Situation Awareness & Collaboration Tool

New Agency Onboarding & Registration Policy and Procedures

Version: 1.0

Date: August 2017

Author: SCOUT Principal Agencies

Document Control

Document Version

Version	Reason	Date
1.0	Initial Version	8/16/2017

Document Approvals

Name	Title	Date Approved	Version Approved
Joe Tyler	Assistant Deputy Director, CAL FIRE	8/16/2017	1.0
Dan Bout	Assistant Director, Cal OES	8/16/2017	1.0

1 Purpose

The purpose of this document is to describe the process for new agencies to join the SCOUT Program.

2 Onboarding Process Overview

Agencies interested in joining the SCOUT Program must complete the following onboarding and registration steps:

- Review: SCOUT FAQs
- Review: Onboarding and Registration Policy & Procedures
- Review: Responsibilities Matrix (please read carefully)
- Review: Concept of Operations and Technical & Operational Support Plan - available at www.caloes.ca.gov/scout
- Complete and return Appendix A: SCOUT Onboarding Checklist
- Review, sign and return Appendix B: SCOUT Agency Participation Agreement (attached)
- Review, sign and return Appendix C: SCOUT Agency Administrator Agreement (attached)
- Complete and return Appendix D: Agency Administrator Designation Form

2.1 List of attachments

The following attachments are available for reference:

- Exhibit A: SCOUT FAQs
- Exhibit B: SCOUT User Acceptable Use Agreement
- Exhibit C: SCOUT Terms & Conditions

3 SCOUT Overview

The California Governor's Office of Emergency Services (Cal OES)—in association with the California Department of Forestry and Fire Protection (CAL FIRE) and through a strategic partnership with the Department of Homeland Security's Science & Technology Directorate (DHS S&T)—acquired the Next-Generation Incident Command System (NICS) software for use by California's emergency services professionals. The NICS software was developed by MIT Lincoln Labs—with direct input from field-level first responders and incident commanders, primarily California first responders—as a tactical incident management information sharing platform.

The California deployment of the NICS software is called Situation Awareness and Collaboration Tool (SCOUT). SCOUT provides an information sharing environment to facilitate operational and tactical incident collaboration among California emergency responders and interagency situational awareness for local, tribal, state, and federal partners on small to extreme scale homeland security incidents, such as natural disasters, technological hazards, intentional attacks, and human-caused emergencies. SCOUT enables incident responders and collaborators to share incident information, such as

- Incident Location
- Area or Perimeter of Impact
- Road Closures
- Evacuation Areas
- Weather Conditions
- Utilities
- Resource Automated Vehicle Locator (AVL) Information
- Tactical Response Operations

3.1 Primary Features

The primary features of SCOUT are:

- Incident Map for shared common Situational Awareness
- Working Map for coordinated Tactical Incident Response
- Theme-specific Collaboration Rooms for Tactical Incident Collaboration, such as Evacuations and Incident Communication Network.
- Digital whiteboard for Incident Log and Private Chat
- Standard Base Maps

- Real-time Weather, including Remote Automated Weather Stations (RAWS) stations
- Statewide data sets, such as facilities, transportation and jurisdiction areas
- Local data sets, such as pre-plans and fire hydrants
- Local Automated Vehicle Location (AVL) data feeds

See the **SCOUT Concept of Operations** for full overview of features and operational workflows.

4.0 Policies, Practices and Procedures (PPPs)

4.1 Eligibility Requirements

Local, regional, and state government agencies with a mission in public safety are eligible to access SCOUT. Participating agencies have the responsibility to identify and control individual user accounts within its agency. User accounts should be limited to those that have a legitimate business purpose for view, read/write, and/or GIS administrative account access. Misuse of access right will result in termination of user and/or agency eligibility.

Non-government agencies with a direct mission in public safety may apply for access. Eligibility will be reviewed and assessed by the SCOUT Program Office and granted at its discretion.

To become a **SCOUT Participating Agency**, agencies must meet one of the following set of requirements:

1) Government Agencies
    - Has an emergency response, emergency management, public health, or public safety defined mission within the State of California.
    - Agrees to the SCOUT Concept of Operations, Operational & Technical Support Plan, Onboarding and Registration policy and procedures, and completes proper agreement forms.
    - Receives approval from a Principal Agency Administrator or Executive.

