Surveillance Impact Report

ICAC Data System (IDS)
San Diego Police Department

DESCRIPTION

The National Internet Crimes Against Children Task Force Data System (IDS) is a web-based application that provides a secure dynamic infrastructure to facilitate online law enforcement investigations of child exploitation. The program promotes data deconfliction and information sharing between the National Center for Mission and Exploited Children (NCMEC), Internet Crimes Against Children (ICAC) Task Forces, and ICAC-affiliated agencies. IDS also enhances the capability of the Office of Juvenile Justice and Delinquency Program (OJJDP), the head of the national task force, to collect and aggregate data on the extent of child exploitation.

IDS is only used by members of the Internet Crimes Against Children Task Force.

PURPOSE

ICAC Commanders, investigators, and prosecutors access IDS to manage, triage, transfer, and assign CyberTips reported by electronic service providers, law enforcement agencies, social services agencies, and the public. These CyberTips are collected and disseminated to the sixty-one (61) national ICAC task forces utilizing IDS by the National Center for Missing and Exploited Children, the congressionally recognized clearing house for CyberTips.

LOCATION

IDS is a web-based case management tool that can be accessed using many internet-connected devices. Only task force members who have been authorized by the task force commander can access IDS. All transactions are for the furtherance of law enforcement activity.

City of San Diego crime statistics can be viewed at:

- Crime Statistics & Crime Mapping | Police | City of San Diego Official Website.

IMPACT

Only task force members who have been trained and authorized by the ICAC Commander and managers of IDS may use the software. All new users must receive training from IDS before being given access to the system. Only trained investigators are authorized to use IDS to manage CyberTips and casework. Two-factor authentication is required to log in to the system.

ICAC's IDS Surveillance Use Policy safeguards civil liberties and civil rights. Surveillance technology's uses and deployments are not based on discriminatory or viewpoint-based factors. The Department's use of surveillance technology is intended to support and benefit the communities of San Diego while minimizing and mitigating potential impacts on community members' civil rights and civil liberties.

MITIGATIONS

IDS is a web-based case management tool that provides a secured space to transfer case information, including CyberTips, Child Sexual Abuse Materials (images, videos, and text communication depicting the physical and sexual abuse of minors), and casework, between ICAC task forces and their members. Investigators may upload/download information relevant to their criminal investigations to include, police reports, investigator reports, research data, forensic extractions and analysis, imagery, and legal process. That information is made available only to the assigned investigator, certified forensic examiner, and/or prosecutor. Only the ICAC Commander, their designee, or the IDS manager may assign a case and its related data to a member of the task force.

The collection, use, retention, or dissemination of data shall not be used to violate the Constitutional rights of any person or in any manner that would discriminate against any person based upon their ethnicity, race, gender, natural origin, religion, sexual orientation, or gender identity.

The general public has no access to the IDS system or information contained in the ICAC NAS database.

DATA TYPES AND SOURCES

IDS is a web-based case management tool that provides a secured space to transfer case information, including CyberTips, Child Sexual Abuse Materials (images, videos, and text communication depicting the physical and sexual abuse of minors), and casework, between ICAC task forces and their members.

DATA SECURITY

Only task force members who have been authorized by the task force commander and IDS managers can access IDS. Each member is provided a unique identifier. To access the site, a user must log in with that identifier, and an alphanumeric password, and utilize two-factor security measures.

FISCAL COST

There is no cost. This case management tool was designed and is supported by the West Virginia ICAC for use by the National Task Force.

There are no ongoing or personnel costs associated with it.

THIRD-PARTY DEPENDENCE

Data that has been selected and downloaded from IDS is not shared without a court order or other legal proceedings such as discovery. The extracted data is confidential, and there is no third-party access or sharing.

ALTERNATIVES

There are no other programs used by the National Task Force or NCMEC to distribute and manage ICAC-related cases. Without this system, SDICAC would be unable to receive cases to investigate,

unable to deconflict case information, unable to receive or send evidentiary imagery, and unable to transfer cases/information with other ICACs. Without IDS, SDICAC would be operationally ineffective.

TRACK RECORD

IDS is used daily to assign casework, review imagery, and share cases across the task force. IDS is maintained and updated on a regular schedule by the West Virginia ICAC. It is reliable and its program functions work without issue.

