OWNERSHIP/REGULATION/ADMINISTRATION

1. What entities make up NCRIC? (e.g. public, private)

The NCRIC has members assigned from the following Federal, State, and Local agencies:

Federal Agencies represented consist of:

- Federal Bureau of Investigation (FBI)
- Department of Homeland Security’s Office of Intelligence & Analysis (DHS I&A)
- Drug Enforcement Administration (DEA)

State Agencies represented consist of:

- California Department of Justice (CA DOJ)
- California Highway Patrol (CHP)
- California National Guard (CNG)

Local Agencies represented consist of:

- San Mateo County Sheriff’s Office
- San Francisco Police Department
- San Francisco Sheriff’s Department
- San Francisco Fire Department
- Marin County Sheriff’s Office
- Contra Costa County Sheriff’s Office
- Alameda County Sheriff’s Office
- Santa Clara County Sheriff’s Office
- San Jose Police Department

2. How is NCRIC funded?

The NCRIC's personnel and technology resources are funded through the Office of National Drug Control Policy (ONDCP) and Department of Homeland Security through the State Homeland Security Grant Program and the Urban Area Security Initiative Grant Program.
3. What governing body, if any, provides for oversight of NCRIC?

The NCRIC is governed by the Northern California HIDTA (NCHIDTA) Executive Board. The NCHIDTA Executive Board is comprised of 18 law enforcement executive members, 9 federal and 9 state & local agency members:

- Sheriff - San Mateo County
- SAC - Drug Enforcement Administration
- US Marshal – US Marshals Service
- United States Attorney - Northern District of California
- Sheriff - Contra Costa County
- Chief of Police - San Jose
- Chief of Police - San Francisco
- SAC - Federal Bureau of Investigation
- SAC - Alcohol, Tobacco, Firearms & Explosives
- Director - CA DOJ-Division of Law Enforcement
- Chief of Police - Daly City
- SAC - IRS - Criminal Investigation Division
- District Attorney - Alameda County
- Inspector in Charge - U.S. Postal Inspection Service
- Sheriff - Marin County
- SAC - DHS Homeland Security Investigations
- Sheriff – Alameda County
- SAC – US Forest Service Law Enforcement & Investigation

4. Who or what administers NCRIC’s functions? (e.g. governing board, agents)
   a. Who or what establishes policy for NCRIC?

      The NCHIDTA Executive Board establishes policy.

   b. Are policy setting meetings open to the public?

      No
i. Does NCRIC seek and/or accept public comment on policy matters?

Yes, via public meetings and outreach. City Councils, County Board of Supervisors and Public Safety Agencies may submit requests for presentations to privacyofficer@ncric.ca.gov.

5. Geographic jurisdiction

The Federal Northern District of California that includes the 15 counties from Monterey County to Del Norte County.
6. Legal jurisdiction

a. Does NCRIC initiate investigations in its own name, upon request from member or non-member agencies, or both?

The NCRIC is a government program that is designed to support Federal, State, Local, Tribal (FSLT) Government Organizations and Private Sector Critical Infrastructure and Key Resource Facilities. The NCRIC does not initiate investigations.

b. Statutes or regulations that provide for NCRIC’s authority?

21 USC Chapter 22 Section 1706 provides the foundation for our programs. Each agency assigned to the NCRIC brings their individual agencies authorities from United States Codes to California Codes.

c. Is NCRIC legally confined to certain categories of investigation (e.g. drug trafficking)?

The NCRIC as the designated and federally recognized fusion center for the Federal Northern District of California provides support to federal, state, local and tribal law enforcement agencies major criminal investigations, criminal intelligence support, major criminal/hazards threat identification/information sharing and the collection, analysis and sharing of suspicious activity reports (SARs) as defined by the INFORMATION SHARING ENVIRONMENT (ISE) FUNCTIONAL STANDARD (FS) SUSPICIOUS ACTIVITY REPORTING (SAR). There are no limitations on the type of criminal investigations we support, but we focus on those criminal activities that pose the highest risk to our communities.

https://www.dhs.gov/state-and-major-urban-area-fusion-centers
MEMBERSHIP CRITERIA

1. How does NCRIC determine membership of outside partners (public and private)?

Law Enforcement Membership Qualifications

The standards for membership with the Northern California Regional Intelligence Center as a Law Enforcement Partner, are based on both a "right" and a "need" to know Law Enforcement Sensitive (LES) information. It is vitally important that members of law enforcement have access to information generated or obtained by the NCRIC that will assist them in more effectively accomplishing their day-to-day responsibilities. It is equally important that those that do not have a similar responsibility, or moreover a legitimate need to access LES information, do not obtain it.

As such, these standards are in place to provide the NCRIC staff with the ability to share sensitive information and to ensure that the information is provided to only those who need it and should receive it. Further, these standards are designed with the protection of civil liberties and civil rights in mind, as well as to safeguard active law enforcement investigations and public safety efforts. To qualify as a law enforcement partner the applicant must be currently employed by a law enforcement agency and must serve in an enforcement, investigative, intelligence, analytical or communications role.

Public Safety/Government Membership Qualifications

The standards for membership with the Northern California Regional Intelligence Center, as a Public Safety/Government Partner are based on both a "right" and a "need" to know sensitive information connected to public safety (information that has been categorized as "For Official Use Only," or commonly referred to as "FOUO"). It is vitally important that members of Public Safety/Government have access to information generated or obtained by the NCRIC that will assist them in more effectively accomplishing their day-to-day responsibilities. It is equally important that those that do not have a similar responsibility, or moreover a legitimate need to access "FOUO" information, do not obtain it.
As such, these standards are in place to provide the NCRIC staff with the ability to share sensitive information and to ensure that the information is provided to only those who need it and should receive it. Further, these standards are designed with the protection of civil liberties and civil rights in mind, as well as to safeguard active law enforcement investigations and public safety efforts. To qualify as a Public Safety/Government Partner the applicant must be currently employed by a government agency, or affiliated with a government agency through an executed contract, and must serve in a public safety function, i.e. Firefighter, EMT, Paramedic, Emergency Manager. In addition, employees of agencies that are affiliates of the United States Department of Homeland Security (DHS) qualify for Public Safety/Government membership.

