SAN DIEGO URBAN AREA

REGIONAL TECHNOLOGY STRATEGIC PLAN

A FRAMEWORK FOR REGIONAL TECHNOLOGY COORDINATION

August 2016

Contents

DOCUMENT CONTROL ..... **VI**

DOCUMENT INFORMATION VI

DOCUMENT HISTORY VI

DOCUMENT APPROVALS VII

EXECUTIVE SUMMARY **1**

1. PURPOSE **3**

2. VISION **3**

3. GOVERNANCE **4**

4. TECHNOLOGY PLANNING AND IMPLEMENTATION CYCLE **6**

5. GOAL 1—INTEROPERABLE VOICE COMMUNICATIONS **6**

ACCOMPLISHMENTS AND CURRENT ACTIVITIES 7

CAPABILITY GAPS 8

INITIATIVES 9

Initiative 1.1 - Migration of land mobile radio systems to P25 standards *9*

Initiative 1.2 – VHF radio infrastructure *9*

Initiative 1.3 - Cloud hosted video/web conferencing solution *9*

Initiative 1.4 Regional Tactical Interoperability Communications Plan Update *9*

CHALLENGES 9

6. GOAL 2—INTEROPERABLE DATA SYSTEMS **10**

ACCOMPLISHMENTS AND CURRENT ACTIVITIES 10

CAPABILITY GAPS 12

INITIATIVES 14

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

2.1 Regional CAD Interoperability. *14*

2.2 Mobile Data Devices *14*

2.3 ARJIS Dashboard/CAD Interfaces *15*

2.4 ARJIS Data Enhancements. *15*

2.5 Prehospital Emergency Medical Services Information System *15*

2.6 Cyber Security. *15*

2.7 Risk Analysis Center Infrastructure Asset Data *15*

2.8 Mobile Device and Data Security Enhancements. *16*

2.9 Wireless Data Services *16*

2.10 Resource and People Location Services *16*

2.11 Palantir *16*

CHALLENGES 16

7. GOAL 3—INTEROPERABLE GEOGRAPHICAL INFORMATION SYSTEMS 17

ACCOMPLISHMENTS AND CURRENT ACTIVITIES 17

CAPABILITY GAPS 18

INITIATIVES 20

3.1 Digital Target Hazard Plans (Fire Preplans). *20*

3.2 Synchronization of data between Regional Public Safety Geodatabase and SanGIS. *20*

3.3 Situational Awareness Mapping Tools. *20*

3.4 SanMAPS *20*

3.5 ARJIS GIS Services *20*

3.6 Next Generation 911 GIS Requirements. *21*

3.7 InSIDeR Plans *21*

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

CHALLENGES 21

8. GOAL 4 – GOVERNANCE 21

ACCOMPLISHMENTS AND CURRENT ACTIVITIES 22

CAPABILITY GAPS 22

INITIATIVES 23

4.1 GIS Program Sustainment 23

4.2 RCIP Program Sustainment 23

4.3 Regional Technology Partnership (RTP) Services 23

4.4 New Technology Policies and Procedures 23

CHALLENGES 23

9. IMPLEMENTATION STRATEGY 24

10. SAN DIEGO URBAN AREA TECHNOLOGY INVESTMENTS 26

CITY OF SAN DIEGO AND REGIONAL COMMUNICATIONS SYSTEM MIGRATION TO P25 STANDARD 26

VHF RADIO INFRASTRUCTURE 28

REGIONAL VIDEO/WEB CONFERENCING 29

REGIONAL TACTICAL INTEROPERABILITY COMMUNICATIONS PLAN 30

REGIONAL COMMUNITY EMERGENCY NOTIFICATION SYSTEMS 30

REGIONAL COMPUTER AIDED DISPATCH INTEROPERABILITY PROJECT 33

REGIONAL LICENSE PLATE READER (LPR) PROJECT 35

CALCOP-HAYSTAX RISK MANAGEMENT SOFTWARE 36

NETRMS INTERFACES 38

ARJIS DASHBOARD 39

ARJIS MOBILE 40

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

ARJIS NETWORK AND DATA CENTER 41

PALANTIR 42

ARJIS CAD INTERFACES 43

ARJIS NET PORTAL 43

LAW ENFORCEMENT COORDINATION CENTER (LECC) CYBER SECURITY 44

SAN DIEGO REGIONAL PUBLIC SAFETY GEODATABASE 48

SITUATIONAL AWARENESS MAPPING 50