Examples include: Local Fire, Law Enforcement, or Emergency Services; County Fire, Law Enforcement, or Emergency Services; and Federal Supporting Partners, such as Federal Emergency Management Agency, US Forest Service, Bureau of Land Management, and locally-based military installations.

or

2) Non-governmental Organizations (NGO)

- Is an approved "Cooperating or Assisting Organization" for emergencies within the State of California—as defined by the State Emergency Management System (SEMS) and/or the National Incident Management System (NIMS).
- Receives sponsorship from an existing government SCOUT Participating Agency.
- Agrees to follow the SCOUT Concept of Operations, Operational & Technical Support Plan, Onboarding and Registration policy and procedures, and completes proper agreement forms.
- Receives approval from a designated Principal Agency Administrator or SCOUT Executive Committee Member.

Examples include: non-profit support services, such as the American Red Cross and local or regional utilities, such as transportation, water, power, sanitation, and gas.

4.2 Agency Participation Expectations

Participating Agencies are expected to:

- Actively participate in the use of SCOUT for tactical incident management, coordination and/or collaboration. Examples include:
  - Use of SCOUT for tactical incident operations on home agency incidents.
  - Use of SCOUT for supporting incident operations on mutual aid incidents.
  - Use of SCOUT for emergency management supporting tactical operations.
- Identify a designated **SCOUT Agency Administrator** for your agency.

  The Administrator must:
  - Satisfactorily execute the responsibilities of Agency Administrator pursuant to the SCOUT Concept of Operations, Operational Support Plan, Agency Administrator Agreement, and all published Administrator instructions.
- Optional: If the Participating Agency requests to establish a real-time feed of SCOUT data into their local system, the Participating Agency must agree to also share agreed upon local incident information with SCOUT, i.e. two-way sharing. (Participating Agencies are not required to share their local incident data if they do not request electronic feeds of incident information from SCOUT.)

Mutual Aid Use:

- Willing to train agency users for use of SCOUT on mutual aid deployments.

4.3 Agency Participation & User Agreements

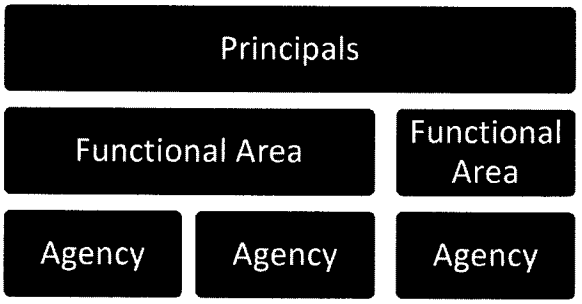
All agencies accessing SCOUT must have on file an Agency Participation Agreement signed by the agency head. All Agency Users will be required to read and agree to the SCOUT Acceptable Use Agreement and Terms of Use. New SCOUT agreements shall be completed when the head of the agency changes, or upon request from Cal OES.

Each agency accessing SCOUT must submit an Agency Participation Agreement and be approved for access by a Principal Administrator or Agency Executive. Each agency must identify a SCOUT Agency Administrator to act as the primary contact to Cal OES for their agency. The SCOUT Agency Administrator will be responsible for authorizing and training users in their jurisdiction and auditing the use of SCOUT by their users.

4.4 Security Requirements

All agencies applying for SCOUT access must adhere to the requirements established in these policies, practices, and procedures and state and federal law. If access is granted, it is each agency's responsibility to ensure, on a regular basis, the requirements of these policies, practices, and procedures and applicable law is reviewed to ensure the agency is continually in compliance.

4.5 Operational Structure



State Agency Regional Staff

Local Agencies or State Agency Field Units

4.5.1 Agency Administrator

Each Local SCOUT Participating Agency must designate a SCOUT Agency Administrator who serves as the administrator with Cal OES on matters pertaining to the use of SCOUT. The SCOUT Agency Administrator will be responsible for ensuring compliance with Cal OES, state and federal policies and regulations. The SCOUT Agency Administrator's responsibilities shall be designated by Cal OES on a SCOUT Agency Administrator Responsibilities sheet (Appendix C). If an agency requests to have other than a permanent, full-time employee as its SCOUT Agency Administrator, Cal OES must be notified in writing and will review the request. Agencies must complete and return the Agency Administrator Designation Form (Appendix D) to the SCOUT Program Office for initial designation and immediately upon any changes in designation of the Agency Administrator.

The designated Agency Administrator is responsible for

- Agency Org Account Maintenance and Administration
- Agency User Account Set Up and Maintenance and Administration
- Agency User Training
- Agency User Tier 1 Helpdesk Support
- Agency Point of Contact for SCOUT Communications

State Agencies that participate as a Principal Agency will maintain their own internal chain of command for their SCOUT Administrators. For example, CAL FIRE Units will designate a Unit SCOUT Administrator who reports to their regional Functional Area Administrator (South Ops or North Ops) and up through to the Principal Administrator.