Private Sector Partner Membership

The standards for membership with the Northern California Regional Intelligence Center (NCRIC), Private Sector Partner Program are based on both a "right" and a "need" to know sensitive information connected to public safety (information that has been categorized as "For Official Use Only," or commonly referred to as FOOUO). It is vitally important that members of the private sector, tasked with safeguarding critical infrastructure and key resources, have access to information generated or obtained by the NCRIC that will assist them in more effectively accomplishing their day-to-day responsibilities. It is equally important that those that do not have a similar responsibility, or moreover a legitimate need to access sensitive information do not obtain it.

As such, these standards are in place to facilitate the ability for NCRIC staff to share sensitive information and to ensure that the information is provided to only those who need it and should receive it. Further, these standards are designed with the protection of civil liberties and civil rights in mind, as well as to safeguard active law enforcement investigations and public safety efforts.

Membership / Application Process

Prior to being granted membership with the Northern California Regional Intelligence Center (NCRIC) all Law Enforcement Partners shall undergo a background review. During this process employment verification will be obtained, as well as the applicant's current standing with the organization that he or she represents. As part of the application process, the applicant will be
asked to submit an electronic Non-disclosure Agreement (NDA) which addresses the proper handling of sensitive or controlled information provided to the applicant by the NCRIC. Online training is provided as part of this process. The NDA will be maintained as part of the applicants file.

PURPOSE

1. What is NCRIC’s mission or purpose?

Coordinate the exchange of criminal intelligence, threats and hazards information and facilitate regional communication among Northern California Law Enforcement, First Responders, Government and Private Sector Partners to improve our region's ability to identify, prevent, protect against, mitigate, respond to and recover from the man-made threats and hazards that pose the greatest risk to our region.

To accomplish our mission we collect tips, leads, suspicious activity reporting (SAR) and criminal information; conduct analysis; disseminate intelligence; provide training; provide technology resources; as well as facilitate communications between federal, state and local public safety agencies, homeland security agencies, and private & public sector critical infrastructure partners to help them take action on threats and public safety issues.

The personnel assigned to the NCRIC are dedicated to protecting public safety and the privacy, civil rights and civil liberties of the members of the public we serve.


TRAINING

1. Do member agencies have to complete training of any sort, in order to utilize any services, or to join NCRIC? If yes, please explain.

Access to certain systems require training regarding privacy, civil rights and civil liberties as well as securing and safeguarding classified, sensitive
security information, sensitive but unclassified information, protected critical infrastructure information, and criminal intelligence.


https://ncric.org/html/NCRIC%20ALPR%20PIA.PDF


https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf

https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf


https://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf

https://www.ncirc.gov/Training_Privacy_LineOfficer.aspx

The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety training video was developed by the Global Justice Information Sharing Initiative's Criminal Intelligence Coordinating Council to assist local, state, and tribal law enforcement line officers in understanding their role in the protection of privacy, civil rights, and civil liberties as they perform their everyday duties. The video provides an introductory overview of what privacy, civil rights, and civil liberties protections are; examples of these protections; and the important function line officers have in upholding these protections.

This short video may be used during roll call and in-service training, incorporated into agency distance-learning capabilities, and used to complement other agency privacy-related training efforts.
Launch the training video

FIRST AMENDMENT ONLINE TRAINING

The Responding to First Amendment-Protected Events—The Role of State and Local Law Enforcement Officers videos are designed to assist law enforcement personnel in:

- Understanding their roles and responsibilities as they prepare for and respond to a First Amendment-protected event
- Protecting the privacy, civil rights, and civil liberties of persons and groups participating in a First Amendment-protected event
- Reinforcing fundamental concepts learned at law enforcement training academies and during in-service programs.

When responding to First Amendment-protected events, whether a planned demonstration or a grassroots-developed protest, law enforcement officers must understand their roles and responsibilities. The Bureau of Justice Assistance, with the support of the Global Justice Information Sharing Initiative and the Criminal Intelligence Coordinating Council, developed the Responding to First Amendment-Protected Events—The Role of State and Local Law Enforcement Officers videos to assist agency leadership in providing training to officers and agency personnel as they prepare for and respond to a First Amendment-protected event, in a manner that diligently protects the privacy, civil rights, and civil liberties of persons and groups.

Versions

There are two versions of the video.

Training Video: The longer training video (9 minutes in length) is designed to provide an overview to help law enforcement personnel prepare for and respond to a First Amendment-protected event and understand the privacy, civil rights, and civil liberties issues associated with a First Amendment-
protected event. At the end of the video is a short quiz, with the option to print a certificate of completion.

**Line Officer Roll Call Video:** The shorter line officer roll call video (4 minutes in length) provides an introductory overview of law enforcement personnel’s roles and responsibilities at a First Amendment-protected event. This version is designed to be used during roll call and pre-event briefings.

**Additional Resources**
In addition to this training video, BJA, with the support of Global, has released numerous resources to assist agencies in the ongoing protection of privacy, civil rights, and civil liberties.

- [Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies](#)
- [The Role of State and Local Law Enforcement at First Amendment Events Line Officer Reference Card](#)
- [Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities](#)
- [The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety Line Officer Training Video](#)

CA AG GUIDELINES FOR CRIMINAL INTELLIGENCE FILES

https://www.ncirc.gov/28cfr/

**What Is 28 CFR Part 23 Online Training?**
Welcome to the Bureau of Justice Assistance's Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations Part 23) Online Training Program. This site is a tool for our nation's law enforcement and homeland security professionals. 28 CFR Part 23 is the guideline for law enforcement agencies that operate federally
funded multijurisdictional criminal intelligence systems. The guideline specifically provides guidance for the submission, entry, security, inquiry, dissemination, review, and purge of criminal intelligence information. This site includes an introductory-level training on the regulation's core principles and provides an understanding of privacy and civil liberties concerns related to criminal intelligence information sharing.

**ATTENTION!**
Since this training is limited to sworn law enforcement, support staff, and approved criminal justice and approved public safety users, NEW users can no longer register and be vetted for access to the 28 CFR Part 23 training through the PUBLIC portion of the National Criminal Intelligence Resource Center ([www.NCIRC.gov](http://www.NCIRC.gov)) Web site.

