligence Tracking System

2. Additional entries in to other tracking and record systems are required (e.g., Suspicious Activity Reporting, Field ID cards, etc.), if necessary.

F. Advisories/Alerts

1. Advisories and Alerts are the mechanism by which the Intelligence Center communicates notifications, in mass, to pre-identified personnel, and via e-mail groups. The e-mail groups are maintained under the direction of the CID Commander or his/her designee, and are constantly updated, as required. Intelligence Center personnel or personnel assisting the Intelligence Center are required to send out these notifications as directed by this protocol.

2. Advisories and Alerts will be accurate and professional in appearance and content. All information should be proofread by other Intelligence Center personnel or an analyst prior to authorization and distribution.

3. Authorization and Authority

a) All information received from another agency shall be distributed according to this protocol, unless the sending agency has placed special restrictions on the information or document; in this case, dissemination shall be made with the authorization of the CID Commander.

b) If there is any question as to when an alert or advisory should be issued, consult the CID Captain or his/her designee.

c) All information is released with the approval and under the authority of the CID Captain or his/her designee.

4. Types and Differentiation:

a. Alert – an e-mail that does or may require immediate attention, including:

- (1) Federally-generated time-sensitive threat information
- (2) Officer safety information
- (3) Amber Alert
- (4) Wanted – Armed and Dangerous
- (5) Silver Alert
- (6) Stolen Law Enforcement Equipment
- (7) Stolen Weapons or Explosives
- (8) Any information where the threat to life, property or public safety in general is imminent — can be an “Advisory” category that should be enhanced to an “Alert”.

b. Advisory – an e-mail that does not require immediate attention. It is intended to provide information, advice or situational awareness.

- (1) Wanted Subject
- (2) Missing Person

- (3) Traffic Advisory
- (4) Weather Advisory
- (5) Situational Awareness
- (6) Stolen Vehicles
- (7) Trends & Tactics
- (8) Homeland Security Bulletin
- (9) Public Health Bulletin
- (10) Worldwide Breaking News (See Section H)
- (11) General Law Enforcement Information
- (12) Any information where there is not an imminent threat to life, property or public safety.

Note: if Intelligence Center personnel or an Analyst has any questions or concerns regarding the release of information, consult the CID Captain.

5. Format:

a) All alerts and advisories shall be released on the authorized Criminal Intelligence and Analysis Unit templates — this includes the distribution of email and hardcopy information.

b) Information received from another agency in the form of an attached file or document shall retain its original format and be distributed or attached to an email according to this protocol.

c) Information received from another where the information is not organized or formatted in a professional manner maybe transferred to the authorized Criminal Intelligence and Analysis Unit template.

d) The template will contain:

- (1) The SFPD logo/graphic

(2) The Category (e.g., Wanted Subject, Situational Awareness, Stolen Vehicle, etc.)

(3) Region (Area where the incident, person, activity resides)

(4) Restriction

(5) Incident Type

(6) Distribution

(7) Intel Case Number

(8) Agency Case Number

(9) Date

(10) Time

(11) Source Reliability

(12) Content Validity

(13) Details – Subject or Incident information; the details/body will provide basic information, including:

(a) Date, Time, Address of the event;

(b) Brief narrative;

(c) Intelligence action taken (e.g., SFPD or other unit notified, identify by name or call sign)

(d) Sender's name and contact information.

(14) Authority (should be the on-duty supervisor)

(15) Confidentiality Statement (current approved version)

Note: Because these advisories and alerts may be sent to non-law enforcement agencies, the body/details of the e-mail will use plain language (i.e., no 10 or disposition codes).

6. All Criminal Intelligence Center distribution will be sent using the "SFPDINTEL" email group.

7. The subject-line of the email for all Advisories and Alerts will include, in the following order:

- a) ADVISORY or ALERT in capital letters,
- b) A hyphen (-),
- c) Intel Case Number, if applicable,
- d) Category (e.g., Wanted – Armed and Dangerous, Situational Awareness, etc.)

8. Non-Law Enforcement Advisories and Alerts

The majority of the Criminal Intelligence Center distributions will be to law enforcement personnel, using the Restriction "LES/FOUO" or Law Enforcement Sensitive/For Official Use Only; however, public and non-law enforcement distributions of Advisories and Alerts will never include:

- a) The identity, date of birth, or social security number of a juvenile suspect.
- b) The identity, date of birth, or social security number of any victim.

9. Follow-up Advisories and Alerts

An additional distribution is required when new significant information comes to light. The follow-up will include the initial correspondence in the body/details, along with the newer information placed on the top.

10. Final Advisories and Alerts

Once an Advisories and Alert has been distributed, a copy of the email, PDF, Word Document or other file format will be saved to the Intelligence Center directory.