4.5.2 Functional Area Administrator

Each Principal Agency will designate Functional Area Administrator(s) per their regional organizational structure. The Functional Area Administrator is responsible for Participating Agency management, coordination and support, including Agency Administrator training within their designated area of responsibility.

4.5.3 Principal Administrator

Each Principal Agency will designate a Principal Administrator. The Principal Administrator is responsible for SCOUT policy implementation and adherence, platform management, operational coordination and Functional Area Administrator training within their designated agency's purview.

For more information on the SCOUT governance structure refer to the **SCOUT Charter** available at www.caloes.ca.gov/scout.

4.6 Rules

SCOUT rules are designed to provide the most efficient operating system consistent with the needs of emergency management. Adherence to the rules will ensure the maximum effectiveness of SCOUT. Violations of these policies, practices, and procedures may result in termination of access rights, as determined by a Principal Agency.

Each Participating Agency is required to comply with all SCOUT policies, practices and protocols, including but not limited to:

- SCOUT Concept of Operations
- SCOUT Operational & Technical Support Plan
- SCOUT Onboarding and Registration Policy and Procedures, supporting agreements and instructions
- SCOUT standard operating procedures and user instructions, including all help guides and instructions developed to aid SCOUT users.

4.7 Information Technology Security Incident Response Reporting

Agencies shall immediately notify Cal OES of security incidents or data breaches affecting their systems, network or any infrastructure. The participating agency shall immediately notify the SCOUT Program Office by electronic mail when a security incident(s) is known. Participating Agency support staff are expected to respond and resolve system security issues that would include, but not be limited to malicious code, policy violations, unauthorized access, intrusion and misuse of the systems and/or information.

SCOUT security incident reporting contacts:

- Cal OES CISO: **Michael Crews, micahael.crews@caloes.ca.gov**
- Cal OES SCOUT Principal Administrator at **scout@caloes.ca.gov**

4.8 Misuse

Violation of these policies, practices, and procedures shall be investigated by the local agency head or his/her designee and reported to the Principal Agency. The local agency head or his/her designee shall investigate the incident of SCOUT misuse by reviewing its internal processes and documentation. In the event the agency head requires assistance from the Principal Agency in conducting a search of the SCOUT activity, a written request on agency letterhead, signed by a supervisor or agency head, shall be submitted to the Principal Agency. Any information as a result of the system search will be provided to the agency head in writing. The agency head shall return an assessment of the investigation and statement of corrective action to the Principal Agency. If the reported explanation and corrective actions do not resolve the problem to the satisfaction of the Principal Agency, the local agency head may be requested to provide additional information to Principal Agency to explain the incident.

In the event a violation of law or these policies, practices, and procedures results in SCOUT misuse, the Principle Agency will take appropriate action, such as:

1. Letter of censure.
2. Suspension of access. This may be for varying lengths of time.
3. Removal of access.

If a sanction is recommended by the Principal Agency, the effective date of the action shall be ten (10) working days. The ten (10) working day notice can be waived if extraordinary circumstances exist. If the agency head chooses to appeal the action, the request for review or reconsideration shall be forwarded to the Principal Agency's designee within ten (10) working days from the date of the action. If no such request is received within that time frame, the action shall be considered final.

4.9 Discontinuance of SCOUT Access

The Principal Agency or the Participating Agency may, upon thirty (30) working days written notice, discontinue access.

4.10 Training

The Principal Agencies in conjunction with their designated Functional Area Administrators will provide Administrator training and/or training materials to the SCOUT Agency Administrator on the use and administration of SCOUT. It will be the responsibility of the SCOUT Agency Administrator to provide training to SCOUT users in their agency.

Principal Agency Contact Information

Cal OES
Caroline Thomas Jacobs

Principal Administrator
3650 Schriever Ave
Mather, CA 95655
(916) 845-8510
scout@caloes.ca.gov

CAL FIRE
Chris Starnes
Principal Administrator
1416 9th Street
PO Box 944246
Sacramento, CA 95655
(916) 653-5123
scoutsupport@fire.ca.gov

5.0 Access & Data Security

Access to SCOUT is managed through the SCOUT User Registration, New Agency Onboarding Policy and Procedures, and all associated procedures and agreements. Information contributed to SCOUT is accessible to all SCOUT Users unless specifically restricted in a secured data layer or a secured Collaboration Room.