For information about printing your certificate, login issues, passwords, preauthorization codes, changes to your account, or RISS/LEEP, please review the [Frequently Asked Questions](#).

Automated License Plate Reader Training Includes:

- Legal authorities, developments and issues involving the use of ALPRs
- Current policy and use of ALPR systems
- Evolution of the technology
- Technical, physical, administrative, and procedural measures to protect the security of ALPR data against unauthorized access or use
- Practical exercises in the use of the ALPR system
1. What is a SAR?

A SAR is official documentation of observed behavior that is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism. An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). ISE-SAR business rules and privacy and civil liberties requirements will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf

a. What criteria does NCRIC use to determine validity of info?

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Observation</td>
<td>The information flow begins when a person observes behavior that, based on the circumstances, would appear suspicious to a reasonable person. Such activities could include, but are not limited to, expressed or implied threats, probing of security responses, site breach or physical intrusion, cyberattacks, indications of unusual public health-sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other usual behavior or sector-specific incidents. Race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes). The observer may be a private citizen, a government official, or a law enforcement officer.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Activity</td>
<td>Process</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 2    | Initial Response and Investigation | An official of a Federal, State, local, tribal, or territorial agency with jurisdiction responds to the reported observation. This official gathers additional facts through personal observations, interviews, and other investigative activities. At the discretion of the official, further observation or engaging the subject in conversation may be required. Additional information acquired from such limited investigative activity may then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process, which may include reporting it to the FBI's JTTF. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of information systems to continue the investigation. These systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of such systems and the information they may provide include the following:  
  - The Department of Motor Vehicles provides driver’s license and vehicle registration information.  
  - The National Crime Information Center provides warrants; criminal history information; and access to the Terrorist Screening Center, the terrorist watch list, and Regional Information Sharing Systems (RISS).  
  - Other Federal and SLTT systems can provide criminal checks within the immediate and surrounding jurisdictions.  
 When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency’s records management system (RMS). | The event may be documented using a variety of reporting mechanisms and processes, including, but not limited to, reports of investigation, event histories, field interviews, citations, incident reports, and arrest reports. The record may be hard and/or soft copy and does not yet constitute an ISE-SAR. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Process</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 3    | Local/Regional Processing | The agency processes and stores the information in the RMS, following agency policies and procedures. The flow will vary depending on whether the reporting organization is an SLTT agency or a field element of a Federal agency.  
**SLTT:** Based on specific criteria or the nature of the activity observed, the SLTT law enforcement components forward the information to the State or major urban area fusion center and/or FBI’s JTTF for further analysis.  
**Federal:** Federal field components collecting suspicious activity forward their reports to the appropriate resident, district, or division office. This information is reported to field intelligence groups or headquarters elements through processes that vary from agency to agency.  
In addition to providing the information to its headquarters office, the Federal field component provides an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center’s area of responsibility. | The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region, whether collected by SLTT entities or Federal field components. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
<th>Process</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Creation of an ISE-SAR</td>
<td>The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information for suspicious behavior based on his or her training and expertise and against ISE-SAR behavior criteria. Second, based on the context, facts, and circumstances, the analyst or investigator determines whether the information meeting the criteria has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). Once this determination is made, the information becomes an ISE-SAR and is formatted in accordance with the <em>ISE-SAR Functional Standard</em>. The ISE-SAR is then shared with the FBI’s JTTF and appropriate law enforcement and homeland security personnel in the State or major urban area fusion center’s area of responsibility.</td>
<td>Some of this information may be used to develop criminal intelligence information or intelligence products that identify trends and other terrorism-related information and are derived from Federal agencies such as NCTC, DHS, and the FBI. For SLTT law enforcement, the ISE-SAR information may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23.</td>
</tr>
<tr>
<td>5</td>
<td>ISE-SAR Sharing and Dissemination</td>
<td>In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and made accessible to other law enforcement agencies in the NSI SDR. The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters. The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis. The ISE-SAR is also made available to the FBI for investigation.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Activity</td>
<td>Process</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>6</td>
<td>Federal Headquarters (HQ) Processing</td>
<td>At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with NSI participants and other ISE members. The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>NCTC Analysis</td>
<td>When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources. NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure Web site. The Joint Counterterrorism Assessment Team (JCAT), formerly the Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of SLTT entities and, when appropriate, private-sector entities. JCAT is the mechanism that facilitates the sharing of counterterrorism information with SLTT entities.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Activity</td>
<td>Process</td>
<td>Notes</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>8</td>
<td>NCTC Alerts, Warnings, Notifications</td>
<td>NCTC products, informed by the JCAT as appropriate, are shared with all appropriate Federal departments and agencies and with SLTT entities through the State or major urban area fusion centers. The sharing with SLTT entities and the private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and JCAT informed products to help develop geographic-specific risk assessments (GSRAs) to facilitate regional counterterrorism efforts. The GSRAs are shared with SLTT entities and the private sector as appropriate. The recipient of a GSR may use the GSR to develop information gathering priorities or requirements.</td>
<td>NCTC products form the foundation of informational needs and guide collection of additional information. NCTC products should be responsive to informational needs of SLTT entities.</td>
</tr>
<tr>
<td>9</td>
<td>Focused Collection</td>
<td>The information has come full circle and the process begins again, informed by another Federal organization’s product and the identified information needs of SLTT entities and Federal field components.</td>
<td></td>
</tr>
</tbody>
</table>
Gathering and Processing

State, Local, Tribal, Territorial (SLTT) law enforcement agencies, homeland security agencies, or field elements of Federal agencies participating in the NSI gather, document, and report information about suspicious activity in support of their responsibilities to investigate potential criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. Information acquisition begins with an observation or report of unusual or suspicious behavior which, under the circumstances, is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. Behaviors that may be reasonably indicative of pre-operational planning associated with terrorism include, but are not limited to, theft, loss, or diversion, site breach or physical intrusion, cyberattacks, possible testing of physical response, or other unusual behavior or sector specific incidents. It is important to emphasize that context, facts, and circumstances are essential elements for determining the relevance of suspicious behaviors to criminal activity with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).

