THE CITY OF SAN DIEGO

M E M O R A N D U M

DATE: February 19, 2025

TO: Steven Lozano, Deputy Chief, Special Operations

FROM: Jeffrey Ring, Captain, Special Operations

SUBJECT: The San Diego Fire-Rescue Department's Response to the Privacy Advisory Board's Member Brett Diehl, Regarding Unmanned Aircraft Systems and the UASI Camera Project.

Summary:

The San Diego Privacy Advisory Board (PAB) was created by the Transparent and Responsible Use of Surveillance Technology Ordinance (Surveillance Ordinance) adopted on September 9, 2022. The Surveillance Ordinance mandates a process of community meetings, Use Policies, Impact Reports and reporting out to the PAB and San Diego City Council before acquiring or using surveillance technology. The San Diego Fire-Rescue Department (SDFD) is required to submit annual reports to PAB regarding all approved surveillance technology. SDFD has submitted two annual reports to be heard at the February 20th, 2025, PAB meeting. Prior to the scheduled meeting, questions from PAB member Brett Diehl were posted on the PAB website.

This memorandum will outline each PAB question from Brett Diehl, followed by SDFD's Response.

Unmanned Aircraft Systems (UAS)

1. **Why was data from the two incidents retained (and why was data from the other six incidents not retained)?**

   Most use cases for SDFD UAS are to provide real time imagery for ongoing emergencies. Prior to each flight, the crew will establish the purpose and objective of the flight. If a request to capture and retain imagery has been received, the crew will develop a plan to capture only the requested imagery consistent with the use policy. For the two incidents referenced in the annual report, requests were received to retain imagery. One request was from the SDFD Training Division, and the other request was from the City of San Diego Office of Emergency Services. It is SDFD policy to only captured imagery that is requested.

2. **What are the data management/deletion protocols for video gathered by the UAS?**

   Data collection protocols are detailed in the Data Collection section of the SDFD Surveillance Use Policy for UAS. The use policy specifically states that imagery that contains Personally Identifiable Information (PII) will not be retained for longer than 180 days unless retention of the information is determined to be necessary to an authorized mission or investigation.

3. **How long is data stored before deletion?**

   Any data captured will be reviewed to determine if any PII was captured. Imagery will also be categorized as DME or not DME. Any imagery that contains PII will not be stored beyond 180 days unless approved in writing by supervisory personnel.

4. **Who has access to stored imagery without seeking specific permission?**

   Only SDFD UAS Program personnel have access to stored imagery.

5. **What other departments/agencies have the ability to request sharing of video?**

   Any City, State, or Federal agency may request UAS imagery. Each request will be reviewed on a case-by-case basis in accordance with SDFD policy.

6. **What surveillance/video/audio/other detection capabilities do the new aircraft purchased/projected for FY25 possess?**

   The capabilities of the new aircraft are the same as the previous versions. The capabilities remain both EO and IR still and video imagery.

Urban Area Security Initiative Camera System

1. **How/why were these specific locations chosen?**

   These cameras are a replacement for the current camera system that was established in 2005. The purpose of this system is to provide situational awareness for activities on Mission and areas adjacent to Ocean Beach Pier. The system is intended to increase capabilities for public safety, emergency management, and homeland security.

   These locations were selected to be able to observe highly used open bodies of water for safety, security, and efficiency of safety personnel deployment.

2. **What are the data management/deletion protocols for videos recorded on the UASI?**

Below is the pertinent information from the Use Policy:

DATA PROTECTION
All information will be viewed in the following secured buildings: The Lifeguard Communication Center (LCC) at Lifeguard Headquarters, JHOC at USCG Sector San Diego, and the City's EOC at the City of San Diego Office of Emergency Services (EOS). The information will be safeguarded from unauthorized access. The system must be activated and logged on at the three secure buildings (LCC, JHOC, EOC) with unique passwords. No confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

DATA RETENTION
Data will be stored on its own hardware in a secure location at Lifeguard Headquarters for no longer than 180 days unless explicitly authorized by the Lifeguard Chief. The stored data will automatically be deleted on the 181st day unless explicitly authorized to be saved for a legal reason. All data sources collected by the Camera System will only be copied or released to an officer of the City, State or Federal Court. All authorization of saved or copied data will be in writing and save for no less than 2 years. In the reporting of this information, no confidential or sensitive information should be disclosed that would violate any applicable law or would undermine the legitimate security interests of the City.