INSIDER 53

REGIONAL PUBLIC SAFETY GEODATABASE (RPSG) GOVERNANCE 54

REGIONAL CAD INTEROPERABILITY PROJECT (RCIP) GOVERNANCE 55

3C'S PUBLIC SAFETY DATA NETWORK TRANSITION 56

ARJIS ACCEPTABLE USE POLICIES 56

PRIVACY IMPACT ASSESSMENTS 57

11. REFERENCE TO SAN DIEGO URBAN AREA SECURITY STRATEGY 58

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

DOCUMENT CONTROL

Document Information

©	Information
Document ID	[RPT130208]
Document Owner	Mike Scott
Issue Date	[February 15, 2013]
Last Saved Date	[August 19, 2016]
File Name	[San Diego Regional Strategic Technology Plan 2016]

Document History

Version	Issue Date	Changes
1.0	2/7/13	
2.0	7/1/16	Updated entire plan

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Document Approvals

Regional Technology Partnership Members	Name	Signature©	Date
City of San Diego Homeland Security	John Valencia,		
County of San Diego Office of Emergency Services	Holly Crawford,		
City of San Diego Fire Rescue	Brian Fenessy		
City of San Diego Police Department	Al Guaderamma		
County Fire Chiefs Association	Don Butz		
San Diego Sheriff Department	Todd Frank		
District Fire Chiefs Association	Brett Van Wey		
Police and Sheriff Association	Walt Vasquez		

This plan has been reviewed and approved by the Regional Technology Partnership members.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Executive Summary

"A Framework for Regional Technology Coordination"

The Regional Strategic Technology Plan (RSTP) provides the San Diego Urban area with a road map for implementing an effective approach to everyday prevention, protection, mitigation, response and recovery through regional interoperability technology solutions. The plan provides a comprehensive technology review of current San Diego Urban Area (SDUA) accomplishments, capability gaps, recommended initiatives, challenges and details on regional investments.

The SDUA has made significant advances in the area of planning and implementing regional technology solutions. Some key examples are the San Diego/Imperial County Regional Communications System (RCS), the Automated Regional Justice Information System (ARJIS), San Diego Regional Public Safety Geodatabase, Regional Computer Aided Dispatch (CAD) Interoperability, Regional Mass Notification System, Situational Awareness Mapping tools and SanMAPS to name a few. Many more key examples are described at length in this plan.

The success of technology initiatives, shared systems and collaborative agreements has been possible due to the cooperative efforts of the organizations and agencies within the SDUA. These agencies are responsible for Public Safety personnel and resources and a commitment to the betterment of the region both inside and outside the SDUA. Each agency has made a strong commitment to share resources and approach solutions from a regional perspective whenever possible.

This plan serves as a guiding document for implementation of regional technology projects over the next 36 months.

The remainder of this page is intentionally left blank.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