SCOUT Users must adhere to the following security protocols for data shared within SCOUT:

- User contributes data to SCOUT within the residing agency's standard operating procedure(s).
- Shared data may be exported by SCOUT users only for internal operational use within the scope of the user's emergency management and public safety role.
- Shared data will not be released publicly, except as approved through the applicable incident's designated Incident Commander.
- All shared information will be considered "For Official Use Only" and may only be used within the capacity of official emergency management and public safety operations.
- All public information requests will be referred to the relevant Incident's agency of jurisdiction, i.e. the "Incident Owner".

5.1 Access

Authorized users can access SCOUT through any network-connected device (e.g., PC, laptop, tablet, or mobile devices) that is secured in accordance with the Participating Agency's information security policies.

Note: some information security policies—specifically browser security settings—may interfere with SCOUT functionality, such as the Census App or access to certain data layers. Users must work with their designated SCOUT Agency Administrator to work through specific, local agency system conflicts.

5.1.1 Web Portal Access

The SCOUT platform is accessible via a web portal. www.scout.ca.gov

- New Participating Agency
    - Agencies interested in joining SCOUT must submit a letter (or email) of interest to scout@caloes.ca.gov to request participation and begin the Onboarding and Registration process.
- New SCOUT User
    - Users within a SCOUT Participating Agency may request a SCOUT User account via the web portal (www.scout.ca.gov) and will be required to read and sign a User Acceptable Use Agreement upon registration.

5.2.2 Web Service Access

The primary purpose of SCOUT is to enable information sharing across agencies and jurisdictions during complex, multi-jurisdictional incidents. To achieve this goal, it provides for easy import and export of incident information via the following standard file formats:

Data Imports

- Web Map Service (WMS, OGC compliant)
- Web Feature Service (WFS, OGC compliant)
- ArcGIS REST Map Server
- KML
- KMZ
- GPX
- GeoJSON
- Shapefile

Data Exports

- Static KML
- Shapefile
- Web Map Service (WMS, OGC compliant)

- Web Feature Service (WFS, OGC compliant)

GIS and Administrative users are authorized to import and export data in accordance with SCOUT policies, practices and protocols and the user's home agency data management standard operating procedures. When a home agency's policies or procedures are in conflict with SCOUT policies or procedures, SCOUT policies and procedures supersede the home agency policy and/or procedure. All data sharing must adhere to state and federal rules, regulations and laws.

5.3 Operating Systems / Browser Requirements

NOTE: SCOUT requires JavaScript to be enabled.

5.3.1 Operating System Requirements

Desktop	Mobile
• Windows 7 or higher • Mac OS X.5 or higher	• iOS 10 or higher • Android

5.3.2 Browser Requirements

SCOUT maintains compatibility with updated versions of Chrome, Firefox and Safari. While it will work in Internet Explorer 10+, some features may not function properly, including the Census App.

It is highly recommended that users access SCOUT via Chrome, Firefox, or Safari.

6 Shared Data Integration

Participating Agencies may request to make direct data connections between their home agency system(s) and SCOUT by submitting a request to scout@caloes.ca.gov.

- Systems accessing SCOUT will be authenticated and authorized as approved by SCOUT governance.
- Authorized systems will be allowed to ingest SCOUT incident data, as long as the receiving agency utilizes shared data within SCOUT Policies, Practices and Procedures.
- SCOUT will ingest approved web services from external authorized systems.

6.1 Shared Agency Data Elements

Participating Agencies may choose to establish real-time data integrations from their home agency system(s) into SCOUT. If an Agency chooses to establish data integration, the agency is agreeing to both receive information from SCOUT, as well as, share local incident information into SCOUT.

The recommended data elements to share include:

- Incident Name/Number
- Area or Perimeter of Impact
- Threat Direction
- Incident Command Post Location
- Staging Location
- Evacuation Areas
- Affected Population
- Road Closures
- Known Hazard Location(s)
- Shelter Location(s)
- Automatic Vehicle Location (as available)
- Infrastructure pertinent to the incident

Final shared data elements will be evaluated and approved through the SCOUT governance structure for individual data integration.

6.2 Potential Data Sources

Potential data sources for integration consideration include:

- Resource Tracking Systems, such as Automatic Vehicle Locator (AVL), Automatic Flight Following (AFF) and Personal Locator Information (PLI)
- Local Incident Management Systems
- Computer-Aided Dispatch (CAD) Systems

6.3 Data Integration Details

Agencies interested in establishing data integration with SCOUT, should contact scout@caloes.ca.gov.

- Data Integration Technical Specification document is in development.
- After the agency identifies its data source, a meeting will be scheduled to discuss the technical details that include, but are not limited to:
    - How data will be pushed and pulled from either endpoint
    - Transport details, i.e. web service, etc.
    - Refresh/update schedule

7 Responsibilities Matrix

The Matrix below defines which agency is responsible for each key New Agency Onboarding & Registration task.

