Surveillance Use Policy

Nighthawk LEOVision
San Diego Police Department

PURPOSE

Nighthawk LEOVision is a data analysis tool. This technology is used to perform a visual analysis of large digital data records. It allows data returns from a variety of sources (e.g., social media, search histories, cellular device data) to be synthesized, organized, and reviewed by investigators. The system only allows for analysis of information, it does not gather data sets.

USE

The Department currently has twenty (20) authorized users of the Nighthawk LEOVision tool. The users are primarily assigned to the Homicide Unit and the Crime Analysis Unit and have been vetted and approved by the program administrator as having an investigative need for the technology. Authorized users are assigned an account and must complete a multi-factor authentication (MFA) to log into the system.

This technology does not gather or otherwise obtain data. It is an analytic tool to help investigators review data returns from a variety of platforms to enhance their investigations. This technology significantly reduces the amount of time that would be required to manually review these returns. This technology also allows users to synthesize multiple returns into a searchable data set to establish a timeline of activity and/or communications from a variety of data sources.

DATA COLLECTION

This technology does not gather information or data. This technology is a cloud-based system (Amazon GovCloud which meets or exceeds CJIS requirements set forth by the FBI) that stores digital data record files uploaded by the investigators from legally obtained sources. Legally obtained sources typically include court-approved search warrant returns and data obtained via signed consent.

DATA ACCESS

Access to the Nighthawk LEOVision system is restricted to those users possessing an account assigned to them by the administrator. The users are required to complete an MFA process to access the technology.

DATA PROTECTION

The Nighthawk LEOVision technology is designed with a variety of security tools, techniques, processes, and configurations that meet or exceed the CJIS requirements set forth by the FBI. All data transmissions are connections made using secured connections. All user data and databases are stored via encrypted technology and are maintained in the Amazon government-classified domain.

Access to the Nighthawk LEOVision system is restricted to those users assigned an account. The users are required to complete an MFA process to access the technology. Users uploading data sets

into the system can limit access to those having an investigative need for their case. Users without a right-to-know / need-to-know can be restricted from accessing the information, requiring approval from the uploading user to be granted access. All logins, access requests to the system, and the information uploaded and searched is tracked in an audit trail.

DATA RETENTION

Data uploaded to the Nighthawk LEOVision system will be maintained in the Amazon Government Cloud until the information is no longer needed by the investigator. The data sets uploaded to the system will be maintained in their original form by the requesting investigator. The information uploaded to the system will be removed by the investigator when the need to analyze the data sets no longer exists (e.g., a conclusion or an investigation or adjudication of a criminal case).

PUBLIC ACCESS

As Nighthawk LEOVision is a secured data analysis tool, public access is not allowed. All the data sets uploaded into the system will be maintained in their original form for the period allowed and/or required by law.

Investigators are required to comply with all applicable laws, including the California Electronics Communications Privacy Act (ECPA) when requesting search warrants for data sets, including the notification requirement to users whose data is obtained.

THIRD PARTY DATA SHARING

Information and/or data sets from Nighthawk LEOVision will not be shared with any third party except under situations authorized by law. Information shall only be shared in the following situations:

- Pursuant to a Court Order
- As part of case submission to a prosecuting agency
- As part of an ongoing criminal investigation as allowed by law
- In accordance with all applicable California State Laws

TRAINING

All authorized Nighthawk LEOVision users are provided training in the security features, uploading and analysis of data into the system. Additionally, all users will be required to sign a user's agreement acknowledging access and restrictions to use the system and are required to have a supervisor's approval to have and maintain access to the system. Their immediate supervisor and the system administrator must approve their access.

AUDITING AND OVERSIGHT

The first layer of oversight is in the collection of the data sets. Data sets uploaded to the Nighthawk LEOVision system will typically be obtained via search warrant, consent, or other lawful means. The affidavit for search warrants requires legal sufficiency review by a Deputy District Attorney prior to

submission to the court for review (Department Policy (DP) 4.07). Data sets obtained via consent must comply with DP 4.01,IV Procedures for consensual contacts, consensual searches, stops, pat-downs.

Only authorized users may access the Nighthawk LEOVision system and must complete an MFA process to log in. As part of the login process, users will be required to acknowledge their duty to obey all applicable laws and user agreements. All attempts to access the system and activity in the system are logged on an audit trail for review by the administrator. The administrator will communicate regularly with the vendor to identify potential unauthorized or inappropriate use of the system. Users accessing the system are required to comply with all applicable laws, Department Policies and Procedures, and the signed user agreement. Violations of the laws, Departments Policies, or user agreement terms will subject the user to discipline and/or criminal proceedings or civil process.

MAINTENANCE

The vendor maintains the security and integrity of the Nighthawk LEOVision system. The Nighthawk LEOVision technology is designed with a variety of security tools, techniques, processes, and configurations that meet or exceed the CJIS requirements set forth by the FBI. All data transmissions are connections made using secured connections. All user data and databases are stored via encrypted technology and are maintained in the Amazon government-classified domain. Nighthawk LEOVision is routinely inspected and audited to ensure all security protocols have been updated and follow CJIS protocols.