G. Intelligence Center Emails/Responses

1. SFPDINTEL emails and responses are the mechanism by which the Intelligence Center communicates information or requests to both law enforcement and non-law enforcement personnel. Intelligence Center personnel or personnel assisting the Intelligence Center are required to send out these emails and responses as directed by this protocol.

2. Emails and responses will be accurate and professional in appearance and content.

All information should be screened to ensure that it meets privacy guidelines and is as directed by this protocol prior to authorization and distribution.

3. All Criminal Intelligence Center distribution will be from the "SFPDINTEL" email group.

4. Authorization and Authority

a) All information received from another center shall be distributed according to these protocols, unless the sending agency has placed special restrictions on the information or document; in this case, dissemination shall be made only with the authorization of the CID Commander or his/her designee.

b) If there is any question as to the content of an email or response, consult the CID Captain or his/her designee

c) All information is released with the approval and under the authority of the CID Captain or his/her designee.

5. Format:

a) All Intelligence Center emails and responses will be sent using the "SFPDINTEL" email group. Information originating from another source or agency received in the form of a file or

document shall retain its original format and be attached to the email for further distribution.

b) The email will contain:

- (1) A subject-line with a brief content description,
- (2) A salutation, along with the name and rank,
- (3) The appropriate content,
- (4) A valediction, along with the senders information, including title and phone number,
- (5) Authority (should be the on-duty supervisor),
- (6) The authorized Confidentiality Notice and appropriate disclaimer shall be placed at the bottom of the email.

Note: Because emails may be sent to non-law enforcement agencies, the body/details of the e-mail will use plain language (i.e., no 10 or disposition codes).

6. Non-Law Enforcement emails and responses

The majority of the Intelligence Center's emails will be to law enforcement personnel, using the Restriction "LES/FOUO" or Law Enforcement Sensitive/For Official Use Only; however, public and non-law enforcement emails and responses will never include:

- a) The date of birth, social security number, or any personally identifying information other than the first and last name of an arrested or wanted person;
- b) The identity, date of birth, or social security number of a juvenile suspect; or,
- c) The identity, date of birth, or social security number of any victim.

7. Follow-up emails and responses

An additional email or response is required when new significant information comes to light. The follow-up will include the initial correspondence in the body/details, along with the newer information placed on the top.

8. Final emails and responses

Once an email or response has been distributed, a copy of the email, PDF, Word Document or other file format will be saved to the SFPD Criminal Intelligence directory.

9. Federal, State or Local Threat Information

Upon receipt of information generated by any agency regarding a threat to national security, the Intelligence Center will obtain all available information and make notification to the CID Captain or his/her designee as defined in Section D, Intelligence Unit Notifications.

The threat information will prepare an alert or advisory to all distribution groups. If no additional relevant information (e.g., terrorism, DTO, local or regional nexus) comes to light, no other action needs to be taken, other than monitoring.

The goal is to inform members of the Department and the region of the receipt of time-sensitive threat information received by the SFPD Intelligence Center.

H. Worldwide Breaking News

Upon learning of a major worldwide event, the Intelligence Center will prepare an alert or advisory to all distribution groups. If no additional relevant information (e.g., terrorism, DTO, local or regional nexus) comes to light, no other action needs to be taken, other than monitoring. Examples of events that would fit into this expectation are, but not limited to:

1. Plane crashes worldwide

2. Hijacked aircrafts or cruise ships worldwide
3. Nationwide major shooting events (e.g., Columbine, Fort Hood, Washington State Police shooting)
4. Major industrial accidents

The goal is to inform members of the Department and the county that a major event has occurred and it is being monitored by the Santa Fe Police Department Intelligence Center.

I. Unattended Bags or Suspicious Packages

1. Upon learning of a call involving an unattended bag or suspicious package, the Intelligence Center will obtain the available information and make notification to the CID Captain or his/her designee as defined in Section D, Intelligence Unit Notifications.
2. The Intelligence Center will monitor the call. If no additional relevant information (e.g., terrorism or drug trafficking organization nexus) comes to light, no other action needs to be taken, other than monitoring the call to its conclusion.
3. If relevant information (e.g., terrorism or drug trafficking organization nexus) comes to light, the Intelligence Center will prepare an Advisory.

J. Officer Involved Shootings

Upon an officer involved shooting, the Intelligence Center will send an email to the "SFPD EXEC STAFF" and "SFPD COMMANDERS" groups, as an advisory of the incident. Use the following as a template for the format of that email:

1. CAD Event Number
2. Case Number, if issued
3. Location of Occurrence
4. Time of Occurrence

5. Brief Synopsis

6. End with the statement: "This E-mail is for information only. The Intelligence Center is monitoring the incident and will distribute additional information, as required. Please do not contact the Intelligence Center for further details unless your personnel are involved. Thank you."

