City of Chula Vista Technology & Privacy Task Force
Summary of Questions and Answers from the On-site CVPD Tour

Questions about the Police Dispatch / 911 Center:

The Chula Vista Police Department operates a state-of-the-art Public Safety Answering Point (PSAP), or 911 center, as a part of the national 911 system regulated by the Federal Communications Commission. The 911 center also serves as a radio dispatch center for various Police Department resources, including police officers on patrol. The Police Department's 911 dispatch center is a lifeline and conduit between police services and the community that needs them. The 911 dispatch center uses a variety of technologies, in accordance with best practices or regulatory requirements, to make it possible for citizens to call 911 for help, and to dispatch emergency responders to their aid as quickly as possible.

- **About geospatial data in the 911 dispatch center:** ***What type of commercial or other external geospatial (mapping) data is integrated into dispatch systems or other systems?***

  The dispatch center may use mapping data from a variety of sources. Mapping data is commonly used by 911 centers nationwide to provide critical safety information so that first responders can quickly locate emergency events or fellow personnel.

  A common example of the use of mapping data in a 911 center is the geospatial location of a 911 call. In a world where consumers increasing rely on wireless devices, the ability for 911 centers to know the location of a 911 call can be crucial to sending help – especially when a caller in unable to describe their location during an emergency. The Federal Communications Commission (FCC) required all wireless carriers to provide PSAPs accurate location information by 2012. The specific requirements are complex, but the FCC essentially requires that wireless phones provide PSAPs with location information within a certain range of accuracy. The FCC's complete location requirements can be found at https://www.fcc.gov/.

  In the event the caller is unable to provide their location (such as a child or person that doesn't know their location, a person being prevented from speaking, an unconscious person or a person in an altered state of consciousness), the 911 center may be able to ascertain there location using mapping data. This is commonly used to direct first responders (EMS, police, fire) to the scene as fast as possible to provide emergency aid or other assistance.

  Another example of the use of mapping data is the ability for dispatchers to see the GPS location of officers in the field whose vehicles are equipped with GPS technology. The City equips certain equipment with GPS sensors to monitor its location. Similarly, the Police Department equips certain vehicles with GPS equipment. This technology cannot be disabled by employees. The location information for on-duty police officers is generally available to on-duty dispatchers, supervisors, and even other officers. The location information helps in the efficient dispatching of the closest resource to a specific need. The location information also helps the city, as an employer, to ensure that city employees are properly performing their work duties.

  The availability and accuracy of location data in a 911 center can vary wildly by the type of phone or technology used by the caller, the capabilities of wireless carriers, the strength of a wireless signal and more. Some location data may still be available to 911 centers even if a caller had previously turned-off location services on their device. But even that can depend on the technical capabilities of the device and carrier.

For the Chula Vista Police Department, the most-frequent source of geospatial data is the City of Chula Vista's own internal geographic information system data (GIS). But some systems, including Live911, may use other maps of their own.

Live911 provides dispatchers and officers with the geolocation of an incoming 911 call, and can also stream the audio from the 911 call directly to officers in the field. The geolocation data is visually displayed as a dot on a map contained within Live911's web-based software. The source for that map is under the exclusive control of Higher Ground, Inc., the corporate provider of the Live911 service. We have contacted Higher Ground to inquire what source they use for mapping data, and they informed us that their maps are pulled from ESRI/ArcGIS online.

- **About dispatch operations*: Tell us about dispatch operations. What type of information does dispatch collect from incoming calls, how are they assigned to officers, and how long is that data stored?***

The Police Department's 911 dispatch center acts as the nerve center for all Police Department operations. Dispatch personnel answer all emergency 9-1-1 phone calls and all other non-emergency requests for police service. The 911 dispatch center is also responsible for all police radio communications, dispatching officers where they are needed, and coordinates communication with a variety of other entities in the region.

The operations of the Police Department's 911 dispatch center are similar to that of many dispatch centers across the nation. In general, the duty of a dispatcher upon receipt of a 911 or other telephone call is to collect as much information from the caller that is necessary to get the appropriate resources to the scene as fast as possible, to help the situation. Examples of the type of information collected by our dispatch center include the nature and details of the situation, the location of the situation, whether anyone is injured or currently under threat, the description or identity of persons involved in the situation, whether any weapons are involved in the situation, and the name and telephone number for the caller in the event the dispatcher needs to reach them again. Keep in mind that providing this information is entirely optional – every caller is free to provide whatever information they feel comfortable providing, and to withhold whatever information they want to withhold.

While on the phone, the dispatcher enters this information into a Computer Aided Dispatch (CAD) system – software systems intended to assist in the dispatching of public safety resources wherever they are needed. Other dispatchers monitor the CAD system and are empowered to dispatch the necessary resources where they are needed. Dispatchers may request or assign a variety of resources, appropriate to the specific facts of the situation, such as police officers, supervisors, EMS personnel, firefighters, drone operations personnel, detectives, animal control officers, regional PERT team assets, water control or water quality personnel, utility company personnel, the Mobile Crisis Response Team (MCRT), and many more.

Resources may be dispatched over secure radio frequencies, by telephone, or by other digital communications. The radio systems used for Police Department are secure and encrypted. In addition, to foster interagency capability in the response to critical incidents and other circumstances that impact more than one agency, dispatchers and officers are equipped with

radios that can communicate with a wide variety of local, state and national public safety entities. Examples of these entities may include neighboring local police agencies, regional firefighting assets, some state agencies operating in our region, and some federal entities operating in our region. Some incidents require the rapid response by multiple agencies to enhance or expedite emergency control of a critical event. Radio communications are the most-common means to coordinate between agencies in these situations.

Dispatchers are highly trained professionals that have thousands of hours of specialized training and are empowered with discretion to evaluate each situation, to determine which resources are likely needed. Dispatchers are also guided by a series of state and national dispatching standards, and by a set of Police Department policies. Lastly, all dispatchers and on-duty personnel are monitored by a variety of supervisory and management personnel at all times.

Whenever a police officer is dispatched to a call, the CAD system automatically transmits the appropriate CAD system information (generally all of the information collected by the dispatcher) directly to that officer's computer through an encrypted, private network tunnel. Other 911 systems, including Live911, can also live-stream information about active 911 calls directly to officers in the field using the same encrypted, private network tunnel. It does this by transmitting an audio feed from the live 911 call through internal servers, which can then stream the data over encrypted wireless communications to officer computers.

