The City of San Diego

Staff Report

DATE ISSUED:	November 6, 2023	
TO:	Privacy Advisory Board	
FROM:	San Diego Police Department (SDPD)	
SUBJECT:	Presentation of Use Policies and Surveillance Impact Reports Associated with the Internet Crimes Against Children Data System (IDS)	
Primary Contact:	Captain Matt Novak	Phone: (619) 531-2339
Secondary Contact:	Lieutenant Michael Swanson	Phone: (619) 531-2563
Council District(s):	Citywide	

OVERVIEW:

On August 10, 2022, the City of San Diego amended and added Chapter 2, Article 10, of the San Diego Municipal Code – the "Transparent and Responsible Use of Surveillance Technology" (Surveillance Ordinance). The Surveillance Ordinance is designed to provide greater transparency to the City Council and the public when the City uses or acquires any technology that meets the City's definition of surveillance. The Surveillance Ordinance requires that for each technology that meets the criteria for surveillance, City Departments must:

- Hold at least one or more community meetings in each City Council district where the proposed surveillance technology is deployed, with an opportunity for public comment and written response.
- Prepare a Surveillance Use Policy that includes the purpose, use, data collection, data access, data protection, data retention, public access, third-party data sharing, training, auditing, oversight, and maintenance.
- Prepare a Surveillance Impact Report including description, purpose, location, impact assessment, mitigations, data types and sources, data security, fiscal cost, third-party dependence, alternatives, track record, public engagement, and comments.
- Present the item to the Privacy Advisory Board for review.
- Present the item to the City Council for the acquisition and deployment of all new and currently used surveillance technologies.
- Provide annual reports on surveillance technology use, impact, and acquisitions.

PROPOSED ACTIONS:

In accordance with the Board Notification and Review Requirements outlined in section 210.0102 of the Surveillance Ordinance, the San Diego Police Department (SDPD) is requesting approval for the use, funding, acquisition, and sharing of technology that falls within the definition of surveillance technology under the ordinance. Specifically, the item being requested is known as the Internet Crimes Against Children Data System (IDS).

DISCUSSION OF ITEM:

SDPD's mission is to provide the highest quality police services to the communities it serves. SDPD values transparency, and public input and welcomes open dialogue about its practices and operations. The preservation and sustainability of public safety, officer safety, and civil rights are paramount. SDPD further recognizes the importance and value of public disclosure regarding the qualified surveillance technology we use. We intend to present to the Privacy Advisory Board our use of IDS.
SDPD's lead, the Internet Crimes Against Children Task Force (SDICAC) is one of a national network of sixty-one coordinated task forces, representing over 5,400 federal, state, and local law enforcement agencies, dedicated to investigating, prosecuting, and developing effective responses to internet crimes against children. SDICAC is composed of thirty-three law enforcement agencies and four prosecutorial bodies spanning three counties: San Diego, Riverside, and Imperial Valley. As the lead agency of the task force, the Commander, a San Diego Police Department Detective Sergeant, is responsible for providing and procuring technology/equipment, training, and travel to each member of the task force, ensuring each agency/investigator/prosecutor is capable of executing their duties to proactively and reactively protect children from online predators. The SDICAC is funded primarily through grant funding awarded by the Department of Justice, Office of Juvenile Justice and Delinquency Program (OJJDP). Additional grant funding is provided by the California Governor's Office of Emergency Services (CalOES).

The IDS is a web-based application that provides a secure dynamic infrastructure to facilitate online law enforcement investigations of child exploitation and enticement. 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 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.

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 NCMEC, the congressionally recognized clearing house for CyberTips.

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.

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.
The materials required under the Surveillance Ordinance accompany this Staff Report in compliance with the ordinance to provide information surrounding the proposed use of IDS and answer the many questions associated with their use and community impact.

David Nisleit

Chief of Police