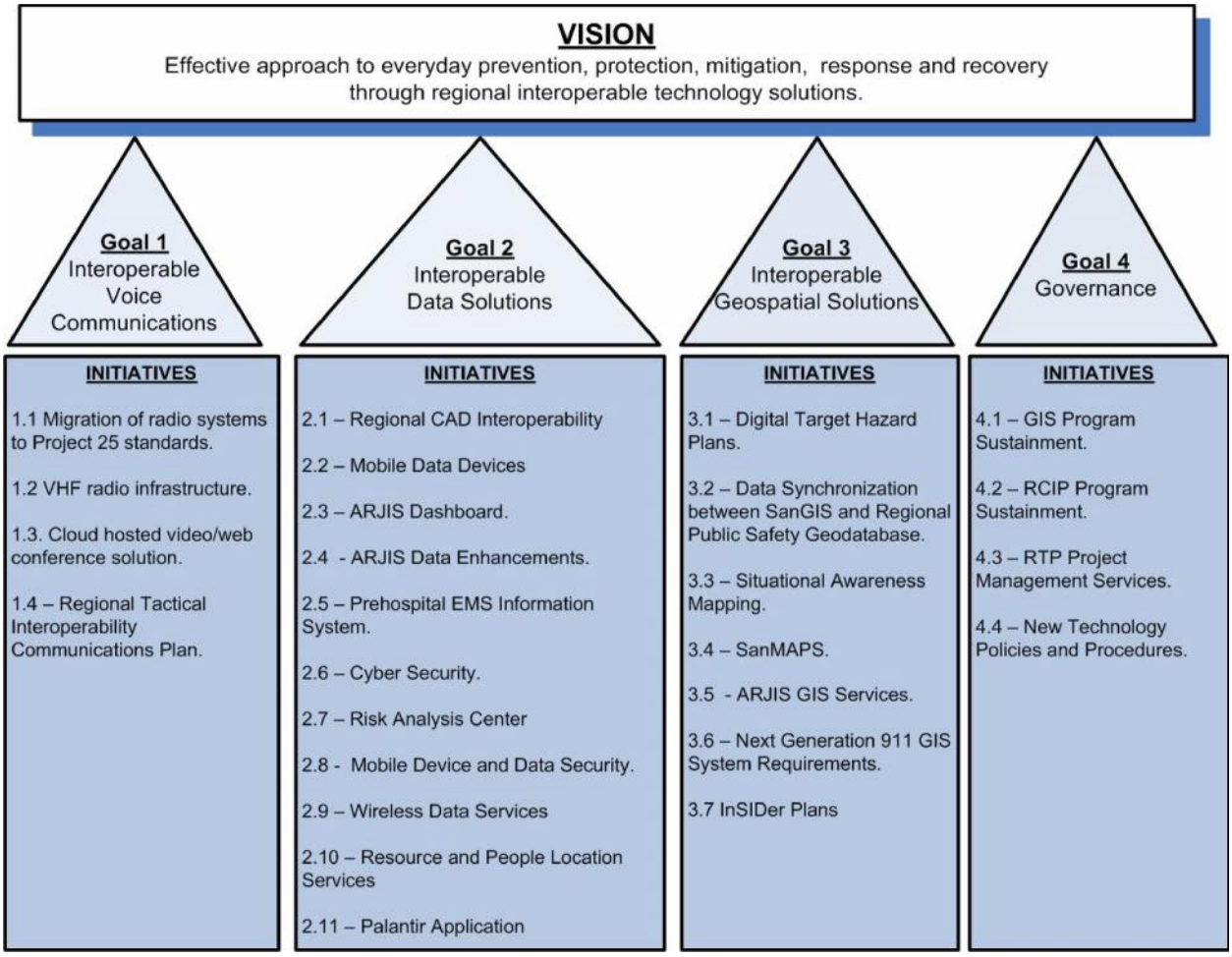


Figure 1 – Regional Technology Strategic Plan Vision, Goals, Initiatives

These initiatives are not prioritized in any particular order and only serve as a list of regional technology solutions that the region should continue to work on or begin engagement. In conjunction with the San Diego Urban Area Security Strategy, the RSTP should be used as a tool to support funding decisions for the regions policy and funding authorities.

The RSTP can be utilized to implement regional technology solutions regardless of the funding source. While the primary focus in recent years has been the Homeland Security grant funds, there will continue to be opportunities to leverage multiple funding sources to implement this plan.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

This plan has been developed utilizing a variety of sources. These sources include the 2012 San Diego Homeland Security Strategy, the 2013 Regional Strategic Technology Plan and interviews and input from the various stakeholders who manage the technology initiatives listed in this plan.

1. PURPOSE

The overall purpose of the RSTP is to document accomplishments and current activities, identify capability gaps, recommend initiatives, identify challenges and provide background information on regional technology investments. This document provides a roadmap portraying the managed, phased growth of technology solutions and systems to position the SDUA with the ability to uniformly:

- Respond to emergencies and multi-agency mutual aid situations.
- React to expanding needs in basic service requirements.
- Respond to growing voice, data and information sharing traffic loads.
- Provide the ability to leverage enhanced technologies.

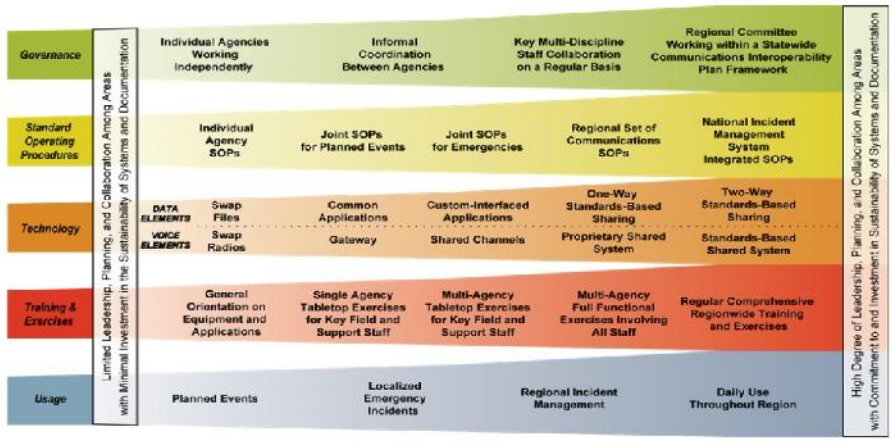
The plan also serves to help inform stakeholders on projects to focus efforts and funding.