PUBLIC ACCESS
The Data will not be released to the public unless required by applicable local, State, or Federal law. Data will be released in a court proceeding in the process of discovery if the data is determined to be disclosable.

THIRD PARTY DATA SHARING
There will be no third-party sharing of this data.

TRAINING
Training is required for any individual authorized to use the Camera System or to access information collected by the Camera System. Security, authorized uses, and retention will be part of the training conducted.

AUDITING AND OVERSIGHT
Annual review of procedures used to ensure that this Surveillance Use Policy is followed, including identification of internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the Camera System and access to information collected by the Camera System, technical measures to monitor for misuse, identification of any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy will be conducted by an agent of the City of San Diego.

MAINTENANCE
Maintenance will be conducted by authorized personnel listed in this policy.

Third-party contractors who conduct hardware and software maintenance will not have access to data collected or stored by this Camera System.

3. **How long will data be stored before deletion?**

   Up to 180 days.

4. **Who will have access to stored imagery without seeking specific permission?**

   DATA ACCESS
   The following classifications can access and use the data collected:

   1. SDFD Classifications:
      Lifeguard II, Lifeguard III, Lifeguard Sergeant, Marine Safety Lieutenant, Marine Safety Captain, Lifeguard Chief, Battalion Chief, Deputy Chief, Assistant Fire Chief, Fire Chief.
   2. San Diego Police Department (SDPD) Classifications:
      Police Officer II, Police Sergeant, Police Detective, Police Lieutenant, Police Captain.
   3. JHOC Personnel**:** All have "Secret Clearance" through the Federal Government

Agency	**Title**	**Position**
USCG*	Ops. Specialist Chief	Command duty officers
USCG	Ops. Specialist 1st class	Sensor Operator
USCG	Ops. Specialist 2nd class	Situation watch standers
USCG	Ops. Specialist 3rd class	Communications watch standers
USCG	JHOC Technical Lead	Technical Support
USCBP*	Border Patrol Agent	Sensor Operator
NIWCP*	Contractor	Equipment support
Port of SD	Contractor	Port Camera Operator
USCG	Ensign	Command duty officers
USCG	LTJG	Command duty officers
USCG	LT	Command duty officers
USCG	Auxiliary CG Volunteer	Communications watch stander

   *USCG: United States Coast Guard
   *USCBP: United States Customs and Border Protection
   *NIWCP: Naval Information Warfare Center Pacific

   4. If the data is regarded as Digital Media Evidence (DME), the data can be accessed and used by sworn SDFD personnel in accordance with applicable sections of the SDFD Operations Manual, Lifeguard Division Policies, and local, State, and Federal Law. DME is forensic information stored or transmitted in digital form that may be used in court proceedings. Authorized investigators and attorneys of the City, State, and Federal Court may also access DME in accordance

with applicable law.

5. What other departments/agencies will have the ability to request sharing of UASI video?

Only those listed in the response to question #4.

General Questions

1. Where is video and other data stored generated by cameras and other employed technologies used? Is data stored on third-party-accessible servers (such as proprietary technology provider's servers)?

No.

2. Do law enforcement investigators require a warrant to gain access to SDFD-controlled data (including video)?

No.

3. What federal agencies have access to SDFD-controlled data?

Please see question #4 above.

Conclusion:

SDFD has carefully considered and responded to all questions put forth by Privacy Advisory Board member Brett Diehl.

Please contact Deputy Chief Steven Lozano if additional questions arise.