Law enforcement needs timely and secure access to services that provide data wherever and whenever it is needed to help reduce or stop crime and victimization. The security and control of the CAD system, the encrypted, private network tunnel, and all other systems that may connect with it (e.g. other internal police servers, routers, network switches, fiber optics lines, etc.) is governed by the FBI through a collection of strict requirements collectively known as the Criminal Justice Information Services (CJIS) Security Policy. The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's Advisory Policy Board decisions along with nationally recognized guidance from the National Institute of Standards and Technology.

The CJIS Security Policy controlling document is a 253-page volume of topics that include relevant laws, policies, requirements, proactive logging and monitoring protocols, auditing requirements and many more topics. The Chula Vista Police Department is required to adhere to the strictest requirements of CJIS Policy for all of its criminal justice systems. This includes the CAD system and related networks.

Like all computer systems in use for public safety operations, data in our CAD system is retained in strict accordance with legal or regulatory authority, and in accordance with the data retention policies of the City of Chula Vista and the Police Department. Although these policies allow for exceptions for certain situations (one example may include information that becomes evidence in a court of law), the citywide retention schedule requires that CAD system data shall be retained for a minimum of two years. The schedule does not specify a timeline for when CAD data should be destroyed, and we currently have CAD data dating back to 1998. The schedule requires that recordings of 911 calls are retained for a minimum of 100 days. The schedule does not specify a timeline for when 911 calls should be destroyed. Due to the length of some

criminal investigations among other reasons, we have a practice of destroying non-evidentiary 911 recordings after three years.

- **About geo-fencing:** ***Can you describe in more detail how "geo-fencing" works and if there is any data collection related to it? What is the range of a geo-fence that surrounds officers when they patrol? Do officers use geo-fencing technology to execute warrants, conduct geo-fence warrants, or to identify the location of a person?***

  Geo-fencing is a very broad term defined as the act of creating a virtual boundary line around a specific geographic space. In simple terms, geo-fencing is the equivalent to drawing a box or other boundary on a map. It is intended to "mark" an area on the map, such as the location and perimeter of a crime scene, for a specific purpose. Examples include but are not limited to marking the location and perimeter of a crime scene or marking the outside limits of police beats. As it relates to police technology used in Chula Vista, geo-fencing is a critical component to the flight safety of our UAS (drone) program. We use geo-fences – areas on a map – to electronically control the areas where UAS devices (drones) can safely fly. Once enabled, the drone software will automatically prevent a drone operator from flying the drone into or out of a geo-fenced space. For example, we create geo-fences around large trees or tall buildings so that the drone doesn't crash into them. We also geo-fence the outer limits of where our drones are allowed to fly in accordance with FAA requirements or other authorities.

  Except as described herein, the Police Department does not otherwise use of geo-fences to mark the position of officers or personnel. There is no geo-fence that surrounds officers when they are on patrol. As previously mentioned, many police patrol vehicles are equipped with GPS sensors that can relay the location of the vehicle through our CAD system. This type of Automatic Vehicle Location (AVL) system helps in the efficient dispatching of the closest resource to a specific need. The AVL information also helps the city, as an employer, to ensure that city employees are properly performing their work duties. Some other systems, such as Live911, my utilize the AVL information so that live 911 calls that are close to a particular officer may be streamed directly to that officer's computer.

  The Police Department also does not routinely use geo-fencing to execute warrants or to identify the location of a person. The Police Department may, when necessary for a criminal investigation and acting upon a duly issued warrant, seek to use a geo-fence during a criminal investigation (also known as a geo-fence warrant). It is also possible that, while responding to a police emergency, an investigator or incident commander may elect to mark the location or perimeter of the incident on a map for the purposes of managing the incident. But geo-fences used in this capacity are not a part of any automated electronic systems in use by the police department.

- ***About sharing information with other agencies: What types of information-sharing can be done with County Sheriff, other police departments such as SDPD, Border Patrol and other federal agencies? Are there any MOUs that establish these relationships?***

  The police department has a responsibility to keep the city safe and to respond to police-related service requests of our residents, businesses, and visitors. The City of Chula Vista is part of a greater San Diego metropolitan community. Acts of violence, theft, destruction and other

criminal behavior are not confined to the city limits, as criminal offenders may traverse in-between city limits and across the entire region, state, or nation. The Police Department's criminal investigations often take our officers and detectives into the jurisdiction of neighboring agencies to further or resolve a criminal investigation. In addition, the employees of other law enforcement agencies may cross into the City of Chula Vista or any other jurisdiction for the purpose of furthering or resolving their own agency's criminal investigations. As a result, all law enforcement agencies in the San Diego region have a long history of working cooperatively with each other, along with a wide variety of local, state and national public safety agencies, to investigate crimes or to apprehend criminal offenders.

As this relates to information-sharing or data-sharing between agencies, this particular question as written is very broad and could cover an endless number of potential situations and circumstances. If the context of this question surrounds immigration enforcement, we can categorically state that the Police Department does not involve itself with the enforcement of immigration laws, that no data is shared by the police department for that purpose, and that we have always and continue to adhere to all requirements of SB54 and other laws.

The Police Department is not certain of the exact nature of this question as written, and may therefore be unable provide a comprehensive answer in this format. The Police Department is available to provide answers to more specific questions, or can provide further information and context at a future meeting of the task force.

City of Chula Vista Technology & Privacy Task Force
Summary of Questions and Answers from the On-site CVPD Tour

Question about the Drone as First Responder (DFR) Program:

The Chula Vista Police Department's Drone as First Responder (DFR) Program provides airborne support to public safety operations in a safe, responsible, and transparent manner to protect the public, preserve the peace, reduce response times and increase overall quality of life in Chula Vista.

The intent of the DFR program is to get a drone on scene before responding officers arrive. Certified teleoperators can evaluate the situation remotely and relay information to officers and field supervisors. The drone can also feed live-streaming video of the incident to commanders and first responders. This helps personnel determine the best tools, tactics and resources to safely mitigate a problem – often before officers arrive on scene.

The DFR program also gives first responders real-time tactical information and even "eyes on scene", proving to be a powerful de-escalation tool. Since the program was first launched, there have been multiple incidents where officers have scaled down their tactics and successfully defused situations with reduced use of force.