Regardless of whether the initial observer is a private citizen, a representative of a private-sector partner, a government official, or a law enforcement or homeland security officer, suspicious activity may be reported to an SLTT law enforcement agency, a fusion center, or a local, regional, or national office of a Federal agency. When the initial investigation or fact gathering is completed, the investigating officer or official documents the event as a SAR, in accordance with the ISE-SAR Functional Standard, agency policy, local ordinances, and State and Federal laws and regulations.

The SAR is then reviewed within an SLTT or Federal agency by appropriately designated supervisors or other officials, who may have operational, privacy, and civil liberties responsibilities, for linkages to other suspicious or criminal activity in accordance with agency or departmental policy and procedures. Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to their State or major urban area fusion centers or their local FBI JTTF, where further analysis can take place to determine whether the SAR reflects a Part B terrorism pre-operational behavior, has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism), and is therefore an ISE-SAR. Major
cities, on the other hand, may have trained counterterrorism experts on staff that perform analytic review of the initial reports and filter out those that can be determined not to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).

After appropriate local processing, SLTT agencies make SARs available to their relevant State or major urban area fusion centers. Field components of Federal agencies participating in the NSI forward their SARs to the appropriate regional, district, or headquarters office, employing processes that vary from agency to agency. In those cases in which a local agency can determine that an activity has a direct connection to terrorism, it should immediately provide the information directly to the responsible FBI JTTF for follow-on action against the identified terrorist activity. In those cases in which the local agency can determine that an activity has a direct connection to a terrorist event or pre-operational planning associated with terrorism, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

Analysis and Production

The SLTT agency, fusion center, or Federal agency enters the SAR into an NSI SDR-connected platform. The SAR undergoes a two-part review process by a trained analyst or an investigator to establish or discount a potential nexus to terrorism (i.e., discount that it is reasonably indicative of pre-operational planning associated with terrorism). First, the trained analyst or law enforcement investigator reviews the newly reported SAR information against 16 pre-operational behaviors associated with terrorism that are identified in Part B of this ISE-SAR Functional Standard, keeping in mind—when interpreting the behaviors—the importance of context, facts, and circumstances.15 The analyst or investigator will then review the input against all available knowledge and information for linkages to other suspicious or criminal activity and determine whether the information reflects Part B behaviors.

Second, if the information reflects one or more Part B behaviors, the officer or analyst will apply his or her professional judgment to determine whether, based on the available context, facts, and circumstances, the information has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). If the officer or analyst
cannot make this explicit determination, the report will not be accessible in 
the NSI SDR, although it may be retained in local fusion center or Federal 
agency files in accordance with established retention policies and business 
rules or reported to the FBI or other law enforcement or homeland security 
agencies under other legal authorities. However, if that determination is 
made by the analyst or investigator, the SAR will either be submitted 
immediately to the NSI SDR or forwarded for secondary review and 
approval, which may lead to submission to the NSI SDR. 
As described in Part B, the activities listed as “Potential Criminal or Non-
Criminal Activity” are not inherently criminal behaviors and are potentially 
constitutionally protected; thus, additional facts or circumstances must be 
articulated in the incident.

b. Who makes the determination as to validity, and what would be the 
next steps in the process of investigation?

NCRIC personnel review all reported tips and leads and determine if 
the information meets privacy, civil rights and civil liberty standards 
for processing as a Suspicious Activity Report. The process includes 
an analyst that processes the submitted tip/lead, the review of the 
information by a senior investigator assigned to the NCRIC from a 
local law enforcement agency and the review by a lead intelligence 
analyst. SARs that are submitted to the Joint Terrorism Task Force for 
further review are processed into the FBI’s eGuardian and/or 
Guardian system for further investigation and processing by the JTTF.

c. Are SARs input into any database, and if yes, which ones?

Approved SARs with a potential terrorism nexus are entered into the 
FBI’s eGuardian and/or Guardian system and those with a potential 
criminal nexus are also entered into the NCRIC Intelligence 
Management System.
2. How many were submitted to NCRIC in 2017?

We are currently calculating stats for 2017, but in the first 11 months 733 SARs were processed for de-confliction and determination of a criminal, including terrorism, nexus.

3. How many resulted in initiation of a criminal investigation?

The NCRIC passes SARs to law enforcement agencies related to potential criminal activity, but the agencies are under no obligation to report whether they initiated an investigation. We are collecting end of year statistics related to those SARs identified as criminal (non-terrorism).

4. How many led to filing of a criminal charge?

The NCRIC passes SARs to law enforcement agencies related to potential criminal activity, but the agencies are under no obligation to report whether they initiated an investigation.

5. How many led to a criminal conviction?

The NCRIC passes SARs to law enforcement agencies related to potential criminal activity, but the agencies are under no obligation to report whether they initiated an investigation.

6. What is the retention policy – for those reports that meet criteria? Don’t meet criteria?

Those reports that meet criminal intelligence file guidelines have a five-year retention period, those that meet temporary file requirements have a one year retention and those that do not meet the criteria are purged within 30 days barring additional information.

7. What are the access rights? (e.g. direct need to know; all partner entities; any sworn law enforcement agent)

Authorized personnel with a need and right to know may have access to SAR information.
Right to Know — It is the status of being a person or entity engaged in a specific homeland security and/or critical infrastructure/key resource protection activity that, because of official capacity and/or statutory authority, may have access if there is a need to know.

Need to Know — This is the second part of the two-part test to determine whether dissemination ought to occur. A need to know is a state of facts that supports the legitimacy of access to specific intelligence or homeland security information by a person with a right to know. The need to know must be pertinent to and necessary to the performance of a specific homeland security and/or critical infrastructure/key resource protection activity.

