12-006 Cybercrime, Cyber-related Crime, and Cyber-related Incidents

Los Angeles County Sheriff's Department

FIELD OPERATIONS DIRECTIVE

CYBERCRIME, CYBER-RELATED CRIME, AND CYBER-RELATED INCIDENTS

PURPOSE

The purpose of this Field Operations Directive is to establish procedures for handling cybercrimes, cyberâ€'related crimes, and cyberâ€'related incidents. This FOD also provides instruction for the proper use of newly created statistical codes 551, 552, and 559 which shall be used for the tracking of these incidents.

BACKGROUND

Computers, electronic tablets, smart phones, and related technology have become commonplace in our society. Rapid advances in technology along with the increased number of affordable computer-related devices have caused a rapid increase in the number of individuals using technology for the commission of crimes. In addition, Penal Code Section 13023.5 specifically requires the Los Angeles County Sheriff's Department to gather and report statistical information regarding the use of electronic devices in the commission of various crimes.

Law enforcement personnel need to be aware and recognize when cyber devices might be in use, or have played a part in the commission of a crime. In addition, a working knowledge of how to properly handle these devices is necessary so valuable evidence is not lost or rendered inadmissible in court.

DEFINITIONS

Cybercrime: A crime wherein the internet, computers, mobile communications devices, or any related technology is used as the primary instrument. Examples may include:

- Computer/System Intrusion ("Hacking");
- Computer/System Denial of Service;
- Identity Theft (through use of computers, mobile devices or Internet);
- Child pornography (production, sending, receiving or possessing);
- Illegal/illicit communications with a minor (sexting, enticement);
- Computer Fraud;
- Terrorist Threats; and
- Stalking (646.9(g) P.C.)

Cyberâ€'Related Crime: Crimes wherein the internet, computers, mobile communications devices, or any

related technology were used in its commission, preparation, or furtherance, but not as the primary instrument. Examples may include:

- Physical theft of a computer or device;
- Prostitution advertised online or via text; and
- Flash mob for criminal purpose (riot).

Cyber-Related Incident: Nonâ€‘criminal incidents requiring a police response, or which generates a call for service, wherein the internet, computers, mobile communications devices, or any related technology were used. Examples may include:

- Flash mob for lawful protest;
- Cyber-Bullying (when 528.5 P.C. is not applicable);
- Cyberâ€‘Stalking (when 646.9 P.C. is not applicable);
- Civil damage complaints; and
- Social Media Parties openly advertising the sale/use of illegal drugs (if no arrests made or crime report taken).

Cyber Device: Any electronic device which can be used to create, send, receive, or store digital information, files, photos, text, eâ€‘mail, or any other type of electronic code.

Social media: includes any electronic medium where users may create, share, and view userâ€‘generated content, including uploading or downloading videos or still photographs, blogs, video blogs, podcasts, or instant messages, or online social networking content. Examples may include:

- Facebook;
- Twitter;
- YouTube;
- Instagram; and
- Virtual worlds.

POLICY AND PROCEDURES

The following statistical codes (stat codes) have been developed for the tracking and reporting of cybercrime:

551 â€‘ Cybercrime

552 â€‘ Cyber-Related Crime

559 â€‘ Cyber-Related Incident (nonâ€‘criminal)

These stat codes shall be entered as a secondary stat code on the Incident Report (SHâ€‘Râ€‘49) and DDWS, in addition to the primary crime's stat code.

The SHâ€‘Râ€‘49 has been updated to include checkâ€‘boxes for "Cyber" incidents. The appropriate checkbox shall be used in conjunction with the new 55x series of stat codes.

PATROL STATION PERSONNEL

Desk Personnel

Desk personnel shall dispatch a patrol unit to handle cybercrime, cyber-related crime or cyber-related incidents. The incident's priority level shall be determined in the same manner as other calls for service. It is important to acquire pertinent information from the caller and include it in the narrative of the call.