- ***About drone operations: Tell us about drone operations, launch locations, and dispatch criteria.***

  The Drone as First Responder (DFR) concept is different than traditional drone programs in that it is proactive rather than reactive. Instead of launching a drone after an officer is already on scene, Chula Vista's DFR program stations drones at permanent locations throughout the city and respond proactively to emergencies as soon as we are called about them.

  The drones are operated by an experienced police officer who is assigned to remotely operate the drones from the police headquarters in response to calls for service. From a resource deployment perspective, the officer assigned to operate the drone, known as a teleoperator, is no different than an officer assigned to patrol the city in a patrol car. The only difference is the teleoperator's vehicle is a remotely controlled drone rather than a police car. The drone officer can be dispatched to respond to a call for service, and can also monitor calls for service on their own and self-dispatch as needed.

  Currently, the Police Department operates drones from four launch locations strategically positioned throughout the city to maximize coverage area and minimize response times. FAA regulations limit each flight to a maximum distance of 3 nautical miles from the launch location. But each drone's range is also determined by its battery power. On average, we have found that drone batteries often provide 25-35 minutes of flight time. But that time can vary wildly depending on a number of factors such as speed, wind conditions, and more. The four launch locations are sufficient to provide aerial coverage over the majority of the city limits.

  The location of drone launch locations are determined by a wide variety of factors including but not limited to: a needs assessment, an assessment of current capability, distance between existing launch locations, hazards surrounding locations, a review of crime and demand for police services, the needs, capabilities, and cooperation with partner organizations, the

availability of space, cost implications, and oversight and management controls. The current drone launch locations were selected based on a careful review of all known factors.

DFR operations are governed by a number of policies, regulations, and laws. The Federal Aviation Administration (FAA) broadly governs drone flights in US airspace. The Police Department has several special certifications with the FAA, which also govern aspects of the DFR program. Some of these certifications, also known as Certificates of Authority (COA), are unique to Chula Vista's DFR program. For example, the FAA has granted the Police Department a COA that allows our teleoperators to fly multiple drones at the same time. Finally the Police Departments maintains a comprehensive policy on drone operations which may be found on our website at https://www.chulavistaca.gov/departments/police-department/department-policies. The policies also outline a number of requirements for officer conduct and decision making in response to calls for service or criminal investigation.

All police officers have some discretion to determine the calls to which they respond. The teleoperator is no different, and also has discretion to respond to calls where the use of a drone could help expedite the response of other emergency equipment or public safety resources, could help get "eyes on scene" faster than ground-based officers, could aid in the active investigation of a criminal offense, or where an aerial view of an incident can help preserve life and/or property.

A wealth of information about the history of the DFR program, including the selection of launch locations, may be found on our website at https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program.

- ***About the selection and training of drone operators: How are drone operators selected, trained? Are there any training or certification requirements to be a drone operator?***

  Candidates for our Drone as First Responder program undergo a difficult competitive process intended to evaluate a number of factors before selection. These factors can include experience, integrity, judgement, capability, education and training, skills and abilities, and much more. The Chief of Police retains ultimate authority to select and assign candidates to the program.

  All drone operators attend drone flight training. They must successfully obtain and maintain a license by the FAA as a Part 107 Remote Pilot. In addition to the training and study required to maintain a FAA Part 107 Remote Pilot License, all drone team members train regularly in a variety of locations and settings to ensure operational efficiency. All training is documented, and the records are subject to review by the FAA.

- ***When and why drones are used: Who dictates when and how drones are used? Are there any limits on where drones can fly, or what types of purposes they can be used for?***

  DFR operations and all drone flights are governed by a number of policies, regulations, and laws. The Federal Aviation Administration (FAA) broadly governs drone flights in US airspace. The Police Department has several special certifications with the FAA, which also govern aspects of the DFR program. Some of these certifications, also known as Certificates of Authority (COA),

are unique to Chula Vista's DFR program. For example, the FAA has granted the Police Department a COA that allows our teleoperators to fly multiple drones at the same time.

All police officers have some discretion to determine the calls to which they respond. The teleoperator is no different, and also has discretion to respond to calls where the use of a drone could help expedite the response of other emergency equipment or public safety resources, could help get "eyes on scene" faster than ground-based officers, could aid in the active investigation of a criminal offense, or where an aerial view of an incident can help preserve life and/or property. Police officers also have limited discretion to reprioritize their immediate demands to meet the needs of our community.

- ***About drone data security: Tell us about the technology and policies relating to recording, retaining, and securing drone video recordings and other drone electronic data.***

  Much like the Police Department's Body Worn Camera systems, all DFR flights are recorded and may be retained as evidence. DFR recording systems activate immediately upon launch , and teleoperators are trained to begin using the camera as quickly as possible to zoom in and view the area of the incident. At the conclusion of the flight and upon initiating a "return to base", DFR software is programmed to automatically tilt the camera upward and zoom-out to reduce the chances that private property is accidentally recorded.

  All video and photo evidence taken during any DFR mission is stored in the same manner and location as Body Worn Camera (BWC) video and other investigative evidence. Videos and photos are generally accessible to police investigators for official use only. Like all police records, video and photos may also be subject to additional release under the same rules and restrictions as BWC video and other items of evidence. Generally, UAS photos and video are considered part of the investigative record and are not available to the public under the California Public Records Act (CPRA) or Freedom of Information Act (FOIA).

  The Police Department utilizes a secure government "cloud" service, Evidence.com, to store digital photo and video evidence. The service is authorized and certified under both state and federal regulations for the security and protection of confidential criminal justice information and is available only for official law enforcement purposes. Evidence is stored and saved for a limited time (one year or less), unless it is categorized as evidence in an actual crime or formal investigation. Then it is stored for a period of time consistent with all other evidence related to that incident/investigation.

- ***About the selection of drone launch locations: How are drone launch locations determined and approved?***

  The location of drone launch locations are determined by a wide variety of factors including but not limited to: a needs assessment, an assessment of current capability, distance between existing launch locations, hazards surrounding locations, a review of crime and demand for police services, the needs, capabilities, and cooperation with partner organizations, the availability of space, cost implications, and oversight and management controls. The current drone launch locations were selected based on a careful review of all known factors.