K. Violent Gang/Criminal Organization File Notifications

1. The VGCOF provides law enforcement with identifying information about violent criminal gangs and criminal organizations and the members of such groups. This information may warn law enforcement officers about the potential danger posed by violent individuals, and allow for the exchange of information about these groups and members to aid criminal investigations. The information listed in this file is investigative/intelligence information that has not been subjected to an independent judicial review.
2. The role of the Intelligence Center is to receive notifications on VGCOF hits, advise the caller to contact the New Mexico All Source Intelligence Center, and notify the CID Captain or his/her designee (via email). A hit may come from a person, DMV, or computer check; therefore, we will receive these notifications from a variety of sources. Upon receipt of a VGCOF hit, the Intelligence Center will:
 - a) Log all information from the hit in the Intelligence Center system, to include the source of the hit (e.g., DOB, license plate, partial name), officer involved and their contact number (for CIU), reason for stop/running plate or person, all information on person or vehicle, if known.
 - b) Assist the initiating party by providing the email or telephone number of the New Mexico All Source Intelligence Center at Intelligence.Fusion@state.nm.us or 505-476-9625, if needed.

c) Notify the CID Captain or his/her designee, via telephone, on confirmed subject hits,

d) Follow-up with an email to the CID Captain or his/her designee, and copy to all Intelligence Center personnel

e) "DOB only hits" will be subject to an email notification to the CID Captain or his/her designee.

The following template will be utilized to assist with documenting, and forwarding

VGCOF hit notifications:

- (1) CAD Event Number
- (2) Case Number
- (3) Officers/Employee's Name
- (4) Officer/Employee ID#
- (5) Officer's Call-sign
- (6) Officer/Employee Contact Number(s)
- (7) Location of Stop
- (8) Circumstances of Contact
- (9) Name of Subject
- (10) DOB of the subject
- (11) SSN of Subject
- (12) ID# of Subject
- (13) Vehicle Description & Plate Number (If applicable)

L. Computer Aided Dispatch (CAD) - Administrative Messages (AM)

Most Patrol Officers responding to, and at the scene of incidents, do not have the ability to

receive Intelligence Center Alerts and Advisories. These members do have the ability to receive Messages within CAD. However, messaging should be used in limited situations only.

Examples of when a message would be appropriate include an ongoing crime spree, or a barricaded subject, when further information is required at the scene. If questions exist about use of messages, personnel should be guided by their supervisor. This notification process should only be used to inform officers of confirmed information relating to a subject, address, or incident. In order to provide information to responding or on-scene officers, the following steps must be taken:

M. Email Groups and Lists

- PD ALL contains a distribution list of all members of SFPD – officers and civilians,
- PD OFFICERS contains a distribution list of all commissioned police officers of SPPD,
- PD OUTSIDE AGENCIES contains a distribution list of all participating law enforcement agencies.

Situations could involve the use of two or more groups, or just 1 of the groups. It is impossible to account for all the possibilities within this protocol. Any questions on the dissemination of an alert or advisory, consult with the Intelligence Center representative disseminating the information.

N. Regional Alert E-Mail Groups

1. The Regional email groups include other law enforcement agencies surrounding the City of Santa Fe, NM, which include; local, state, and tribal territories.

2. Regional alerts will be disseminated, based on the need to share intelligence with the respective Departments and agencies within the region.

3. In cases where questions exist, personnel will consult with the CID Captain or his/her designee on group dissemination.

O. Corporate and Private Security Alert Groups

In order to improve communication between the Santa Fe Police Department Intelligence Center, private security directors, corporate security chiefs, and the City of Santa Fe Convention & Visitors Bureau, this protocol will outline the guidelines for the dissemination of certain information, which is defined in Section P.

P. No Consolidated Criminal History (CCH), Counter-Terrorism, Homeland Security, or criminal intelligence related information will be sent to the Non-Law Enforcement Agencies.

1. A non-law enforcement agency and its personnel will only receive information related to its specific industry. Types of information they can receive includes but is not limited to:

- a) Crime Sprees
- b) Crime Trends
- c) Unattended Bag or Package
- d) Road closures
- e) Security Breaches
- f) Fraud incidents

2. These emails will be limited to the following information: Type of incident (using plain language), property name, time of incident, and a suspect description, if applicable.

Q. Tactical Workup (Packet)

1. The Intelligence Center also assists in the support of critical incidents, emergency responses, and investigations, when a timely response is mandatory.

As part of this, the Intelligence Center is required to assist with the completion of a Tactical Workup on any person, place, or item, when requested by a supervisor, field personnel or a participating agency.