DATA

1. From what sources does NCRIC obtain data?
   a. List of Fed entities

   The list of federal systems does not exist that provides an overview of the entire federal domain. The NCRIC does use proprietary systems from both DHS and the FBI. The systems listed below are a few of those that exist in a listed format:

   - Infrastructure Protection Gateway - Automated Critical Asset Management System (ACAMS)
   - Bomb Arson Tracking System (BATS)
   - Homeland Security Information Network (HSIN)
   - Intelink
   - Law Enforcement Enterprise Portal (LEEP)
   - The National Criminal Intelligence Resource Center (NCIRC)
   - RISSNET™
   - Technical Resource for Incident Prevention (TRIPwire)
b. List of State entities

CA Department of Justice, Department of Motor Vehicles, CalCOP, and participating state law enforcement agencies records are accessible from across the United States through Forensic Logic, Nlets and N-DEx.

c. List of local gov entities

Participating sheriff’s offices and police departments records are accessible from across the United States’ 18,000 state and local law enforcement agencies through Forensic Logic, Nlets and N-DEx.

d. List of private partners

We do not access private partner’s data.

e. List of commercial vendors

The NCRIC uses numerous commercial and no cost open source databases. The commercial vendors include Vigilant Solutions, Thomson Reuters, FirstTwo, and LexisNexis.

2. What types of data does NCRIC host for its partners? (e.g. ALPR)

At the election of law enforcement partners, the NCRIC can host Law Enforcement Records (arrests, calls for service), ALPR data, court ordered electronic intercept data, as well as voice and video surveillance data for specific regional criminal investigations.

a. Who manages the data storage?

Data is managed by NCRIC IT and Investigative Equipment Program Personnel
b. Where is data stored?

Data is stored in a secure federal facility that requires a minimum of a Secret Security Clearance to access. The facility has 7 days a week/24 hours a day armed security and requires three levels of physical security to access.

3. What types of data does NCRIC collect on its own, if any?

The NCRIC’s data collection is limited to those categories of criminal and open source information requested to support federal, state and local law enforcement’s criminal investigations, protection of critical infrastructure sites and the protection of major special events or public gatherings that may be targeted by individuals planning acts of violence.

4. What rules, policies, or agreements determine access rights to data collected or hosted by NCRIC?

Nondisclosure Terms & Conditions

NONDISCLOSURE TERMS & CONDITIONS AGREEMENT BETWEEN THE NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER (NCRIC) AND THE APPLICANT PERTAINING TO THE PROPER HANDLING OF "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION.

1. I hereby accept the obligations contained in this Agreement in consideration of my being granted access to FOUO information. As used in this agreement, FOUO information is marked or unmarked FOUO information, including oral communication, which is FOUO information under the standards of the NCRIC. I understand and accept that being granted access to FOUO information, special confidence and trust shall be placed in me by the NCRIC.

2. I hereby acknowledge that I have read the attached document, titled "Safeguarding Sensitive but Unclassified Information" and a copy has been provided to me, and that I have received a security indoctrination concerning the nature and protection of FOUO information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate
disclosing this information have been approved for access to it, and that I understand these procedures. I also acknowledge that I have been advised that the NCRIC adheres to 28 CFR (Code of Federal Regulations) Part 23 guidelines, with respect to criminal intelligence files, and will only share criminal intelligence information with other law enforcement agencies that adhere to (same).

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of FOUO information by me could cause damage or irreparable injury to the NCRIC. I hereby agree that I will never divulge FOUO information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the NCRIC to receive it; or (b) I have been given prior authorization from the agency responsible for the information that such disclosure is permitted; or (c) the recipient has the "need to know" in order to perform their official, public safety duties. I understand that if I am uncertain about the classification status or handling control authority of information received from the NCRIC, I am required to confirm from an authorized NCRIC official that the information is FOUO before I may disclose it, except to a person as provided in (a) or (b) above.

4. I have been advised that any breach of this Agreement may result in the termination of my affiliation with the NCRIC.

5. I have read this agreement carefully and my questions, if any, have been answered.

Safeguarding Sensitive but Unclassified Information
For Official Use Only (FOUO)

FOUO is the marking used by DHS to identify Sensitive but UNCLASSIFIED information within the DHS community, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other operations essential to the national interest and that is not otherwise covered by a statute or regulation.

Other government agencies and international organizations frequently use different terms to identify sensitive information, such as "Limited Official Use (LOU)," "Official Use Only (OUO)," and in some instances "Law Enforcement Sensitive (LES)." In most instances the safeguarding requirements for this type of information are equivalent to FOUO.
However, other agencies and international organizations may have additional requirements concerning the safeguarding of their sensitive information. When available, follow the safeguarding guidance provided by the other agency or organization. Should no guidance be available the information will be safeguarded in accordance with FOUO guidance provided in this document.

It is not permitted to mark information as FOUO to conceal government negligence, ineptitude, or other disreputable circumstances embarrassing to a government agency.

Marking

Information determined to be FOUO will be sufficiently marked so that persons granted access to it are aware of its sensitivity and protection requirements. At a minimum, it is marked on the bottom of each page "FOR OFFICIAL USE ONLY." Materials containing specific types of FOUO information can be further marked with an applicable caveat, e.g. "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Additional access and dissemination restrictions may also be cited as the situation warrants.

Markings typically associated with classified information such as originator information, downgrading instructions, and date/event markings are not required on FOUO documents.

Access and Dissemination

A security clearance is not needed for access to FOUO information. Access to FOUO information is based on a "right-to-know" and "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's right-to-know or need-to-know, the holder should request dissemination instructions from the NCRIC.

FOUO information may be shared with other agencies, federal, state, private sector, or local government and law enforcement officials, provided a need-to-know has been established and the information is shared in the furtherance of an official government activity, to include homeland defense, and no dissemination restrictions have been cited by the originator.
When discussing FOUO information over a telephone, use of the STU-III or STE (secure/encrypted telephone) is encouraged, but not required.

FOUO information may be transmitted via non-secure fax machine, although the use of a secure fax is encouraged. Where a non-secure fax machine is used, ensure that a recipient is present at the time of the fax and that the materials faxed will not be left unattended or subject to unauthorized disclosure.

FOUO information may be transmitted over official email channels. However, it shall not be sent to personal email accounts. For added security when transmitting FOUO information by email, password protected attachments may be used with the password transmitted or otherwise communicated separately.

FOUO information may be mailed by regular US Postal Service first class mail or any commercial mailing service.