City of Chula Vista Technology & Privacy Task Force
Summary of Questions and Answers from the On-site CVPD Tour

- ***About the contract with Motorola Solutions: Tell us about the contract with Motorola Solutions regarding Motorola's alleged use and sale of Chula Vista's data.***

  This question appears to relate to the contract with Motorola Solutions for the Command Central Aware software. This software is not used by the DFR program but is a part of our Real Time Operations Center (RTOC). Please see the similar question under the RTOC section, below.

- ***About the information collected by drone flights: Besides drone video, what other information is collected through drone flights, how is it secured, and is any of it accessible to the public?***

  Besides video or photo evidence, the DFR program also collects the following data about every DFR flight:

  - The date and time of the flight,
  - The corresponding police case number of incident number of the call for service,
  - The location of the call for service,
  - The nature of the call for service, and
  - The GPS coordinates and flight path of the DFR flight .

  All of this information is publicly available through our website at https://app.airdata.com/u/cvpd.

  In addition, the Police Department maintains aggregate statistics about DFR flights overall. In total the DFR program has responded to more than 11,000 calls for service, was the first resource on-scene at more than 6,300 incidents, and assisted in the arrest of more than 1,300 suspected offenders. In addition, thanks to the DFR arriving first on-scene, its use has been able to successfully avoid dispatching other ground units to more than 2,800 incidents, allowing those units to be rerouted to other calls for service. All of this data and more is maintained daily and publicly available on our website at https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program.

- ***About the use of drones during mental health crises: How are drones used to respond to mental health calls, in comparison to other resources such as PERT or the Mobile Crisis Response Team?***

  Police Department dispatchers may request or assign a variety of resources, appropriate to the specific facts of the situation, to any call for service. Resources may include but are not limited police officers, supervisors, EMS personnel, firefighters, drone operations personnel, detectives, animal control officers, regional PERT team assets, water control or water quality personnel, utility company personnel, the Mobile Crisis Response Team (MCRT), and many more. These resources may be dispatched simultaneously, as they become available, or as the situation unfolds and their need becomes known.

  A DFR may respond to a police call about a mental health crisis in order to provide ground-based first-responders real-time tactical information and even "eyes on scene." This can prove to be a powerful de-escalation tool. Since the program was first launched, there have been multiple

incidents where officers have scaled down their tactics and successfully defused situations with reduced use of force.

A response by DFR to a mental health crisis does not otherwise have any impact on a response by other assets, such as PERT or MCRT.

- ***About the use of drones as part of the Department's mission: How do drones fit into the Police Department's mission and values of compassionate, community-based policing practices?***

  A safe and effective law enforcement response to an emergency so often depends on having accurate and timely information. This has always been true in public safety but is even more important today. Having better information helps first responders put the right resources in the right place as fast as possible, resulting in a more effective response that keeps our community safe.

  The DFR program provides airborne support to public safety operations in a safe, responsible, and transparent manner to protect the public, preserve the peace, reduce response times and increase overall quality of life in Chula Vista. The intent of the DFR program is to get a drone on scene before responding officers arrive. Certified teleoperators can evaluate the situation remotely and relay information to officers and field supervisors. The drone can also feed live-streaming video of the incident to commanders and first responders. This helps personnel determine the best tools, tactics and resources to safely mitigate a problem – often before officers arrive on scene.

  The DFR program was created after national events demonstrated the horrific consequences that can result when first responders are sent to a call without accurate, comprehensive or timely information. The DFR program was created to address that gap. The DFR program gets "eyes on scene" faster than ground-based officers, allowing them to see or hear about a situation before they enter a danger zone. This type of real-time and first-hand information helps officers to know if they need to speed-up their response to save a life, or can slow-down their response to de-escalate the situation. For example, the DFR program has responded to multiple events where the DFR video allowed first responders to know what an object in someone's hand was, before ground-based officers arrived and were forced into a rushed confrontation.

  Simply put, the DFR program provides first responders with accurate real-time information that helps keep them safe, helps them better protect others, helps de-escalate circumstances, and helps reduce the potential need for force. The DFR program also helps expedite the response of emergency equipment or public safety resources, can aid in the active investigation of a criminal offense to help reduce future victimization, and can provide an aerial view of an incident that helps preserve life and/or property.

  All of these factors and more and crucial components to effective community-based and compassionate policing strategies.

- ***About the definition of "emergency": What is the operational definition of "emergency" in the use of drones?***

This particular question as written is vague and could relate to a wide variety of contexts. The Police Department is not certain of the exact nature of this question as written. We remain available to provide answers to more specific questions, or can provide further information and context at a future meeting of the task force.

City of Chula Vista Technology & Privacy Task Force
Summary of Questions and Answers from the On-site CVPD Tour

Questions About the Real Time Operations Center (RTOC):

The Police Department recently constructed a new office and working space that we call the Real-Time Operations Center (RTOC). The RTOC is intended to support the response to active emergencies and criminal investigations. When not being used to support an active emergency or investigation, the space serves as the day-to-day office space for the Police Department's pre-existing team of crime analysts. The analysts assist with crime analysis requests to meet the department's needs.

The RTOC space has been constructed but is not yet in operation. It has yet to install the Motorola Command Central Aware software that will facilitate the ability to combine real-time information in a cohesive format for staff to utilize in critical decision making.

When operational and used for the support of active emergencies or investigations, the RTOC will provide incident commanders and crime analysts with coordinated access to information to make more timely and effective decisions, increasing the safety for officers, suspects and the entire community. The intent of the RTOC is to help in the safe and effective response to emergencies and criminal investigations by providing a single command location with real-time information. For example, the RTOC is expected to provide incident commanders with quick access to GPS data about the location of first responders, an overhead view of an incident scene from our Drone as First Responder program, and the ability to hear incoming 911 calls in real time. The RTOC is intended to be a hub for the safe and effective management of public safety operations and criminal investigations.

- ***About usage of the RTOC: When, how, and by whom is the RTOC used?***

  The RTOC is intended to support the response to active emergencies and criminal investigations. Examples of situations where the RTOC may be used can vary but can include a major response to a natural or human disaster, an ongoing critical safety emergency, a significant or unusually complex criminal investigations, and more.

  In order the manage the response to any public safety emergency, the Federal Emergency Management Association has instituted the use of the National Incident Management System (NIMS) by local agencies. One important component to effectively managing an incident is command and control of responders. According to NIMS protocols, an Incident Commander is designated for this purpose. The Incident Commander is usually a high-level manager or supervisor in a public safety agency and has the responsibility to deploy a variety of resources in order to effectively manage the incident. Resources may include first responders, public works crews, firefighter personnel, subject matter experts, logistics management tools, working space, computers and other equipment, and more. The RTOC is one of many potential resources that an Incident Commander may utilize to effectively manage the incident.