2. VISION

The vision of the RSTP is to enable the region to have an effective approach to everyday prevention, protection, mitigation, response and recovery through regional interoperable technology solutions. The RSTP is available to the SDUA as a guideline document to assure operability, interoperability and economy of scale in the future application of technologies across the region. The RSTP is complimentary to the requirements of previously approved documents that meet the goals and objectives for technology initiatives in the SDUA. The RSTP works in conjunction with the San Diego Urban Area Security Strategy which serves to identify capability strengths and gaps in the SDUA, and establishes a process to help fill those gaps.

The RSTP is in alignment with the Department of Homeland Securities Interoperability Continuum vision. This document focuses on the Technology, Governance and Usage sections of the continuum.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.



3. GOVERNANCE

Governance is an organized structure of individuals or agencies that are authorized to make decisions about and oversee the implementation of strategic initiatives. It provides management oversight and serves as the policy and decision maker for an organization or effort. The governance structure for the SDUA consists of existing boards, committees, or councils that have already been authorized or created specifically to oversee technology initiatives.

Based on lessons learned during the San Diego region's wildfires in October 2003 and an ARJIS hosted Interoperability Communications Workshop, the SDUA sought a method for improving technology interoperability opportunities. To meet this need, the Unified Disaster Council (UDC) established the Regional Technology Partnership (RTP), a group comprised of senior Public Safety representatives involved in emergency and disaster response. In 2005, the RTP was tasked with establishing a regional technology support structure for the SDUA. The RTP in turn, with support of the UDC, approved the creation of the Regional Technology Center (RTC) to be the operational arm and independent technology clearinghouse for SDUA agencies. The San Diego State University Research Foundation provided the RTC services under contract with the City of San Diego. In 2006, after a series of workshops, a strategy for voice/data communications and interoperability, as well as a framework for improving regional cooperation was approved by the San Diego Association of Governments (SANDAG) Public Safety Committee (PSC) and UDC. To implement this strategy, the SANDAG Executive Board, the PSC and the UDC approved support for the RTC to become the technical support arm for these bodies.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

In 2011, the Urban Area Working Group in collaboration with the RTP and City of San Diego Homeland Security modified the technology support structure to focus on project management services through a base contract with options to add additional services. The focus of the effort shifted from research and strategic objectives to implementation of plans and projects. These services have been provided by L.R. Kimball by contract with the City of San Diego.

POLICY AND FUNDING

The policy and funding bodies are responsible for directing regional interoperability and communications policy and funding decisions, as well as providing lobbying and legislative support. The UDC and PSC are responsible for addressing policy and funding issues within their areas of expertise. Additionally, they collaborate with SDUA agencies to drive the region's interoperability and communications efforts, while making the best use of existing resources and mandates. This structure allows the region to involve key stakeholders from all jurisdictions and disciplines in these efforts. The UDC continues its focus on emergency preparedness, response and disaster planning. The PSC's focus is on issues related to information sharing, data and privacy standards and crime analysis and prevention.

Under the authority of the UDC, an Urban Area Working Group (UAWG) Charter has been adopted to make funding decisions for the use of Urban Area Security Initiative grant funds. The UAWG consists of the 18 cities in San Diego County and the County of San Diego as voting members. Additionally, advisory roles are provided for by the Citizen Corps and tribal representation.

ADVISORY ROLE

The advisory level provides recommendations to the policy and funding bodies on the direction of the regional strategy, the definition of scope and priorities for the implementation of strategic initiatives. One of the most important roles of the RTP is the process of scoring and vetting of investment proposals seeking Urban Area Security Initiative Grant funding. The RTP provides the UAWG with a recommendation on allocation of funding based on grant requirements and certain criteria.