R = Responsible Party · C = Consulted · S=Shared · I = Informed

Activity	Participating Agency	Cal OES
Identify SCOUT Agency Administrator	R	I
Complete Onboarding paperwork for agency and agency users	R	I
Provide Agency Administrator Training	C	R
Train agency users	R	I
Identify local data for integration	R	C
Integrate local data feeds	S	
Test data integrations in SCOUT	S	

8 SCOUT Documentation Revision

The Principal Agencies reserve the right to revise all SCOUT documentation, including PPPs as necessary and without notice, pursuant to their sole determination. Current SCOUT documentation is available at www.caloes.ca.gov/scout.

Appendix A

SCOUT Onboarding Checklist

- ☐ We have reviewed: **SCOUT FAQ Sheet**
- ☐ We have reviewed: **SCOUT Concept of Operations**
- ☐ We have reviewed: **SCOUT Operational Support Plan**
- ☐ We have reviewed: **Prerequisites**
- ☐ We have reviewed: **Shared Data Integration**
- ☐ We request integration with a local data source. (Leave blank if not requesting.)

  Local Data Source(s): _____
- ☐ We have reviewed: **Responsibilities Matrix**
- ☐ We have reviewed: **SCOUT User Agreement(s)**
- ☐ We have reviewed, signed and returned: **SCOUT Agency Participation Agreement**
- ☐ We have completed, signed and returned to OES Principal Administrator: **Agency Administrator Responsibilities**
- ☐ We have completed, signed and returned to designated Principal Administrator: **Agency Administrator Designation Form**

Appendix B

Agency Participation Agreement

PURPOSE:

This Agency Participation Agreement (Agreement) is entered into by and between the SCOUT Principal Agencies—California Governor's Office of Emergency Services (Cal OES) and California Department of Forestry and Fire Protection (CAL FIRE)—and _____ (hereinafter referred to as Participating Agency), to define the relationship between Cal OES and the Participating Agency as it relates to the Participating Agency's agreement to abide by the SCOUT Policy, Procedures and Protocols, Terms of Use Agreement, and, if applicable, the sharing of data between SCOUT and the Participating Agency.

RESPONSIBILITIES:

1. Participating Agencies agree to provide applicable SCOUT data to the maximum extent permitted by law or pre-existing agreement, in a mutually agreed upon electronic format, and in accordance with the SCOUT Policy, Procedures and Protocols.
2. Participating Agencies agree to contribute applicable incident data and grant access to SCOUT's other Participating Agencies. Such information may include, but is not limited to, incident name, perimeter of impact, evacuation zones, shelter locations, known hazards, and Command Post Location.
3. Participating Agency agrees to comply with the SCOUT Policies, Practices and Procedures.

For reference, see the following URL: www.caloes.ca.gov/scout

ACCEPTABLE USE:

Participating Agency acknowledges and agrees that its access to and use of SCOUT must be legal, ethical, and not detrimental to the goals, mission, objectives, and reputation of Cal OES, CAL FIRE, or the State of California. Users may not:

1) Use the Portal in violation of applicable local, state, national laws, rules, and regulations.
2) Use the Portal to upload, transmit, or otherwise distribute any content that is unlawful.
3) Distribute information contained within the Portal without authorization.
4) Mine the portal to obtain user data.
5) Use any automated device or manual process to monitor or gather any data from the Portal or its users in any manner inconsistent with the agency's public safety mission.
6) Create multiple user accounts or create user accounts by automated means or under false or fraudulent pretenses.
7) Permit anyone to access the Portal using the User's credentials.
8) Use the Portal for any fraudulent or inappropriate purpose.

INFORMATION OWNERSHIP AND RELEASE

Ownership: Each Participating Agency retains control of all information they provide through SCOUT at all times. The Participating Agency is responsible for creating, updating, and deleting records in its system according to its policies. The Participating Agency shall ensure the completeness and accuracy of its source data. The information contributed from the local data source into SCOUT shall remain the property of the Participating Agency. Agencies may use information contained within SCOUT for purposes consistent with their public safety mission. Any improper or unauthorized use, including the improper or unauthorized use of information, may result in the revocation of the agency's access to SCOUT.

Requests for Information

Any third party request, including but not limited to Public Records Act request or Freedom of Information Act requests, for information authored or originated by another source agency shall be immediately referred to the source agency. The agency that initially receives a request shall not release or make available any information it has accessed to any third party except as required by law.

TERM

Either party to this Agreement may terminate this Agreement by giving 30 days' written notice. Cal OES can terminate the participating agency's access to SCOUT at any time at its discretion.

