Portions of this document are deemed by the San Diego Police Department to be records of security procedures and are exempt from disclosure under the California Public Records Act (CPRA), Government Code Section 6254 (f).

San Diego Police Department

TRAINING BULLETIN

A PUBLICATION OF THE SAN DIEGO POLICE DEPARTMENT

DAVID NISLEIT
CHIEF OF POLICE

21-06 SEPTEMBER 29, 2021

RESPONSE TO CYBER-VIGILANTES

I. PURPOSE

This bulletin is meant to provide guidance to sworn members of the Department who respond to radio calls involving private citizens (cyber-vigilantes) who conduct undercover online operations intended to "catch" potential predators who target minors to entice them to illegal sex acts. It serves to provide a standardized response for law enforcement officers and to ensure proper documentation and the procurement of evidence.

II. SCOPE

This Training Bulletin applies to all sworn members of the Department.

III. BACKGROUND

The San Diego Internet Crimes Against Children Task Force (ICAC) has seen a recent uptick in private citizens (cyber-vigilantes) conducting undercover online investigations. ICAC will typically not work with civilians acting as undercover operatives and does not condone such activities because the training involved to conduct these investigations consists of hours of intense legal training. Without that training, well-meaning civilians not only endanger themselves, but also the person they are contacting, as well as the general public.

Furthermore, the actions of the cyber-vigilantes may result in important evidence being suppressed, impeding ICAC's ability to properly and effectively investigate and prosecute these crimes.

IV. PROCEDURES

If an officer encounters a cyber-vigilante who has conducted an undercover online investigation, often resulting in the luring of a possible predator to meet with an alleged child, he or she should do the following:

1. If the alleged suspect **IS present** with the reporting party (cyber-vigilante), complete a miscellaneous report. If the responding officer establishes probable cause a crime has been committed, seize any and all devices used by both the alleged suspect and the reporting party as evidence. Do not search the contents of the devices. If possible, obtain passwords and place the device into airplane mode. Additionally, get accurate contact information for both parties, photos of the involved parties, and detailed statements from both the alleged suspect and reporting party. It is difficult for ICAC investigators to complete thorough investigations and for prosecutors to file charges without this evidence. **DO NOT** make a probable cause arrest for any alleged crime connected to these allegations. Advise the reporting party that law enforcement does not condone cyber-vigilantism due to the inherent dangers to all parties involved. The reports and evidence shall be forwarded to ICAC for further investigation.

2. If the alleged suspect **IS NOT present** with the reporting party (cyber-vigilante), instruct the reporting party to make a CyberTip with the National Center for Missing and Exploited Children at report.cybertip.org. NCMEC is the congressionally-recognized clearinghouse for online enticement information. When a CyberTip has been made, it will be evaluated, deconflicted and sent to the appropriate ICAC Task Force for evaluation.

The evidence produced by these cyber-vigilantes, while disturbing, is often insufficient to establish the elements of these types of crimes. Cyber-vigilantes lack the ICAC-specific training necessary to properly investigate these cases. Furthermore, the activities of these private citizens cyber-vigilantes are oftentimes considered entrapment and can preclude the prosecution of the alleged offenders.

This Training Bulletin does not supersede Department Procedure 3.02.

If you have any questions, please contact San Diego Police **(Deleted – records of security),** San Diego Internet Crimes Against Children, at **(Deleted – records of security)**.