Each request will be unique and dependent upon the situation.

2. The minimum information to be searched are:

- a) Criminal History
- b) Photographs
- c) Address searches
- d) Website and utilities check.
- e) Vehicle

3. As always, officer safety is the priority and databases related to that issue (e.g., gun registration, criminal history) will be searched first, with results immediately provided to contact person in the field. The Intelligence Center will then follow-up with additional intelligence from other databases.

4. All results of the workup will be placed on Santa Fe Police Department "Criminal Intelligence and Analysis Unit Template," prior to dissemination.

5. Research results will never be provided to a personal cell line/email, and must be picked up in person. If exigent circumstances exist, limited details may be sent to a personal cell line or via

email. A DMV photo of a subject may be sent via a personal phone/device.

Upon the completion of the workup, the Intelligence Center will compile an Intelligence Center Report. The original completed report will be forwarded to the requestor, with a copy attached to the Intelligence Center.

R. SWAT Call-Outs

1. The following delineates the Intelligence Center Call-out protocol:

a) The CID Commander or his/her designee and the Intelligence Center personnel will be notified by the group notification system or current notification system whenever SWAT is activated or called-out to an incident.

2. Whenever SWAT is in route to an incident, the Intelligence Center will take the following steps:

a) During non-operational hours, within 60 minutes of the SWAT activation, the Intelligence Center will stand up the call-out contingent and open the Intelligence Center. The Intelligence Center will then begin to gather the details and pertinent information related to the location, person, and items involved in the incident. The Intelligence Center will compile a Tactical Workup and distribute it to the on-scene SWAT Commander and supervisors, as soon as practicable.

b) During operational hours, the Intelligence Center will immediately begin to gather the details and pertinent information related to the location, person, and items involved in the incident. The Intelligence Center will compile a Tactical Workup and distribute it to the on-scene SWAT Commander and supervisors, as soon as practicable.

c) The Intelligence Center will prepare an alert or advisory, unless the on-scene SWAT Commander requests otherwise. A request from the on-scene SWAT Commander must be made via phone to the Intelligence Center and state a specific basis for the request.

d) If the incident dictates, the Intelligence Center will prepare updated alerts or advisories.

e) The Intelligence Center will be responsible for handling the distribution of all alerts or advisories based on established distribution protocols.

f) Upon receipt of the disposition of the incident, a follow-up advisory will be prepared, containing an update of the incident and outcome. The follow-up advisory will be distributed to the group initially emailed by the Intelligence Center.

S. Criminal Intelligence Unit (CIU) and Special Team Callouts (excluding SWAT) – Tactical Workups

1. The Intelligence Center will receive notification from a CIU investigator or special team member, advising that a tactical workup is required.

2. The notification will outline the requirements of the workup and provide one contact person and a phone number.

3. As always, officer safety is the priority and databases related to that issue (e.g., criminal history) will be searched first, with results immediately provided to contact person in the field. The Intelligence Center will then follow-up with additional intelligence from other databases.

4. All results of the workup will be placed on a Criminal Intelligence and Analysis Unit template, prior to dissemination.

5. The results of the workup will be provided to CIU via the identified group. This group contains the SPPD email addresses of the entire CIU.

6. Criminal history results will never be provided to a personal cell line/email, and must only be sent to an SPPD email address. A DMV photo of a subject may be sent via a personal phone/device.

7. The CIU investigator or special team member will be required to call the Intelligence Center to terminate any workup at the point when information/intelligence is no longer needed.

Note: If the Intelligence Center identifies an event that may require a workup prior to a request, a preliminary workup should begin, based on what is known.

T. Intelligence Alert and Advisory Matrix

1. Alert

When directed by a Supervisor:

- a) Terrorist Attack in the United States
- d) Major local incident, with injuries
- e) Local plane crash

2. Advisory

When directed by a Supervisor:

- a) Terrorist Attacks
- b) Global Measles, Influenza, etc. – Outbreaks
- c) Road Closures that could jeopardize safety/welfare of citizens (e.g., chemical spill)
- d) A major crime event or series of events
- e) No Explosive Device/Suspicious
- f) Homeland Security Advisory

g) Attempt to Locate from outside agency Crime Advisory

h) Public Health Advisory

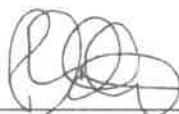
i) Major Vehicle Accident w/ Chemical Spill

j) Transportation Advisory

Note: If a situation is unclear, consult a supervisor: Incident Type Advise/Alert

DRAFTED (rfv) 8/17

APPROVED:



PATRICK G. GALLAGHER
Chief of Police

DATE:

9/15/17