The RTP membership includes the following representatives:

- City of San Diego Chief of Police
- San Diego County Sheriff's Office
- San Diego County Police Chiefs and Sheriffs Association
- City of San Diego Fire Chief
- San Diego County Fire Chiefs Association
- San Diego Fire District Chiefs Representative
- City of San Diego Office of Homeland Security Program Director
- San Diego County Office of Emergency Services Director

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

REGIONAL TECHNOLOGY PARTNERSHIP SUPPORT SERVICES
In 2011, the RTP in conjunction with San Diego Office of Homeland Security modified the method for technical support. Instead of a Regional Technology Center designed to test and evaluate technologies, the focus was shifted to project management support and consulting services. In addition, the contract allowed for issuing specific task orders to complete specific projects or develop plans, needs assessments or studies on an as needed basis. The current contractor for this support is L.R. Kimball. The base contract provides a program director for the RTP and a Geographic Information System GIS project manager. Additional services have been added to support the Regional Computer Aided Dispatch Interoperability (RCIP) project management, GIS System Administrator services, Regional Interoperability Communications Plan (RICP) and Regional Emergency Communications Center (RECC) Study and VHF Gap Analysis.

4. TECHNOLOGY PLANNING AND IMPLEMENTATION CYCLE

The SDUA utilizes an ongoing planning and implementation process to coordinate the region's technology improvements. This can be described as a Homeland Security Strategy Cycle. The first step in this process is to perform a gap analysis, identify capabilities and complete a risk assessment. The next step in the process is to develop a set of goals and objectives in the Security Strategy. Based on those goals and objectives, input from the regional subject matter experts, fire service leadership, law enforcement leadership and emergency manager leadership, the Regional Strategic Technology Plan is developed. This combination of the Security Strategy and the Strategic Technology Plan is then utilized to assist in development of investment proposals, designed to address any regional gaps that would improve our capabilities and reduce our risk.

5. GOAL 1—INTEROPERABLE VOICE COMMUNICATIONs

Interoperable voice communications systems and capabilities are critical in the ability to effectively respond to emergency incidents. The importance of having seamless communications and interoperability in the SDUA cannot be overstated. Interoperable communications is consistently discussed as one of the most critical issues on the priority list for public safety agencies and first responders.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Accomplishments and Current Activities

City of San Diego migration to Project 25 digital radio system

The City of San Diego's Public Safety users including the Police Department and Fire-Rescue Department use the City's radio system as their primary voice system. This network provides service to more than 16,000 users in over 25 City departments and covers an area of approximately 400 square miles. The City operates a Motorola SmartZone Type 4.1 mixed-mode, analog/digital 800 MHz radio system. The City is in the process of installing an Association of Public-Safety Communications Officials (APCO) P25-compliant system.

Regional Communications System (RCS) migration to Project 25 digital radio system

In 2010, the County of San Diego, utilizing Urban Area Security Initiative (UASI) funding, contracted with Federal Engineering, Inc. to develop a plan for procurement and migration to a P25 digital radio system. Based on that plan, the County worked with regional partners to develop a new regional partnership agreement, identify funding mechanisms, and to develop the requirements for competitive solicitations for the procurement and migration. The first steps in this migration have focused on upgrading the microwave backhaul network to an IP based standards system. This phase utilized an estimated eight million dollars in UASI grant funding to implement the new technology. In June 2016, as a result of a competitive procurement, the County awarded a contract to Motorola Solutions, Inc. to design and implement the new Regional Communications System Project 25 digital public safety radio system. This project has an estimated cost of $70 million for the infrastructure replacement and migration. Additionally, the dispatch console systems at 24 public safety dispatch centers will need to be upgraded to be compatible with the new P25 technology (at an estimated cost of eight million dollars).

VHF radio infrastructure gap analysis

In 2012, the County of San Diego Wireless Services Division contracted with Federal Engineering to develop alternatives and identify the associated costs of additional VHF fire mutual aid resources. While a large scale infrastructure improvement plan was not initiated, small incremental improvements have improved VHF capability in some areas. In 2016, L.R. Kimball was contracted to complete an update on the gaps in VHF capabilities. This report will identify opportunities to improve capacity and coverage and recommend a plan for implementation.

Regional Video/Web Conferencing

Through the RTP support services, an analysis of options for regional video/web conferencing solutions was completed. The resulting report identified a cloud hosted video/web conferencing solution as the most cost efficient system to meet the desired objective. The County Office of Emergency Services has been allocated UASI funding to implement a cloud hosted video/web conferencing solution. This project will

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

provide a cloud hosted service to provide connectivity and interoperability between local and interagency organizations.