_____ _____

Participating Agency Head Signature **Participating Agency Head Printed Name, Title**

_____

Date

_____ _____

Principal Agency Representative Signature **Principal Agency Representative Printed Name, Title**

_____

Date

Submit all completed forms in a single pdf package to scout@caloes.ca.gov.
Agency Participation Agreement Form version 1.0 dated July 1, 2017

APPROVED AS TO FORM:
COUNTY COUNSEL
BY: 3/15/18
DEPUTY, #20171626

Appendix C

SCOUT Agency Administrator (AA) Responsibilities

The Agency Administrator serves as the agency's designated staff member with responsibility for all operational, training and support required to successfully utilize SCOUT within said agency.

The Agency Administrator should be familiar with all aspects of SCOUT. The SCOUT Agency Administrator's responsibilities include:

Administration/Record Keeping

- Coordinate and/or respond to SCOUT related correspondence;
- Notify SCOUT Functional Area Administrator and scout@caloes.ca.gov of changes in address, telephone number, agency representatives or other information pertaining to your agency;
- Maintain agency SCOUT incident information;
- Maintain SCOUT user accounts within your agency, disabling users who are no longer employed;
- Ensure only authorized users have access to SCOUT; and
- Maintain agency base data.

Audits

- Ensure compliance with state and federal auditing requirements;
- Promptly respond to SCOUT Functional Area or Principal Administrator requests for agency information.

Information Distribution

- Oversee the distribution of SCOUT information to your agency's SCOUT user base.

Policy

- Ensure compliance with SCOUT Policies, Practices and Procedures; and
- Ensure SCOUT user access is maintained, secure and up to date.

Access Schematics

- Maintain and have available a current system diagram;
- Maintain and have available a list of SCOUT access points within your agency, identifying whether the access is fixed or mobile; and
- Coordinate any access changes.

Training

- Advise users within your agency of training requirements;
- Conduct training of users within your agency; and
- Maintain and have available training records.

(over)

I have read, understand and agree to abide by the responsibilities of a SCOUT Agency Administrator.

_____	_____
Agency Administrator Signature	Agency Administrator Printed Name, Title
_____	
Date	
_____	_____
Agency Head Signature	Agency Head Name, Title
_____	
Date	

Submit all completed forms in a single pdf package to scout@caloes.ca.gov.
Agency Administrator Responsibilities Form version 1.0 dated July 1, 2017

Appendix D

SCOUT Agency Administrator Designation Form

All Participating Agencies are required to designate an Agency Administrator.

☐ **New Request** ☐ **Change Request**

California Office of Emergency Services SCOUT Program Office 3650 Schriever Ave Mather, CA 95655		Telephone: (925) 953-1304 Email: SCOUT@caloes.ca.gov
Participating Agency Name		
Address		
City	Zip	County
SCOUT Agency Administrator Name		Phone
Agency Administrator Email		

Submit all completed forms in a single pdf package to scout@caloes.ca.gov.
Agency Administrator Designation Form version 1.0 dated July 1, 2017

Exhibit A

SCOUT FAQ Sheet

Q. What is SCOUT?

A. The California Governor's Office of Emergency Services (Cal OES)—in association with the California Department of Forestry and Fire Protection (CAL FIRE) and through a strategic partnership with the Department of Homeland Security's Science & Technology Directorate (DHS S&T)—acquired the Next-Generation Incident Command System (NICS) software for use by California's emergency services professionals. The California deployment of the NICS software is called Situation Awareness and Collaboration Tool (SCOUT). SCOUT provides an information sharing environment to facilitate operational and tactical collaboration among California emergency responders and interagency situational awareness for local, tribal, state, and federal partners on small to extreme scale homeland security incidents, such natural disasters, technological hazards, intentional attacks, and human-caused emergencies.

Q. Which agency administers SCOUT for the State of California?

A. SCOUT is administered by the California Governor's Office of Emergency Services, in association with the California Department of Forestry and Fire Protection. These two agencies are referred to as the "Principal Agencies" within SCOUT documentation.

Q. What is the governance structure for SCOUT?

A. A governance charter has been established and signed between Cal OES and CAL FIRE. The structure includes an *Executive Committee* responsible for SCOUT vision, strategy and funding decisions, a supporting *Steering Committee* to manage program operations and *Training, Operations and Technical Subcommittees* to address defined operational needs.

The SCOUT Charter is available for download at www.caloes.ca.gov/scout.

Q. What is the administration structure for the SCOUT platform?

A. There are three levels of administration for the SCOUT platform:

Principal Agency & Administrator is responsible for determining the SCOUT strategy and sustainable funding model, as well as, overseeing statewide use of SCOUT, platform maintenance and support, and managing the training curriculum.