  It is also important to understand that the RTOC is not staffed at all times. Instead, the RTOC may be "activated" for use when necessary. When not being used to support an active emergency or investigation, the space serves as the day-to-day office space for the Police Department's pre-existing team of crime analysts. (In the event that the RTOC be "activated" for use in response to an incident, the crime analysts may be directed with other personnel as

needed to help staff and support the RTOC and the overall response to the emergency. Other managers or subject matter experts may also be called to assist.)

- ***About funding for the RTOC: How was the construction and how are the ongoing operations of the RTOC funded?***

  The construction costs for the RTOC came from the Police Department Asset Forfeiture Fund. In terms of ongoing operations, it is important to understand that the RTOC is not used at all times and not staffed at all times. The RTOC does not have an ongoing budget for operations. The RTOC is merely a physical office space that, during normal circumstances, serves as the day-to-day office space for the Police Department's pre-existing team of crime analysts. Should the RTOC be activated for use in response to the incident, funding for the entire response to that incident (including any costs incurred by the RTOC) would be handled together. Generally speaking, funding for the public safety response to any emergency comes from the General Fund.

- ***About RTOC's Motorola Command Central Aware software: What is the background and operational status of the software used in the RTOC, and concerns about the software raised by members of the public?***

  In order to provide more efficient and more effective situational awareness surrounding an incident, the Police Department was authorized by the City Council to procure Motorola Solution's Command Central Aware software. The contract was first authorized by the City Council on December 3, 2020. It included language that was later interpreted as possibly giving, or appearing to give, Motorola Solutions or other vendors the right to store, share or use other forms of "Customer Data" that could contain personal information. While the Police Department and other authorities maintain substantial protections to keep vendors and others from accessing or using any Police Department confidential information, the potential issues and concerns raised by the community caused the department to work with the City Attorney to amend the contract. The amended language was adopted administratively by the City on February 17, 2022 and deleted the following statement from the contract: "~~In addition to the rights listed above, Customer grants Motorola a license to sell an Anonymized version of Customer Data for any purpose.~~"

  The Office of the City Attorney has stated that all significant city contracts are always reviewed by their legal group. This contract – and others like it involving data collection and usage – are currently under review by a team of lawyers in the City Attorney's office. Until recently, these types of provisions had not been an area of focus. They should have been and now very much are.

  The Command Central Aware software is not yet installed. The software implementation project is coordinated with Motorola Solutions and is fairly complex. The implementation project is ongoing. We do not have a definitive timeline for completion, but progress suggests that it is likely more than a month away.

  It may also be helpful to know that the installation of the software is only one step in the larger implementation of the Real Time Operations Center (RTOC). There are several more steps that

will follow installation of the software. For example, our personnel will need to spend time to be trained on use of the software, and our Department will need to draft procedures and protocols for RTOC operations. In short, we estimate that full implementation and actual use of the RTOC, including use of the Motorola Command Central Aware software, is still several months away.

Once installed, the Command Central Aware software is expected to take pre-existing content that exists in pre-existing but separate public safety systems, and provide "one pane of glass" to view that information. Although all the information in the RTOC already exists in the Police Department and has been used for years to respond to incidents, most of the information is contained within a variety of discrete computer systems – most of which exist in different physical spaces. Without a "single pane of glass" concept, RTOC operators would lack at-a-glance situational awareness of an incident, resulting in slower response times and strategies that could be less effective or less safe.

When the RTOC becomes operational, the following pre-existing systems are planned to be made available in the RTOC:

- Calls for service information in our Computer Aided Dispatch (CAD) system
- Live 911 – livestreaming 911 calls as they are coming in
- Local/international news and media channels
- Police radio communications systems
- Feeds from security cameras at the Police Department headquarters building
- Publicly-accessible social media posts
- Data about crime statistics and crime trends stemming from reports of crimes (the Police Department does not use any predictive policing algorithms)
- The video feed from our Drone as First Responder (DFR) program
- Other officer safety and awareness content, such as "Be On The Lookouts"

The Police Department intends that any future technologies that may have an impact on the privacy of our community will go through a public transparency and dialogue process in line with city policies. We remain committed to engaging in dialogue focused on keeping the community safe before deploying technology that may be perceived to infringe on privacy concerns.

- ***About the view of on-air news broadcasts: The RTOC has the ability to view on-air news broadcasts. Is there a policy dictating what specific news stations may be displayed in the RTOC?***

  The ability to watch live, on-air news broadcasts is among the systems available to the RTOC. There is no policy that dictates which news stations may be displayed in the RTOC. As part of an effective response to an incident, RTOC staff may view a variety of news channels or outlets and would likely tune to whichever channel(s) are providing information deemed valuable to the effective response to the incident. (Most-frequently local news outlets.)

- ***About the view of social media posts: The RTOC may look at publicly-accessible social media posts. What social media account(s) are used to view social media posts?***

Like anyone or any organization, RTOC staff may view publicly-available internet resources (Google, Bing, internet news, blogs, etc.) and publicly-accessible social media posts. No account is needed to view publicly-accessible social media posts.

In general, absent a lawful warrant for a specific criminal investigation, the RTOC does not have access to view private posts on social media or other private internet resources unless they have specifically been shared with the Police Department.

City of Chula Vista Technology & Privacy Task Force
Summary of Questions and Answers from the On-site CVPD Tour

Questions About Automated License Plate Recognition (ALPR):

The Police Department has operated an ALPR system since first authorized by the City Council in 2007. The original system included three ALPR cameras but was expanded to four ALPR cameras after City Council approval in 2011. The Police Department has continued to operate the four ALPR camera systems ever since.

Responsible and effective use of technology is the third of six pillars as noted by President Obama's 2014 Task Force on 21st Century Policing1. Technology provides agencies opportunities to better serve their communities and enable them to solve crimes more quickly and prevent further victimization, as well as create new pathways and connections with the community. Technology can change or adapt rapidly and create both new opportunities and privacy rights concerns. Agencies must work to assess and evaluate new technology and to develop and implement responsible and transparent policies and protocols that maximize crimefighting and crime reduction in a manner that is respectful of and cognizant of individual rights and privacy concerns.