PUBLIC ENGAGEMENT AND COMMENTS

On November 8, 2023, at 1800 hours, there was a publicly held meeting in all nine council districts in the City of San Diego. The following surveillance technologies were presented by the San Diego Police Department:

1. Avalex DRV and FLIR-HDc
2. WHOOSTER
3. MSABs Raven Mobile Triage Tool
4. MSABs XRY Mobile Forensic Data Recovery Software
5. National ICAC Data Systems
6. PENLiNK
7. Vigilant
8. Unmanned Aircraft Systems

There were five attendees in District 1. There were zero attendees in District 2. There were zero attendees in District 3. There were zero attendees in District 4. There were zero attendees in District 5. There were zero attendees in District 6. There were two attendees in District 7. There were two attendees in District 8. There were zero attendees in District 9. There was a total of one comment and two questions out of the nine attendees. There was one comment submitted to an online public comment form.

Comment #1:

> These are all technologies that provide advanced safety to each and every citizen of our city. What I am not in favor of is the requirement that these presentations be held in nine locations throughout the City. Staffing so many locations with SDPD and San Diego Fire and Rescue personnel takes these critical First Responders away from their far more important jobs of keeping the City's citizens of San Diego safe. Our police and fire departments are already understaffed. This is a blatant misuse of our resources. Thank you.

Online Comment #1:

> The policy is vague in which instances the deployment of aerial surveillance with no safeguards to prevent misuse of this technology. Without addressing these shortcomings, I cannot support the use of DJI Avata by San Diego PD.

Question #1:

Is the license plate reader data looking for specific cases and/or are all plates looked at to see if they fit a specific case?

Answer:

License plate readers can look for specific plates if they are involved in an active investigation. An investigator can upload license plate information into the license plate reader operating system and set an alert to notify the San Diego Police Department when the license plate is read. Investigators may upload license plate information into the license plate reader because the plate may be associated with a crime, a missing person, or an identified suspect. The SDPD Communications Division may dispatch officers to investigate a hit on a license plate reader entry. Dispatched officers will confirm that the license plate was identified by the reader correctly before any action is initiated.

Question #2:

I think it is very important that San Diego advances in technology but is also aware of some of the issues that come from having so many technologies. The questions that I have are in three phases. One has to do with lobbying from technology companies to government agencies. I sometimes have concerns over technology companies going to conferences and lobbying Fire Chiefs, Police Chiefs and many other officials during those conferences. How does the City protect itself through accountability on that?

The second is data analytics. I worked in data analytics before and one of the things that I do see is sometimes data analytics has missing information. How do we account for that through the data information that we are gathering that way we can make proper information when citizens don't report crimes that don't add up to the statistics?

The third is, what's going to happen next with all this technology?

Answer:

In terms of lobbying, there are a couple of different processes now in place. The Police Department had a process before the Privacy Advisory Board and a process that took place after. Each technology that goes forward is evaluated by Commanding Officers and personnel to see what need it fits or what mission it serves within the Police Department, Fire Department or whichever Department looks to that technology to solve a problem.

As that solution is suggested, there really is a robust process that begins with discussions throughout the various units and continues on. We look toward guidance and have an established technology process. We have significant in-house experts and a STAC Committee, Strategic Technology Alliance Committee, who look at how technology fits into the overarching goals of the City and ask questions like about their alignment. Are they repetitive in nature? How can we create efficiency and effectiveness? Then we move on and look at funding sources, purchasing and contracting, request for proposal, and what contracting needs to take place. An assessment

by Risk Management and an evaluation by the City Attorney's office is done. This process is to ensure that the technology serves the Department and ultimately the City as a whole. That then goes to our City Council members for a vote, depending on the dollar amount.

Overlapping that process is our Surveillance Ordinance process. In addition to the already established process we now notify the Privacy Advisory Board, complete community outreach, and complete Use Reports and Impact Reports.

People can lobby but Commanding officers are not making any decisions based on that lobbying group due to the established process.

There is a push being made by law enforcement, and with other City departments, to use data to make informed decisions. The office of the City auditor has stressed the need for the City to use data to make more informed decisions, and that is what we are consistently striving for and implementing.

The next part of this process calls for the Police Department to hear from the community. Each one of the technologies presented has a Use Report to accompany it. After these meetings, we take the Impact Reports along with any community feedback and forward them to the Privacy Advisory Board. The Privacy Advisory Board will assess the technologies, roundtable them, form subcommittees, and make recommendations to the City Council to consider.