Functional Area Administrator is responsible for Participating Agency management, coordination and support.

Agency Administrator is responsible for managing the Participating Agency's SCOUT standard operating procedures, user account administration, user training and helpdesk support.

Q. How will SCOUT be rolled out to the user community?

A. SCOUT is being rolled out in three phases.

Phase 1 - April 2016: Agencies participating in the NICS pilot were invited to transition to SCOUT.

Phase 2 - Summer 2017: Select agencies are invited to join SCOUT in a controlled expansion. Interested agencies should contact scout@caloes.ca.gov.

Phase 3 – Late 2017/2018: SCOUT will open to all interested and eligible agencies.

Transition to each phase will be based on the stability and performance of the platform and program operations.

Q. What information will authorized users be able to access through SCOUT?

A. Authorized users will be able to view, search and add incident information—based on user roles and permissions—for a variety of incident types, including but not limited to wild land fires, floods, search & rescue missions, special events, earthquakes and homeland security incidents. Also, SCOUT will integrate incident information with other relevant geographical information, such as weather conditions, road conditions, utilities, census information, known hazards, and government boundaries.

Q. How will authorized users access SCOUT?

A. Authorized users can access SCOUT through any network connected device (e.g., PC, laptop, tablet, or smartphone) that is approved through their internal agency policy.

Q. Will there be a limit to the number of users per Participating Agency?

A. No. Participating Agencies are responsible for managing internal use of SCOUT, in accordance with SCOUT policy, procedures, and protocols, and are authorized to determine the appropriate users within their agency.

Q. Will a Participating Agency be required to contribute data in order to participate?

A. No, agencies will not be required to contribute data to access SCOUT.

Q. How much will it cost to become a Participating Agency in SCOUT?

A. The Principal Agencies expect to implement participation fees in Phase 3. The Principal Agencies will conduct a cost analysis of Phase 1 and Phase 2 operating expenses associated with maintaining, supporting and operating the SCOUT platform. The Principal Agencies will develop a Sustaining Funding Model for implementation in Phase 3. In addition to any expected participation fees, Participating Agencies are responsible for providing staff resources for internal administrative and training support needs. If a Participating Agency chooses to integrate their local system(s) with SCOUT, the local agency is responsible for the local system costs incurred to integrate with SCOUT. There are no participation fees in Phase 1 or Phase 2.

Q. How does my agency join SCOUT?

A. We are currently in Phase 2 of the SCOUT rollout. Agencies interested in joining SCOUT must contact scout@caloes.ca.gov. Agencies invited to participate in Phase 2 will be required to review and complete the **SCOUT Onboarding & Registration Policy and Procedures** and complete all steps outlined in the onboarding procedures.

Q. Who do I contact for more information about SCOUT?

A. Local Agencies can contact their Cal OES Regional Mutual Aid Coordinator or Regional Administrator.

CAL FIRE Units can contact their Regional Functional Area Administrators:

Northern Region – Battalion Chief Dan Dennett and Battalion Chief Philip SeLegue

Southern Region – Division Chief Jennifer Ricci and Battalion Chief Brook Spelman

Exhibit B

Agency User Agreement

Policy Regarding Acceptable Use of SCOUT

PURPOSE:

The purpose of this policy is to provide a clear statement to all users of the Situation Awareness & Collaboration Tool (SCOUT) and the responsibility of those using SCOUT to protect information and use the system properly.

SCOPE & APPLICATION

This policy applies to all those who are granted access to SCOUT including, but not limited to, employees of the California Governor's Office of Emergency Services (Cal OES), employees of the California Department of Forestry and Fire Protection (CAL FIRE), participating agencies, and all other authorized users.

RESTRICTIONS ON USE

Use must be legal, ethical, and not detrimental to the goals, mission, objectives, and reputation of Cal OES, CAL FIRE, or the State of California. Users may not:

1) Use the Portal in violation of applicable local, state, national laws, rules, and regulations.
2) Use the Portal to upload, transmit, or otherwise distribute any content that is unlawful or unprofessional.
3) Distribute information contained within the Portal without authorization.
4) Mine the portal to obtain user data.
5) Use any automated device or manual process to monitor or gather any data from the Portal or its users in any manner inconsistent with the agency's public safety mission.
6) Create multiple user accounts or create user accounts by automated means or under false or fraudulent pretenses.
7) Permit anyone to access the Portal using the User's credentials.
8) Use the Portal for any fraudulent or inappropriate purpose.

