Surveillance Use Policy

National ICAC Data System (IDS)
San Diego Police Department

PURPOSE

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), 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.

USE

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.

DATA COLLECTION

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 including 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.

DATA ACCESS

Only task force members, investigators, and certified forensic examiners, 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.

Surveillance Use Policy

National ICAC Data System (IDS)
San Diego Police Department

DATA PROTECTION

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 their unique identifier, and an alphanumeric password, and utilize two-factor security measures.

DATA RETENTION

Per evidence code sections related to crimes perpetrated against children allowing for historical evidence to be brought forth, extracted data is retained until the death of the suspect.

PUBLIC ACCESS

The data contained within IDS is only used in criminal investigations and is not available to the public. Copies of the data can only be obtained with a court order or the discovery process.

THIRD-PARTY DATA SHARING

Data contained within IDS is not shared without a court order or other legal proceedings such as discovery. The data is considered confidential, and there is no third-party access or sharing.

TRAINING

Investigators and certified forensic examiners who use IDS must complete a training program provided by ICAC before using the software.

AUDITING AND OVERSIGHT

ICAC maintains a log of all authorized IDS users. The ICAC Commander and IDS manager are responsible for granting access to the system.

Misuse of the system would be reported to and investigated by the task force member's Internal Affairs unit. Violations of the laws, agency policies, or user agreement terms and conditions would subject the task force member to discipline and/or criminal proceedings or civil processes.

MAINTENANCE

IDS is controlled and maintained by the West Virginia ICAC. The ICAC commander is responsible for monitoring and training when new versions are released.