ALPR technology has been in-use by law enforcement agencies around the world since at least 20014 and uses cameras and illumination to photograph a license plate and scan the image by image-processing software that extracts the necessary data (such as license plate number and state). That data is then compared against police databases such as lists of stolen and wanted vehicles. ALPR data can also be manually searched by police investigators.

ALPR systems have become an accepted and proven tool for hundreds of law enforcement agencies across the country. A January 2012 Police Executive Research Forum (PERF) Technology Summit in Washington D.C. 5, showed 71% of surveyed police departments in the United States employed ALPR systems to some extent.

ALPR systems function to automatically take a photographic image of the vehicle's license plate, transform that image into alphanumeric characters using optical character recognition or similar software. The images taken often include the license plate as well as enough of the car to allow for identification of the make and model.

The Police Department operates four marked patrol cars equipped with ALPR camera systems that operate while the vehicles are in use. Patrol cars are assigned to patrol officers on an available basis and are not assigned based on geography. Due to shift overlaps, patrol cars may not be used on some shifts (i.e. a day shift officer drives one, making it unavailable for the next shift, but available for an officer on the overnight shift to drive).

The department's ALPR system has two primary functions. While the ALPR-equipped car is in use, the system compares license plate numbers to one or more existing databases of vehicles of interest to law enforcement agencies, and alerts the officer operating an ALPR-equipped car when a vehicle of interest has been observed. This process typically occurs within seconds. At this point, the "automated" part of the process ends and officers must then independently validate that the ALPR system has accurately interpreted the license plate, validate that the license plate matches the vehicle of interest, verify that the alert is valid (e.g. not expired or otherwise deemed invalid), and make an informed decision as to

what action to take, if any. The ALPR system refreshes the comparison list every four hours to obtain the most current information.

An alert alone does not justify a traffic stop or detention. The officer must conduct these verification steps prior to any enforcement action.

The second function is the ability for officers to manually search the database for a specific vehicle related to an official investigation (crimes, missing persons etc.). The department subscribes to Vigilant Solutions, which provides data storage for CVPD ALPR images and allows officers to search for images from the department's images. Officers may also search for images from those of other law enforcement agencies and commercial entities that have specifically shared with law enforcement. Commercial systems are widely used by non-public entities such as shopping malls, apartment complexes, home-owners associations, amusement parks, and parking garages. Commercial systems greatly outnumber law enforcement systems.

This manual search function is the part of the system that is most invaluable to the department as it used in almost every investigation conducted. There are hundreds of instances where cases would not be solved without the use of the ALPR system.

- ***About safety of the ALPR system: How does the ALPR system function in partnership with existing databases, and what safeguards and protocols are in place to mitigate privacy or enforcement concerns? How is the system managed, and used by CVPD?***

  The CVPD ALPR system is a stand-alone system. ALPR data is stored only within the ALPR system, which is a secured, Government approved secure server. ALPR data is protected from disclosure to anyone outside of law enforcement by state law. Additionally, CVPD has chosen to restrict access of our data exclusively to California law enforcement agencies who are bound by SB54 to prevent immigration enforcement. As a matter of routine practice the Police Department does not share ALPR data with any federal agency or fusion center.

  As it relates to ALPR data, the concept of data sharing is best described as follows: If another law enforcement agency is investigating a crime and searching for an involved vehicle, and that vehicle's license plate was detected and photographed by one of CVPD's four patrol car-mounted ALPR camera systems within the past 365 days, then the image and license plate of that vehicle will be included in the search results for the other agency. Conversely, if the vehicle's license plate was not detected and photographed in CVPD's ALPR database, then nothing from CVPD's ALPR data would be shared with the other agency.

  CVPD's ALPR system only takes a photograph of a vehicle after the vehicle-mounted system software detects a license plate within the scope and focus of the ALPR cameras (this range is generally out to 12-15' from the patrol car). Once the system recognizes a license plate number, the system takes a photograph of the license plate and vehicle. That photo, along with the date, time and location of the photograph, is stored in the ALPR system. The system does not record video or constantly take photographs.

  One feature of the ALPR system is that it is able to compare detected license plates with pre-existing law enforcement databases that include stolen cars, stolen license plates, cars

associated with crimes or with persons of interest in criminal investigations (e.g. wanted vehicles). In the event a detected license plate matches that of a wanted vehicle, the system sends an alert to the officer driving the ALPR-equipped police car that a wanted vehicle may have been detected nearby. Upon receiving the alert, officers must verify that the alert is valid, locate the car, and determine what course of action to take (if any). Nothing precludes the officer from calling upon other officers to help. An ALPR alert by itself is not enough for an officer to stop the car, detain occupants, or take any other enforcement action.

Another safeguard built into the ALPR system is that it refreshes the database of wanted vehicles every four hours. This helps prevent an alert from being sent for a vehicle that is no longer wanted. Alerts are not saved in the system and cannot be researched retroactively.

The Police Department's ALPR data is maintained for 365 days. Images are automatically deleted one year from the date they are taken. The Department conducts regular audits to verify that no data exists beyond 365 days.

Within the law enforcement profession, different agencies may maintain ALPR data for different time periods. For example, some agencies retain data for two years or more. The California Highway Patrol is limited by state statute to a 60-day retention period. Many of our criminal investigations are complex and lengthy in nature, often extending in excess of a year. It's not uncommon for new investigative leads to surface months or years later. Access to ALPR information in these types of cases can be a crucial link to the investigation and help detectives locate offenders. Due to the nature and complexity of the steps and processes involved in each criminal investigation, it's not practical for the Police Department to track quantitative data about ALPR's use in criminal investigations. This is similarly true for other functions of the department where the sheer volume and complexity of tasks lack practical feasibility to quantitatively track.

The Police Department's ALPR policy is publicly available on our website at https://www.chulavistaca.gov/departments/police-department/department-policies. In addition, the ALPR administrative team performs quarterly audits of the system and audits are also posted to our website at https://www.chulavistaca.gov/departments/police-department/about-us/transparency-and-accountability/automated-license-plate-readers-alpr.