Do not enter or post any FOUO information on any public website.

Do not post FOUO information in an area accessible to the public or people who do not have a "right to know" (such as janitorial workers/inmates).

Storage

When unattended, FOUO information shall be stored in a locked filing cabinet, locked desk drawer, a locked overhead storage compartment such as a furniture credenza, or a similar locked compartment. Information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without the need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

Destruction

• Hard copy FOUO materials will be destroyed by shredding, burning, pulping, or pulverizing, sufficient to assure destruction beyond recognition and reconstruction.

• After destruction, materials may be disposed of with normal waste.
• Electronic storage media shall be sanitized appropriately by overwriting or
degaussing.

• Paper products or electronic media containing FOUO information will not
be disposed of in regular trash or recycling receptacles unless the materials
have been destroyed as specified above.

Incident Reporting

• Compromise, suspected compromise and suspicious or inappropriate
requests for FOUO information shall be reported to the NCRIC.

• Additional guidance or assistance can be obtained by contacting the
NCRIC @ (866) 367-8847 / dutyofficer@ncric.ca.gov or DHS/FBI security
officers.

a. Please provide template agreements for a public entity (local, state,
   fed) and private partner

   Please see below for the contributing agency agreement template:

   **MEMORANDUM OF UNDERSTANDING AND AGREEMENT**

This Memorandum of Understanding (hereinafter “MOU” or “Agreement”) is
entered into by and between the Northern California Regional Intelligence Center
(“NCRIC”) and the law enforcement or public safety agency indicated on the
signature page “Member Agency.”

WHEREAS, Member Agency provides public safety services; and

WHEREAS, NCRIC is a multi-jurisdictional public safety information fusion center
managed under the Northern California High Intensity Drug Trafficking Area
(NCHIDTA) Executive Board that assists public safety agencies with the collection, analysis and dissemination of information related to criminal threats; and

WHEREAS, NCRIC and Member Agency are dedicated to the most efficient utilization of their resources and services in public safety endeavors; and

WHEREAS, NCRIC and Member Agency are committed to cooperation and coordination in providing the highest level of safety services to the public, guided by the principle that cooperative efforts are in the public’s best interest; and

WHEREAS, Member Agency supports the sharing of information contained within its electronic data systems in furtherance of collaboration with other appropriate public safety entities, through integrated systems of information technology that the NCRIC has developed, established, or maintains; and

WHEREAS, NCRIC and Member Agency recognize the need to protect Member Agency’s ownership and control over its shared information, to optimize the means through which shared information is accessed or analyzed, and to protect privacy and civil liberties in accordance with the law; and

NOW, THEREFORE, NCRIC and Member Agency hereby agree to conditions set forth in this MOU:

Purpose

This agreement provides a framework for Member Agency and NCRIC to facilitate data collaboration – outward sharing of information from Member Agency, as well as providing Member Agency with shared information from other sources - in a manner that protects the rights and authority of Member Agency, allowing participation in sharing environments while simultaneously retaining ownership of its data and control over which records are shared, how they are shared, and with whom.
1) Definitions and other Terminology

Member Agency: the law enforcement or public safety organization whose leadership has signed this agreement and actively participates in information sharing with other law enforcement or public safety entities through assistance from the NCRIC.

Data: electronic records, analyses, images, and other information associated with incidents, persons, or objects, originally created by Member Agency and existing in a Member Agency system or database.

Contributed Data: records originating from Member Agency that Member Agency has elected to share with other appropriate parties.

Shared Data: the aggregate pool of shared information from Member Agency and other contributing sources, made available via the NCRIC or facilitated by NCRIC funding, technology systems, and/or efforts.

Authorized Users: personnel from the Member Agency that have the appropriate clearance and authority to utilize and access shared data as a function of their employment, in support of law enforcement or public safety.

2) Rights, Powers and Authority

This Agreement does not limit the rights, powers, and authority of either party.

Nothing in this Agreement shall be construed to require either party:

a) to disclose any information it determines, in its sole discretion, it does not have the ability or authority to disclose; OR
b) to perform any act that it determines, is contrary to law or public policy; OR

c) to provide personnel, equipment, or services to the other party; OR
d) to modify, restrict, or inhibit utilization of any information technology systems

3) **Data Sharing**

Recognizing that Member Agency has sole discretion to choose exactly the information it wishes to contribute, the audience to which contributed data may be shared, and the unbridled authority to redact or exclude information: Member Agency agrees to promote comprehensive, timely, and accurate data sharing.

Member Agency grants authority to NCRIC to further share the information contributed by Member Agency with other public safety entities who possess a need to know and right to know the shared data, except where explicitly denied by the Member Agency. Member Agency grants authority to the NCRIC to execute information sharing agreements with other agencies, and to expand, incorporate, and unify additional shared information from other agencies. Such agreements will not require further review or approval by Member Agency. Such agreements will have no material differences that would adversely affect or contradict the obligations of this agreement.

Member Agency grants authority to the NCRIC to provide contributed data into software platforms to optimize law enforcement sharing, search, reporting, or analytic capabilities. In any such system connection that would lead to Member Agency’s contributed data residing outside of NCRIC owned and operated infrastructure – such as a commercial datacenter or “Government Cloud” offering – the NCRIC will provide Member Agency with no fewer than 90 days’ advance notice and an opportunity to opt-in or opt-out of the connection.

Member Agency retains right to later determine that any contributed data should no longer be shared, or to opt out of any specific sharing software platform. In these instances, NCRIC will make every reasonable effort to accommodate the updated preferences of Member Agency within ten business days.
In gathering, sharing, and storing information, and in all other respects in performing acts related to this Agreement, the parties will comply with all applicable laws, rules, and regulations.

4) **Information Ownership and Release**

Member Agency remains the official custodian of all contributed data. To the fullest extent permissible by law, all requests for information, including but not limited to inquiries under the California Public Records Act or Freedom of Information Act, will be referred to the Member Agency that is the originator of the requested data. The Member Agency that is the originator of the requested data will be responsible for responding to the request and will indemnify and defend the NCRIC from any action brought related to Member Agency’s response (or lack thereof).