Regional Interoperability Communications Plan

In 2014, L.R. Kimball was contracted to develop a Regional Interoperability Communication Plan. This plan is a combination of a Tactical Interoperability Communications Plan and system failure plans, standard operating procedures and strategic planning.

Regional Community Emergency Notifications Systems Enhancements

The County of San Diego Office of Emergency Services has taken the lead in hosting a variety of capabilities for community emergency notifications systems. This includes Alert San Diego, SDEmergency Mobile Application, communications with hearing impaired and language translation services. This approach has allowed all agencies in the SDUA to utilize one platform for community emergency notifications and helps reduce confusion for the public on where to look for information.

Capability Gaps

Migration to P25 standard for Land Mobile Radio System

The City of San Diego is approximately 80% complete with their migration to P25. The Regional Communications System has developed a migration plan and has selected a vendor to begin the replacement of the infrastructure.

VHF Radio Infrastructure

The current VHF radio infrastructure has some gaps in capacity and coverage to meet operational needs. This includes opportunities to coordinate use of existing local government radio licensing.

Video Teleconference System

The legacy equipment is at end of life cycle and the 3C's videoconference system will not be provided with regional technical support.

Regional Interoperability Communications Plan

The Regional Interoperability Communications Plan was last updated in 2014. Since then, some of the fleet maps have been modified or reorganized to meet operational needs. In addition, a common naming convention has been developed for the VHF frequencies. Replacement of the infrastructure for the P25 standard may also have an impact on the communications plan. These changes need to be reflected in the plan and the impacts on backup communications plan during system failure needs to be understood.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Initiatives

Initiative 1.1 - Migration of land mobile radio systems to P25 standards

Complete the migration of the City of San Diego and Regional Communications System to the P25 standard.

Recommended Milestone
Complete the transition to a P25 digital radio system within 36 months.

Initiative 1.2 – VHF radio infrastructure.

Expand the VHF radio infrastructure to provide improved coverage and capacity for the region. This includes coordination of available local government radio licensing. These improvements will support mutual aid interoperability plans and provide a backup radio system during high use periods or potential trunked radio system failure.

Recommended milestone
Complete the Expansion of VHF Radio Infrastructure Within 24 Months.

Initiative 1.3 - Cloud hosted video/web conferencing solution

The acquiring of a cloud hosted video/web conferencing solution will provide video teleconferencing capability to support region wide communications of information. The system would leverage existing technology infrastructure to allow multiple participants to participate from a variety of devices and platforms.

The County of San Diego is in the process of procuring a solution. Once procured, the solution will need to be implemented in coordination with the participants.

Recommended milestone
Complete the implementation within six months.

Initiative 1.4 Regional Tactical Interoperability Communications Plan Update

Update the Regional Interoperability Communications Plan to capture changes in fleet maps, infrastructure changes, VHF capabilities and the resulting impact on backup plans.

Recommended milestone
Complete the implementation within 12-24 months.

Challenges

- Radio infrastructure replacement requires significant amounts of funding.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

- Deployment of the cloud hosted video/web conference system will likely require technical support to implement.
- Unknown sustainment plan for VHF radio infrastructure.
- Update to the Interoperability Communications Plan will occur during a transition phase of the infrastructure.

6. GOAL 2—INTEROPERABLE DATA SYSTEMS

The SDUA should continue to provide and improve the regions interoperable data systems and capabilities. This includes the ability to have access to mission critical wireless data networks for field applications, shared database information and interoperable data sharing for coordination of emergency response. The ability for all agencies across the region to have access to and share data is critical to the SDUA's effectiveness. Emergency incidents and criminal activity do not stop at jurisdictional boundaries. When a region collaborates and shares data, the regions fire and law enforcement is much more effective.

Accomplishments and Current Activities

Regional Computer Aided Dispatch Interoperability

The Fire Communications Centers implemented a CAD interoperability system to share and dispatch resources across disparate CAD systems. This capability provides the technical capability to share emergency response resources automatically. This allows the deployment of resources in a faster and more effective way.

Regional License Plate Reader Project

ARJIS has provided the infrastructure for a single repository of license plate reader data that can be accessed by all member agencies. A total of 12 agencies contribute license plate data to the single database. In addition, the SANDAG PSC has approved an acceptable use policy for all members who participate in the program

Risk Analysis Center Software

The SDUA and the Law Enforcement Coordination Center have deployed the Haystax -CalCOP solution to catalog the regions infrastructure, perform core capabilities assessments and provide analysis of the region's risks. These tools support the development of the San Diego Urban Area Security Strategy and Threat Hazards Identification Risk Assessment.