The Sheriff's Information Bureau's Electronic Communication Triage Unit (SIB eâ€'COMM) will notify station personnel of large parties, demonstrations, or other events that have been advertised on social media systems. Although these notifications are advisory in nature, these types of events could have a detrimental effect on station resources and have the potential for increased violence in the area. They shall be assessed and handled in the same manner as other information that is received by station desk personnel.

Field Deputies

When responding to a call for service or while conducting a field investigation, the following guidelines shall be followed when cyber devices may have been used:

- Ask the victim, witnesses, etc. if a computer or social network media was involved. Document their statements in the report or call clearance;
- Use the appropriate stat/clearance code for the primary crime when clearing the call or drawing an URN;
- Use the appropriate 55x series stat codes as a secondary stat code, as appropriate;
- Check the appropriate checkâ€'box for "Cyber" incidents on the SHâ€'Râ€'49; and
- If no report is taken, use stat code 559 as a secondary clearance code for the DDWS/call, as appropriate.

Guidelines for Seizing Digital Devices

- Under most circumstances, it is extremely important not to manipulate, search for, or otherwise access the data on a cyber-device, especially when suspected evidence is stored or has even been deleted from the device. Doing so will modify date and time stamp information which may be important to the investigation. Precautions shall be taken to preserve the integrity of digital evidence.
- In most circumstances, it is recommended to power off live computers by simply pulling the power cord.
- If a computer (or mobile phone) is password protected, every reasonable effort shall be made to obtain the password from the owner.
- When evidence is located on a networked computer system (i.e., commercial computer network), do not power off the system. Contact Commercial Crimes Bureau's Cybercrimes Detail immediately for assistance.

Notifications and SRD Guidelines

Commercial Crimes Bureau Cybercrime Detail shall be immediately notified by phone or if after hours, SHB, for incidents involving:

- A breach or attempted breach of a Los Angeles County, contract city, or other government computer system;
- Commercial computer networks;
- Cybercrime or cyber-related crimes that are high profile or mediaâ€‘driven; and/or
- ***Active*** network intrusions.

Routine notifications shall be made to the Commercial Crimes Bureau Cybercrime Detail by phone or FAX at [REDACTED TEXT], whenever any of the following incidents occur:

- Arrests for cyberâ€‘related crimes;
- Cyber-related crimes or incidents involving any of the following:
  - Threats;
  - Theft/Fraud;
  - Unlawful Cyber Intrusion (theft, use, destruction of data);
  - Denial of Service;
  - Fictitious online accounts or web sites in the victim's name; and
  - All cybercrime or cyber-related crimes where the victim is a minor (note: Special Victims Bureau, SAFE Team shall be notified of cases involving child pornography and/or crimes related to sexual assaults).

Approving Sergeant

Shall review all reports for cyber (computer, mobile phone or Internet) involvement; ensure the appropriate secondary stat code is used; ensure the checkâ€‘box for "Cyber" incidents on the SHâ€‘R-49 has been selected, if appropriate; and upon approval of the report, ensure an SRD is made to DD/CCB.

Detectives

Shall determine whether or not a computer and/or social media was involved, and ensure the appropriate secondary stat code was used. If necessary write a supplemental report adding the appropriate secondary stat code. When a cyber-related arrest has been made, ensure the appropriate 55x series stat code was used before completing/clearing a case.

Detective Lieutenants

Shall ensure that the case file has been updated with the appropriate use of cybercrime or cyber-related stat codes and supplemental reports.

CONTACT INFORMATION

Commercial Crimes Bureau Fax: [REDACTED TEXT]
Cybercrime Detail Main Office: [REDACTED TEXT]
Cybercrime Detail Fax: [REDACTED TEXT]
Cybercrime Detail Supervisor: [REDACTED TEXT]

Cybercrime Help Desk: [REDACTED TEXT]

Special Victims Bureau, SAFE Team: [REDACTED TEXT]

SIB Electronic Communication Triage Unit (SHB eâ€'COMM): [REDACTED TEXT]

All after hour notifications shall be made through Sheriff's Headquarters Bureau: [REDACTED TEXT]

CITES/REFERENCES

Penal Code Section 13023.5