5) **Authorized User Access and User Responsibilities**

Member Agency is responsible for management of its Authorized User accounts and the activities of its Authorized Users.

Member Agency agrees that all Authorized Users shall be current employees in good standing that are legally entitled to view law enforcement sensitive content as part of their assigned duties in support of public safety.

If for any reason a user is no longer eligible for such access, including ending his/her employment with the agency, the agency will ensure access is timely removed.

Member Agency agrees that shared information is be used solely for authorized purposes consistent with the law. Member Agency shall not use or share the information for any unauthorized purposes, and Member Agencies agree that such actions will result in the Member Agency or its offending Authorized User being revoked access to the system.

Member Agency will ensure that its Authorized Users will not access shared data by using a name, password, or any authentication mechanism that is
assigned to another person. Member Agency will ensure that Authorized Users will not share passwords with another individual, nor allow another user to utilize the system under their credentials.

Member Agency will ensure that shared data will only be accessed from electronic devices that meet all current security requirements for accessing law enforcement information. Such policies should also forbid utilization of personal / non-agency devices, or enforce appropriate security requirements on those devices to meet CJIS compliance.

6) **No Guarantee of Accuracy**

Member Agency acknowledges that shared data may or may not be accurate. Member Agency further understands that neither the suppliers of shared data nor NCRIC are warranting the accuracy of such information. Member Agency agrees to take necessary steps to appropriately verify the accuracy of any and all information before taking any action based upon it.

Member Agency understands and agrees to put in place a policy that clearly sets forth a requirement of verification and so inform each Authorized User.

Member Agency agrees to use shared data as a pointer system for investigative leads or guidance, and not as the sole source of probable cause for law enforcement actions.

7) **Information Security and Standards Compliance**

Data exchange and user access shall be achieved using encryption, private networks, or other configurations that follow current best practices for information technology, and must remain current and compliant with all applicable standards.

Member Agency and NCRIC shall store information, whether electronic or hardcopy, only in a manner that is compliant with all applicable physical security and cyber security requirements. Data shall be retained, purged, and destroyed in accordance with all applicable standards.
8) **Mutual Indemnification**

Each party shall indemnify, defend, protect, hold harmless, and release the other, its officers, agents, and employees, from and against any and all claims, loss, proceedings, damages, causes of action, liability, costs, or expense (including attorneys' fees and witness costs) arising from or in connection with, or caused by any act or omission of such indemnifying party or its agents, employees, contractors, subcontractors, or invitees. This indemnification obligation shall not be limited in any way by any limitation on the amount or type of damages or compensation payable to or for the indemnifying party under workers' compensation acts, disability benefit acts, or other employee benefit acts.

9) **Costs**

Execution of this agreement shall not be construed to require NCRIC or Member Agency to incur any new costs. For any potential costs associated with information sharing or access to shared information, either party may determine in its sole discretion, whether or not to incur those costs.

10) **Partial Invalidity**

If any terms or conditions of this Agreement shall to any extent be judged invalid, unenforceable, or void for any reason whatsoever by a court of competent jurisdiction, the remaining terms and conditions of this agreement shall continue in full force and effect.

11) **Effective Date and Term of MOU**

This agreement shall remain in effect until terminated by either party by giving written notice.
b. If you are able to provide a screenshot of info that would be provided to a Fed partner/State partner/Private partner, that would be helpful for our review (e.g. one of these partners performs an ALPR query – what info do they receive?)

Only law enforcement personnel that agree to use policies: peace officers, agents, analysts, dispatchers and the law enforcement IT personnel that manage the system.

ALPR may only be accessed to:

- Locate stolen, wanted, and subject of investigation vehicles
- Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement
- Locate witnesses and victims of violent crimes
- Locate missing persons
- Identify vehicles associated with targets of criminal investigations
- Protect participants at special events
- Protect critical infrastructure sites

No data is given or access provided to the public.

NCRIC data is stored in a secure law enforcement facility with 24/7 security, physical access to data is limited to personnel with a “Secret” or higher clearance, and multi-factor authentication, encrypted communications, cyber protective and physical protective measures are in place at the NCRIC to mitigate the risks of unauthorized access, destruction, use, modification, or disclosure of ALPR information.

ALPR data includes ALPR device name, vehicle license plate image, date/time, GPS location of capture, original photo as captured by ALPR camera, and potentially alert data if the plate matched an entry on an investigative hotlist such as “Stolen Vehicles”.

c. Does NCRIC retain a user access log for each database it hosts, and the reason for such access?

Yes
5. Who or what determines retention length?


a. If there are written retention policies, please provide an illustrative example or two for our review.

28 CFR Part 23:

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

CA Attorney General Guidelines for Criminal Intelligence Files

- Once data has been lawfully collected, it goes through several steps that will terminate in one of the following three results:
  - Destruction of the data because there is no criminal predicate and no reasonable likelihood of developing a criminal predicate,
  - Determination that, although no criminal predicate then exists or no person or group has yet been linked to the predicate, there is a reasonable likelihood that within a reasonable period of time (DOJ uses one year) evidence of the predicate or identity of the person or group will be available, or
  - Determination that a criminal predicate exists.
6. Are steps taken to ensure accuracy of data? If yes, please explain.

   a. Is there a procedure for contributing agencies to flag, correct or remove inaccurate data? If yes, please explain.

   The NCRIC reviews each non-automated data element received and processed as a Suspicious Activity Report (SAR), tip or lead with the assistance of an intelligence analyst and in some cases an intelligence officer. If there are any questions related to the accuracy of the information the intelligence analyst or officer contacts the submitting agency for clarification. The analyst develops a report that is reviewed by a lead analyst and after approval of a supervisor a partner update is sent back to the agency and regional public safety partners with a retention timeline for when data is to be purged as well as the mechanism for updating the information. For agency contributed data that is received in an automated fashion from systems such as ALPR and records management systems (RMS), the NCRIC does not ensure accuracy of the contributing agencies’ data. The NCRIC clearly states to participating law enforcement agencies that there is:

   **No Guarantee of Accuracy**

   Member Agency acknowledges that shared data may or may not be accurate. Member Agency further understands that neither the suppliers of shared data nor NCRIC are warranting the accuracy of such information. Member Agency agrees to take necessary steps to appropriately verify the accuracy of any and all information before taking any action based upon it.