NetRMS Interfaces

Several law enforcement agencies have adopted Motorola's NetRMS records management system. ARJIS has worked with those agencies that are using NetRMS to build interfaces to the ARJIS data network

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

system. This has allowed near real time sharing and viewing of crime reporting information. A total of seven interfaces have been completed.

ARJIS Law Enforcement Dashboard

ARJIS has built a platform for law enforcement regional situational awareness using the Omega software. Law enforcement users can visualize data in a dashboard and geospatial format to improve their situational awareness in near real-time. Information includes recent calls for service, crime reporting, critical infrastructure plans, license plate reader data and the ability to perform crime analysis.

Mobile Data Devices

There have been several efforts by law enforcement, fire and EMS providers to deploy mobile data devices in the field. Some of these efforts are multi-jurisdictional shared efforts and some are unique to the individual agency.

ARJIS Mobile

With support from ARJIS, several law enforcement agencies have deployed 456 mobile devices across 35 agencies. The ARJIS Mobile program provides access to Mobile Field Interview, SRFERS tactical query, facial recognition and COPLINK. This project has focused on the Android operating system.

Sheriff Mobile

In 2015 Sheriff's Department began large scale deployment of the mobile devices (phones and tablets). To date the Sheriff's Department has deployed over 1800 mobile devices. These devices provide our users with secure and seamless access to a variety of resources. Access is based on the user's role within the Department.

Fire and EMS

The Fire and EMS communities have deployed hundreds of devices across the SDUA. This includes a variety of types of devices and operating systems. The primary function of these devices has been patient care reporting, fire inspection reporting, situational awareness mapping, special event management, incident location routing, field collection of facility information and access to structure and wildland preplans.

ARJIS Network and Data Center

ARJIS has transitioned their previous data center to the National Law Enforcement Telecommunications System with failover capability at SANDAG. This transition has also moved the ARJIS network servers to a virtualized server environment.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Palantir

The San Diego Law Enforcement Coordination Center has implemented the Palantir Software solution. Palantir brings together data from multiple sources, displays and models data from disparate other IT systems, enables real time updates of information, manages access to the data for security and privacy, visualizes the relationships of data and assists the discovery of connections, trends and patterns in support of law enforcement investigations.

ARJIS CAD Interfaces

ARJIS has completed three Computer Aided Dispatch interfaces that send data to the ARJIS Dashboard (Omega) to display near real time display of current or recent calls for service. The El Cajon, La Mesa and San Diego Police Departments are currently connected.

ARJIS Net Portal

ARJIS has developed a web based portal system that provides law enforcement personnel with a single sign on location to access a variety of resources in one location. This substantially reduces the number of login processes for law enforcement personnel.

Law Enforcement Coordination Center Cyber Security

The LECC has assumed a lead role in supporting the SDUA on issues of cyber security. This has included providing intelligence, awareness, training, incident response and information sharing.

Capability Gaps

Regional CAD Interoperability

The capability of the CAD Interoperability has become mission critical for the SDUA fire communications centers. This capability greatly improves the emergency response system. It is unknown at this time what the long term technology solution will look like to maintain this capability.

Mobile Data Devices

The increasing use of mobile devices to access information creates additional opportunities to expand use to more public safety personnel. Currently, mobile devices are not available to all public safety personnel. An important capability of for these mobile data devices will be the use of shared applications that can work on a variety of operating systems. These applications should focus on the sharing of information across jurisdictions and disciplines.

ARJIS Dashboard

While several agencies are utilizing the ARJIS Dashboard for calls for service, license plate reader data, crime reporting and crime analysis, not all law enforcement agencies are using the capability to its full capacity. This includes the need for additional interfaces and training of personnel on the capabilities.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Law Enforcement Data Enhancements

Additional data sources or enhancements have been identified for including in the ARJIS environment. This includes the addition of data from the Probation Department, Parole Date and Firearms information. This also includes required changes to the Uniform Crime Reports and National Incident Based Reporting Systems to include use of force and bias based policing.

Risk Analysis Center (CalCOP)

Some infrastructure asset data is 7 years old and some sectors have limited information. The capability assessment is 3 years old and should be updated as a part of the update of the San Diego Urban Area Security Strategy process.

