NCRIC UNMANNED AERIAL SYSTEMS POLICY

NCRIC MISSION

The Northern California Regional Intelligence Center (NCRIC) is a multi-jurisdiction public safety program created to assist local, state, federal, and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and dissemination of criminal threat information. It is the mission of the NCRIC to protect the citizens of the fifteen Bay Area counties within its area of responsibility from the threats of narcotics trafficking, organized crime, as well as international, domestic, and street terrorism-related activities through information sharing and technical operations support to public safety personnel.

UNMANNED AERIAL SYSTEMS (UAS) TECHNOLOGIES

The NCRIC uses Unmanned Aerial Systems (UAS) to support authorized law enforcement and public safety operations of local, state, federal, and tribal public safety agencies. Operated at altitude, UAS and associated sensors collect passive imagery, video, and environmental data that provides essential perspective to officials involved in emergency response, tactical operations, or hazard mitigation. In one common use of the technology, UAS can "spot" a fleeing subject at a crime scene while law enforcement officers secure the location. The data collected is retained for a fixed retention period and only accessed for legitimate law enforcement or public safety purposes as listed below.

PURPOSE

This NCRIC Unmanned Aerial Systems (UAS) Policy defines a minimum set of binding guidelines to govern the use of Unmanned Aerial Systems Data (UAS data) to enable the collection and use of such data in a manner consistent with respect for individuals' privacy and civil liberties. The NCRIC will complete a NCRIC UAS Privacy Impact Assessment (PIA) to address in further detail common privacy and civil liberties concerns regarding UAS technology, which will be available on the NCRIC web site at www.ncric.org.

AUTHORIZED PURPOSES, COLLECTION, AND USE OF UAS

To support the mission of the NCRIC, Law enforcement personnel with a need and right to know will utilize UAS technology to:

-Locate and apprehend subjects of arrest warrants or otherwise lawfully sought by law enforcement

-Locate missing persons, witnesses and victims of violent crime

-Assess damage and investigate natural and manmade disasters

-Protect participants at special events

-Protect critical infrastructure sites

-Deliver Mutual Aid when underlying mission meets the uses outlined in this policy

In gathering, sharing, and storing information the NCRIC complies with all applicable laws, rules, and regulations, including but not limited to, to the extent applicable, the California Values Act (Government Code Section 7284 et seq.). The NCRIC will, consistent with Section 7284.8 (b) work to ensure that databases are governed in a manner that limits the availability of information therein to the fullest extent practicable and consistent with federal and state law, to anyone or any entity for the sole purpose of immigration enforcement.

RESTRICTIONS ON COLLECTION OF UNMANNED AERIAL SYSTEMS DATA

NCRIC UAS may be used to collect data that is within public view but may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution. Absent a warrant or exigent circumstances, operators and observers shall adhere to FAA altitude regulations and shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure). UAS operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions can include, for example, deactivating or turning imaging sensors away from such areas or persons during UAS operations. All users of NCRIC UAS equipment or accessing NCRIC UAS data are required to acknowledge that they have read and understood the NCRIC UAS Policy prior to use. NCRIC UAS shall be used only for legitimate law enforcement or public safety purposes.

TRAINING

All UAS operators will be certified by the Federal Aviation Administration under either a) Certificate of Authorization or b) Title 14, CFR Part 107. Training shall consist of:

- Legal authorities, developments, and issues involving the use of UAS data and technology

- Current NCRIC Policy regarding appropriate use of NCRIC UAS devices, sensors, and data

- Evolution of UAS and related technologies, including new capabilities and associated risks

- Technical, physical, administrative, and procedural measures to protect the security of UAS data against unauthorized access or use

- Practical exercises in the use of the NCRIC UAS devices and data

AUDIT

Access to, and use of, UAS data is logged for audit purposes. Audit reports will be structured in a format that is understandable and useful and will contain, at a minimum:

- The name of the law enforcement user

- The name of the agency employing the user

- The date and time of access

- The specific data accessed

- The supplied authorized law enforcement or public safety justification for access

- A case number associated with the investigative effort generating the UAS data query.