   Member Agency understands and agrees to put in place a policy that clearly sets forth a requirement of verification and so inform each Authorized User.

   Member Agency agrees to use shared data as a pointer system for investigative leads or guidance, and not as the sole source of probable cause for law enforcement actions.
7. Are steps taken to ensure security of hosted and transmitted data? If yes, please explain.

Yes, multi-factor authentication, encrypted communications, cyber protective and physical protective measures are in place at the NCRIC to mitigate the risks of unauthorized access, destruction, use, modification, or disclosure of transmitted data.

8. Which outside data sharing entities or databases does NCRIC link to? (e.g. NCIC, CLETS, fusion centers in other states)

The NCRIC contributes/pushes/uploads vetted Suspicious Activity Reports (SARs) shared by partner public safety agencies and the public to the Nationwide Suspicious Activity Reporting Initiative (NSI) through the FBI’s eGuardian System. The NCRIC uses many databases and connections to data sharing entities but we do not directly link information to outside data sharing entities or databases.

9. Is there a process for members of the public to request copies of records that may be stored by NCRIC which contain their own personal information? If yes, please explain.

The NCRIC accepts requests for records at privacyofficer@ncric.ca.gov.

MONITORING OF PUBLIC PLACES

1. What criteria does NCRIC use to determine whether to monitor a public event or gathering?

The NCRIC does not monitor public events or gatherings.

2. When performing such monitoring:
   a. What types of data might be collected?
   b. How long would such data be retained?
   c. Who would have access to such data, and under what conditions?
The NCRIC does not monitor public events or gatherings. The NCRIC does provide support to federal, state and local law enforcement upon request to protect major public events or gatherings that may be targets of violence using real-time open source analysis to identify individuals that may be using threatening language directed at a specific event or individuals attending the event. Any data collected is retained and shared within the scope of 28 CFR Part 23 and the California Attorney General’s Criminal Intelligence File Guidelines.

- [https://it.ojp.gov/documents/d/Recommendations%20for%20First%20Amendment-Protected%20Events%20for%20state%20and%20local%20Law%20Enforcement.pdf](https://it.ojp.gov/documents/d/Recommendations%20for%20First%20Amendment-Protected%20Events%20for%20state%20and%20local%20Law%20Enforcement.pdf)

- [https://it.ojp.gov/documents/d/Role%20of%20State%20and%20Local%20Law%20Enforcement%20in%20First%20Amendment%20Events.pdf](https://it.ojp.gov/documents/d/Role%20of%20State%20and%20Local%20Law%20Enforcement%20in%20First%20Amendment%20Events.pdf)


**SANCTUARY**

1. Has SB54’s adoption (California Values Act) caused NCRIC to implement any changes to operations and/or access rights? If yes, please explain.

   Yes. In anticipation of SB 54 becoming law the NCRIC Director notified the regional head of ICE – Enforcement and Removal Operations (ERO) that his organization’s access to data would require compliance with the new California law.

   a. Same question for SB31 (California Religions Freedom Act)

   No
2. When a (possible) policy conflict exists between a sanctuary city like Oakland, which may provide data to NCRIC, and ICE, which may access data at NCRIC, what steps has or will NCRIC taken to ensure that data collected by one party for a specific purpose is not used by another party for a different purpose?

   The originating agency controls their data and access permissions. Each agency request must be accompanied by a criminal case/criminal investigative purpose.

3. Has ICE used NCRIC data to identify, locate, or detain undocumented immigrants?

   No, the NCRIC supports criminal investigations, criminal intelligence and suspicious activity reporting and does not support solely administrative immigration status related operational activities.

   a. If yes, what NCRIC data was used?
   b. If yes, how many undocumented immigrants?

DOCUMENT REQUESTS

Please provide one or two of each category, for illustrative purposes (redact if necessary):

1. Any efficacy reports as to crime fighting in NCRIC’s possession (e.g. ALPR hits that lead to recovery of stolen vehicles, SARS that lead to convictions, drug seizures)

   The following information was collected over the first 11 months of 2017:

   • 75 Special Event Threat Assessments (SETAs) for our regional public safety partners.
   • 161 Situational Awareness products regarding criminal threats, including terrorism.
   • 733 SARs for de-confliction and determination of a criminal, including terrorism, nexus.
   • 807 Requests for Information from law enforcement agencies.
• 437 Requests to produce intelligence background packages for subjects under investigation by federal, state and local law enforcement agencies.
• 162 Investigative case support requests.
• 93 LES and FOOU Partner Update Briefs regarding SARs, regional crime trends and national threat reporting.
• 28 Complex Drug Trafficking Cases Provided Full Analytical Support
• 3 Organized Crime Drug Enforcement Task Force (OCDETF) Cases Supported
• 229 NC HIDTA Request of Information Support
• 82 Investigative Leads Referred for Services
• 167 Financial Suspicious Activity Reports Reviewed
• 7,530 Criminal Investigation Event Location Deconflictions Submitted
  o 801 Positive Event Deconflictions
• 36,962 Criminal Case Subject Deconfliction Submitted
  o 7,323 Positive Case Subject Deconfliction
• $316,473,385 wholesale street profits denied drug traffickers from the seizure of narcotics
• $8.8 million cash assets seized

2. ALPR Query Reports for 2017 (NCRIC has in the past produced both quarterly and monthly reports, showing partners that accessed ALPR data)

   The NCRIC only produces access reports based on agency requests and those reports are the property of the requesting agency.

3. Retention policy (templates, redact if necessary)


4. Access rights policy (e.g. template MOU for public agency, private partner)

5. Audits (internal and 3rd party report, access rights, accuracy of data, policy violations; redact if necessary)

   The annual assessment process provided through the Department of Homeland Security is not available to the public.

6. SAR retention policy, and access rights agreement


7. Any policy that pertains to monitoring of public spaces

   The NCRIC does not monitor public spaces.

8. Any existing system maps outlining technical infrastructure including connections of systems, networks, or databases.

   The NCRIC does not publicly release sensitive security information.