ENFORCEMENT, AUDITING, AND REPORTING

Anyone accessing SCOUT who has reasonable belief that another individual or entity is accessing SCOUT in violation of this policy must report such activity to the California Governor's Office of Emergency Services. Violation of this policy may result in the revocation of access to SCOUT. Violators of this Agreement will be held accountable to the greatest extent permitted by law. State employees who violate this Agreement may be subjected to discipline up to and including termination.

Users may not:

1) Use the Portal in violation of applicable local, state, national laws, rules, and regulations.
2) Use the Portal to upload, transmit, or otherwise distribute any content that is unlawful, infringing of intellectual property rights, defamatory, harassing, abusive, fraudulent, obscene, contains viruses, or is otherwise objectionable.
3) Distribute information contained within the Portal without authorization.
4) Mine the portal to obtain user data.
5) Use any automated device or manual process to monitor or gather any data from the Portal or its users in any manner inconsistent with the agency's public safety mission.
6) Create multiple user accounts or create user accounts by automated means or under false or fraudulent pretenses.
7) Permit anyone to access the Portal using the User's credentials.
8) Use the Portal for any fraudulent or inappropriate purpose.

If you do not agree to these terms and conditions, you cannot access SCOUT. Any unauthorized or improper use of SCOUT in violation of these Terms of Use, the User Agreement, or any other governing document may result in revocation of the User's and User's Agency's access to SCOUT, as well as civil and/or criminal penalties.

SCOUT USER AGREEMENT

I, _____, acknowledge, have read and understood, and hereby agree to abide by the SCOUT Acceptable Use Agreement set forth above.

I understand that as a SCOUT user, I may have access to confidential and/or protected information controlled by state and federal law. All access to the SCOUT system and any type of protected information obtained through SCOUT is based on a "need to know" and the "right to know." Misuse of such information may adversely affect an individual's right to privacy, civil liberties, and civil rights, and violates constitutional and state law and/or policy.

"Need to know" means you have a legitimate business purpose in accessing the information. "Right to know" means you have legal authority pursuant to both law and department policy to access the information. To access information, the "need to know" and the "right to know" must exist at the same time.

I understand that the unauthorized or improper use of SCOUT may amount to a violation of California Penal Code section 502, as well as other state and federal laws.

I HAVE READ THE ABOVE AND UNDERSTAND THE POLICY REGARDING MISUSE OF ALL ACCESSIBLE INFORMATION. I UNDERSTAND THAT BY SIGNING BELOW, I AGREE TO ALL TERMS AND CONDITIONS AND ANY VIOLATION THEREOF MAY RESULT IN REVOCATION OF ACCESS TO SCOUT AS WELL AS CIVIL AND/OR CRIMINAL PENALTIES.

Users will be required to acknowledge that they have read and understand the above Acceptable Use Policy upon user registration.

Exhibit C

Terms of Use

ACCEPTANCE OF TERMS

The California Governor's Office of Emergency Services ("Cal OES") provides you with access to the Situation Awareness and Collaboration Tool ("SCOUT"), which includes documentation, system information, software, and other services. The use of SCOUT, including any updates, is subject to the following Terms of Use, unless we have provided those items to you under more specific terms, in which case, those more specific terms will apply to the relevant item.

Cal OES reserves the right to update the Terms of Use at any time. The most current version of the Terms of Use can be reviewed by clicking on the "Terms of Use" hypertext link located on the SCOUT Login webpage. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, or sell any of the information, gained or provided through the use of SCOUT, except as permitted by the Terms of Use. **IF YOU DO NOT ACCEPT ALL OF THESE TERMS, DO NOT USE THIS SITE.**

INFORMATION OWNERSHIP AND USE

Ownership: Each Participating Agency retains control of all information they provide through SCOUT at all times. The Participating Agency is responsible for creating, updating, and deleting records in its system according to its policies. The Participating Agency shall ensure the completeness and accuracy of its source data. The information contributed from a local data source into SCOUT shall remain the property of the Participating Agency. Agencies may use information contained within SCOUT for purposes consistent with their public safety mission. Any improper or unauthorized use, including the improper or unauthorized use of information, may result in the revocation of the agency's access to SCOUT.

Requests for Information

Any third party request, including but not limited to Public Records Act request or Freedom of Information Act requests, for information authored or originated by another source agency shall be immediately referred to the source agency. The agency that initially receives a request shall not release or make available any information it has accessed to any third party except as required by law.

- The parties agree this Terms of Use Agreement is subject to all applicable federal, state, and local statutes, ordinances, and regulations.

Users will be required to acknowledge that they have read and understand the above Acceptable Use Policy upon user registration.