- ***About the use of ALPR cars: How are the ALPR cars used or deployed by the department?***

The Police Department operates four ALPR systems that are mounted on four marked patrol cars (although currently only three cars are in use due to a mechanical issue with the fourth vehicle). These patrol cars are part of our standard marked patrol fleet, which consists of 50 vehicles (only 45 of which are operational as of June 16, 2022). The cars are shared by our patrol shifts.

Our patrol shifts overlap each other by several hours. Because there aren't enough cars to go around, cars are checked-out by individual officers as they are available. (Sometimes officers are unable to go into the field due to a lack of cars.) Officers in patrol are assigned to any one of a variety of patrol beats. Officers spend much of their shift in their assigned areas, being dispatched to calls for service or otherwise responding to the needs of the community.

Officers driving ALPR-equipped cars use them like normal patrol vehicles – to patrol their assigned area and respond to calls for service. The limited number of ALPR-equipped vehicles, coupled with the nature of the demand for police services throughout the city, prevents the Police Department from deploying ALPR cars to specific areas of the city. In addition, the Police Department does not deploy ALPR cars for the specific purpose of creating ALPR data.

The Police Department inspects "density maps" each quarter, which provide a visual depiction of where in the city ALPR license plates are scanned. We have found that density maps consistently match other heat maps that depict where the most demand for police calls for service originate from. The majority of these community-driven calls for service originate in the western region of Chula Vista.

- ***About the effectiveness of the ALPR system: How do you measure the effectiveness of the ALPR system?***

  Tracking ALPR success stories or the number of cases solved is highly complex. ALPR data can only be used under strict policy controls and only where a detective has a legal right to use the data, and the use of the data is necessary for an official law enforcement purpose. But ALPR data by itself does not solve crimes. ALPR data is just one among many tools that our officers and detectives may utilize to help them identify vehicles of interest during a criminal investigation, or to help eliminate a potential vehicle from suspicion. Simply put, ALPR data may help to narrow an investigation by providing a resource to investigate the potential presence of related vehicles (or lack thereof) in relation to the location and time of a specific crime. But ALPR data alone is unlikely to be the sole reason for solving a crime.

  Tracking the usage of any of these tools is not practical. About 25,000 crimes are reported to the Police Department each year. Each one of these crimes must be investigated, and the department maintains a small complement of about 43 sworn detectives. Many investigations take dozens of hours of investigative work, and some investigations take hundreds. It is neither practical or efficient for the investigative division to track quantitative data about each individual action, database search, or other investigative step in every case under investigation. This would be especially time consuming for each detective, who may have a simultaneous workload of 30-60 ongoing investigations representing countless victims in our community seeking justice. As a result, the Police Department does not make it a practice to track the types of minute details for many investigative processes for reasons of practicality.

  The Police Department maintains strict policies that govern the security and control over confidential data, including ALPR data. Police Department supervisors and professional staff review and audit the use of confidential police systems. In addition, external audits are conducted each year by a number of external authorities such as the California Department of Justice of the FBI. To date, the Police Department is not aware of a single breach of data security policies or protocols as they relate to ALPR data.

  Throughout the state of California police officers are held to similar standards and regulatory controls that relate to the security of information. While the Chula Vista Police Department is not empowered to conduct administrative investigations into allegations of misconduct by the

personnel of other law enforcement agencies, several policies and laws within the state help insure employee accountability. Should the Police Department become aware of an inappropriate or systemic breach of policy or trust by any agency, we could take several steps to protect our data such as alerting other authorities or shutting-off access to our systems and data.

The ALPR administrative team, acting under the authority of the Chief of Police, controls which agencies the Police Department shares ALPR data with. (Keep in mind that sharing, as used herein, only means that CVPD's ALPR data will be included in an agency's search for a particular license plate.) The list of agencies that the Police Department shares with is publicly available on our website at we share data with is published on our website at https://www.chulavistaca.gov/departments/police-department/about-us/transparency-and-accountability/automated-license-plate-readers-alpr. The list may be updated periodically when a new agency has begun to use the ALPR system, request sharing of our data, is approved by the ALPR administrative team, and we specifically authorize sharing by our system. Anytime the list is updated, the ALPR administrative team posts an updated version of the list to the website. As part of the audit process, the ALPR administrative team verifies that no agency outside our agreement is accessing our data.

Other Questions:

- ***Where do the funds come from for each of the technologies shown?***

  Funding sources for all City processes and products can vary wildly. The Police Department may utilize a number of budget accounts for different projects, that may include but are not necessarily limited to the General Fund, Asset Forfeiture Fund, a variety of grant funds, and more. The specific budget account for any specific technology acquisition is a matter of public record, and the City Council requires that fiscal impacts for any significant expenditure are made a part of its public deliberations.

- ***What data is shared with DHS fusion centers, and how does that sharing happen? To what extent does CVPD participate in the San Diego Law Enforcement Coordination Center? How does CVPD share data in the San Diego Law Enforcement Coordination Center? Does CVPD participate in any other DHS fusion centers?***

  This question as written is very broad. Generally speaking, the Police Department may share specific and independent information related to criminal activity and criminal investigations with the San Diego Fusion Center. The Police Department does not maintain any systems that routinely or automatically share data with any Fusion Center. The Police Department does not collect nor share immigration information. We do not play a direct role in any other Fusion Centers, and only collaborate when criminal investigations and information crosses jurisdictions and coordination between jurisdictions may be assisted by the Fusion Center. Any information shared at that time is information deemed critical to safe and effective public safety operations.

- ***What are the decision-making processes during procurement?***

  Procurement protocols are managed by the City of Chula Vista Department of Finance under the direction of City Administration and City Council. The Police Department, like all other city departments, adheres to all procurement policies and protocols required by the Finance Department.

- ***Do all officers wear body cameras when interacting with the public?***

  Yes. Body worn cameras (BWC) are issued to all uniformed officers and detectives. They are required to be worn and utilized while on-duty in the field. According to departmental policy, employees are directed to activate BWC in a number of circumstances, including whenever anticipate enforcement action or investigative contacts are about to take place. The policy on BWC is contained in the Police Department's policy manual, publicly available on our website at https://www.chulavistaca.gov/departments/police-department/department-policies.

- ***Is the Police Department subject to the City's data retention policies?***

  Yes, in addition to any other data retention requirements or restrictions based on proper legal or regulatory authority.