Audit reports will be provided periodically and on request to supervisory personnel at the NCRIC and partner agencies. In addition, no less frequently than every 12 months, the NCRIC will audit a sampling of UAS system utilization from the prior 12-month period to verify proper use in accordance with the above authorized uses. Any discovered intentional misconduct will lead to further investigation, termination of system access, and notification of the user's parent agency for appropriate recourse. In addition, the

auditing data will be used to identify systemic issues, inadvertent misuse, and requirements for policy changes, training enhancements, or additional oversight mechanisms. These UAS audits shall be conducted by a senior NCRIC official other than the person assigned to manage the NCRIC UAS function. Audit results shall then be reported to the Director of the NCRIC.

DATA QUALITY AND ACCURACY

The NCRIC will take reasonable measures to ensure the accuracy of UAS data collected by NCRIC UAS devices and partner agency UAS systems. The NCRIC acknowledges that, in rare instances UAS sensors may inadvertently capture information contrary to the collection guidelines set forth in this policy. Such records will be purged upon identification. Any discovered notable increase in frequency of these incidents from specific UAS devices or support purposes will be followed up with for equipment repairs, sensor calibration, or personnel training as necessary.

PHYSICAL AND ELECTRONIC SECURITY OF UAS DATA

Data collected by UAS sensors is stored in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to law enforcement staff in good standing who have completed background investigations and possess an active security clearance at the "SECRET" or higher level. NCRIC will utilize strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to UAS data during collection and storage.

RETENTION OF UAS DATA

UAS data collected by NCRIC UAS devices or shared from partner agencies shall not be retained longer than 12 months, or the length of time required by the partner agency who is custodian of the record – whichever is shorter. UAS data linked to a criminal investigation will be entered into the relevant NCRIC database(s) and retained for a period of no more than five years. If during the five-year period NCRIC personnel become aware that the UAS data is no longer associated with a criminal investigation, it will be purged from NCRIC databases.

CUSTODIAN OF RECORDS AND RECORDS REQUESTS

Each agency sharing UAS data retains control and ownership as the official custodian of its own records and must independently verify all external information obtained via NCRIC Information Sharing Systems. To the extent permitted by law, requests for information under the California Public Records Act or Freedom of Information Act or similar applicable laws will be directed back to the owner of the requested data.

SYSTEM MANAGEMENT AND ACCOUNTABILITY

The NCRIC shall assign a senior officer who will have responsibility and accountability for managing UAS data and ensuring that the privacy and civil liberties protection and other provisions of this UAS Policy are carried out. This individual shall also have the responsibility for the security of the hotlist information and any UAS Data which is maintained by the NCRIC. It remains, however, the personal responsibility of all officers with access to UAS data to take reasonable measures to protect the privacy and civil liberties of individuals, as well as the security and confidentiality of UAS data.

DISSEMINATION

The NCRIC may disseminate UAS data to any governmental entity with an authorized law enforcement or public safety purpose for access to such data. The NCRIC assumes no responsibility or liability for the acts or omissions of other agencies in making use of the UAS data properly disseminated. Though the NCRIC will make every reasonable effort to ensure the quality of shared UAS data, it cannot make absolute guarantees of the accuracy of information provided.

UAS data may be disseminated to owners and operators of critical infrastructure in circumstances where such infrastructure is reasonably believed to be the target of surveillance for the purpose of a terrorist attack or other criminal activity. In these situations, the NCRIC also will make notification to appropriate local, state, and federal law enforcement agencies. Information collected by UAS devices or sensors shall not be disseminated to private parties, other than critical infrastructure owners or operators, as limited above, unless authorized, in writing, by the Director of the NCRIC or their designee. UAS information shall not be disseminated for personal gain or for any other non-law enforcement purposes.

POLICY REVISIONS

NCRIC UAS policies will be reviewed, and updated as necessary, no less frequently than every 12 months, or more frequently based on changes in data sources, technology, data use and/or sharing agreements, and other relevant considerations. The most current version of the UAS Policy can be found on the NCRIC website at http://www.ncric.org