City of Chula Vista Technology & Privacy Task Force
Summary of Questions and Answers from the On-site CVPD Tour

- ***Does the Police Department have a policy for sharing data with third parties, such as someone who requests data for academic research purposes?***

  Requests for information or data in these circumstances are handled pursuant to the California Public Records Act (CPRA) and/or the federal Freedom of Information Act (FOIA). The City of Chula Vista complies with all requirements and restrictions of both acts. In addition, for requests that are filed outside those two acts, the Police Department and the Chief of Police have discretion in selecting whether it will participate in a research study. That decision may be based on a variety of factors, including current workload and capacity to participate, legal limitations or prohibitions against sharing data, the impact that sharing information could have on our community, value of the potential research or study, and much more.

- ***Where is the primary data stored – locally or in the cloud?***

  All electronic data in storage for the Police Department is either stored on-site in systems controlled by city employees, or in secure cloud-based systems. Any cloud-based system that contains confidential information must be governed and certified by the FBI through a collection of strict requirements collectively known as the Criminal Justice Information Services (CJIS) Security Policy. The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's Advisory Policy Board decisions along with nationally recognized guidance from the National Institute of Standards and Technology.

  The CJIS Security Policy controlling document is a 253-page volume of topics that include relevant laws, policies, requirements, proactive logging and monitoring protocols, auditing requirements and many more topics. The Chula Vista Police Department and all applicable cloud-based service providers are required to adhere to the strictest requirements of CJIS Policy for all of its criminal justice systems.

- ***Can you provide an inventory of the systems the Police Department uses to collect and manage data?***

  The Police Department maintains servers and systems for a wide variety of purposes, including such things as logging door locking mechanisms, tracking the HVAC status and temperature of office spaces in the facility, recording 911 calls, maintaining payroll records, keeping records of inmates booked into the jail, keeping both digital and hard-copy records of police reports and related investigations, maintaining recordings of internal facility security cameras, and much more. The question as written is very broad, and the Police Department needs more clarification about the types of systems or types of data that the inquiry surrounds.

- ***Beyond the security policies of the cloud provider, what data protection policies does the Police Department have of its own?***

  The Police Department has a significant number of specific data protection and security policies and practices. In addition, all electronic data in storage for the Police Department is also controlled by server-based automation policies. Lastly, all systems that contain confidential information are governed by the FBI through a collection of strict requirements collectively known as the Criminal Justice Information Services (CJIS) Security Policy.

The question as written is very broad. The total summation of data protection policies would be voluminous (exceeding many hundreds of pages). Without greater clarity or specificity, the Police Department is unable to provide a comprehensive answer in this format. But the entire Police Department policy manual is publicly available on our website at https://www.chulavistaca.gov/departments/police-department/department-policies.

- ***Are there any written policies that preclude or limit the purchase or use of particular types of technology by CVPD?***

  Yes. There are a combination of internal policies and legislative or regulatory requirements that limit the purchase or use of certain types of technologies. For example, state law prohibits the use of automated facial recognition by police officers, controls the procurement and use of military equipment, and internal policy prohibits the use of systems for immigration enforcement.

  The Police Department looks forward to working with the Task Force to derive policy recommendations that guide the potential procurement or use of future technologies.

- ***Is there an auditing process to review procurement of contracts?***

  Yes, all procurements are controlled by the Finance Department and all city contracts are reviewed by the City Attorney. All significant contracts also undergo review by the City Council.

- ***If so, does that auditing process specify/address any of the following:***
  - ***Appropriateness and justification of procurement***
  - ***Impact on privacy concerns and balance on civil liberties***
  - ***Cost-effectiveness and efficient spending of public funds***
  - ***Effectiveness – degree of achievement of the set objectives***
  - ***Transparent spending of public funds***

  It is our understanding that existing processes include measures for all of the above. For greater detail, please refer to the Department of Finance and the Office of the City Attorney.

- ***Chief Kennedy spoke of "Community Policing" and "Compassionate Policing" during the Task Force tour, as approaches to policing CVPD aspires to. How can CVPD achieve this with such an extensive reliance on surveillance technology?***

  While the safe, reasonable, and effective application of modern technologies is important to public safety, the Police Department does not rely on surveillance technologies at all. Technologies in-use by the Police Department are not intended nor used to surveil our community, and are merely among many tools and strategies that the Police Department may use to enhance its community policing mission. The vast majority of technologies currently in-use by the Police Department are not classified as surveillance at all, and their use has been a proven and effective practice implemented by public safety agencies across the nation and around the world. Most of these technologies have been utilized by countless public safety

agencies for decades, are well known to the greater community, and are widely considered "best practice" for professional and effective public safety agencies.

Generally speaking, the Police Department currently uses only two specific technologies that are unique to Chula Vista: The Drone as First Responder Program (DFR) and the Live911 system. In both cases, as in all cases of technology used by the Police Department, the intent and purpose of these two technologies is to enhance the Department's community policing mission. For example, DFR has helped officers successfully de-escalate numerous situations or solve countless crimes. It has been described as one of the best de-escalation tools in modern existence. Similarly, Live911 gives officers the ability to help victims faster and with better information about what those victims are experiencing.

In general, community policing and compassionate policing are core to the Police Department's mission, and we utilizes technologies like DFR and Live911 to enhance that core.

- ***Which privacy and tech use policies were in force PRIOR TO introduction of each type of technology in Chula Vista - specifically, ALPR, body cameras, drones, heat sensors, social media scanning, Real Time Operations Center, etc.? Who has been providing oversight for each program?***

  Whenever the Police Department considers the deployment or application of any specific tool or technology, that deployment is usually proceeded by the development and implementation of training and policy. Of the specific technologies mentioned in this question, policies were created for ALPR, body worn cameras, and drones before those tools were ever introduced. In the case of the Real Time Operations Center (RTOC), the RTOC has yet to be implemented. The Police Department anticipates developing training and protocols before the RTOC is implemented. The Police Department does not engage in social media scanning, but may view publicly-available social media posts just like any other person or entity. In general, there are no policy requirements governing any person's ability look at public social media posts. Except for infrared cameras manually used by personnel in response to critical operations (search-and-rescue, DFR, SWAT, etc.), the Police Department does deploy or use heat sensors.

- ***How often are audits conducted for each program and where are these audits available to the public?***

  This particular question as written is vague and could relate to a wide variety of programs and technologies. The Police Department is not certain of the exact nature of this question as written. We remain available to provide answers to more specific questions, or can provide further information and context at a future meeting of the task force.