Mobile Device Data and Security

The expanding use of mobile devices for public safety personnel creates new data and device security challenges. Significant progress has been made by ARJIS to solve data and security issues for law enforcement use of mobile devices. The fast paced evolution of the mobile environment will require additional, ongoing effort to stay current with the technology and operating system updates.

Prehospital Emergency Medical Services Information System

The current County of San Diego Emergency Medical Services patient care reporting system has limited capability to provide near real time collection of patient care and tracking. The County of San Diego is in the process of procuring a new emergency medical services information system that will provide near real time patient care reporting, tracking and analytics. It is anticipated that the new system will be operational early 2017. Agencies utilizing a third party patient care reporting system will be required to implement a near real time interface between their system and the County of San Diego. Full integration between all prehospital EMS providers is anticipated in late 2017.

Cyber Security

The growing threat of cyber-attacks on public and private infrastructure and networks has left many public and private entities trying to catch up with implementing effective protective and response measures. The San Diego Law Enforcement Coordination Center (SD-LECC) is in an ideal position to support the SDUA by providing information on current threats and available resources to prevent and mitigate cyber-attacks. The amount of resources available to the SDUA to deal with this emerging and growing threat is limited.

Wireless Data Services

First responders and emergency managers are increasingly reliant on internet, web browser based tools to communicate or gather intelligence from the field. Many of these incidents are in remote locations where wireless data coverage is limited. The reliability of wireless data services can also be impacted by

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

competition for commercial resources with the public during high events that cause a high demand on the system. The reliability of wireless data services can also be degraded when infrastructure is damaged.

Resource and People Location Services
The SDUA has limited regional capability to provide near real-time location data and asset visualization. Most law enforcement, fire service and EMS agencies utilize resource tracking capabilities through automatic vehicle locating technologies to support emergency response decision systems such as computer aided dispatch.

Many of the current vehicle location systems are dependent on commercial cellular service connectivity to transmit position location. The reliability of this method can be impacted by poor coverage or competition to connect during events with high demand for service.

The SDUA does not have a regional capability to locate individual personnel, equipment and assets in near real time. Another gap in this area is the ability to locate people such as when needed for family reunification or witnesses.

The ability to track vehicles, individual personnel, equipment, assets and locate people in near real time would increase situational awareness and provide valuable information for decision makers.

Palantir
The LECC has acquired and implemented the use of the Palantir application to assist with law enforcement intelligence coordination. Not all law enforcement agencies in the SDUA have received the necessary training and access to utilize the Palantir application.

Initiatives

2.1 Regional CAD Interoperability.
Evaluate future technology options for maintaining the RCIP capability.

Recommended milestone
Complete the evaluation within 12-24 months.

2.2 Mobile Data Devices
Expand the use of mobile data devices and common applications for information sharing across jurisdictions and disciplines.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Recommended milestone
Ensure that a majority of first responders have access to mobile data devices and shared applications within 36 months.

2.3 ARJIS Dashboard/CAD Interfaces

Expand the number of agencies contributing data and utilizing the dashboard for situational awareness and crime analysis.

Recommended milestone
Ensure that the majority of law enforcement agencies have access to the Dashboard capability 24 months.

2.4 ARJIS Data Enhancements.

Integrate additional sources of data into the ARJIS data sharing environment. This includes probation data, parole data, firearms data and required changes to the Uniform Crime Reports and National Incident Based Reporting Systems to include use of force and bias based policing.

Recommended milestone
Complete the enhancements within 12-24 months.

2.5 Prehospital Emergency Medical Services Information System

Complete the implementation of the new County of San Diego Prehospital Emergency Medical Services Information System and integration with all prehospital care providers to provide near real time patient care information, patient tracking and analytics.

Recommended milestone
Complete the implementation within 12-24 months.

2.6 Cyber Security.

Ensure the SD-LECC has adequate resources to support the SDUA's emerging cyber security threat through intelligence, awareness, training, incident response and information sharing.

Recommended milestone
Evaluate the resource requirements and ensure adequate capability within 12-24 months.

2.7 Risk Analysis Center Infrastructure Asset Data

Update the infrastructure asset data to address data gaps and provide a more complete picture of assets and risk. Complete an update of the SDUA capabilities to support an updated Security Strategy.

Recommended milestone
Identify necessary resources and complete an update to the data within 12-24 months.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

2.8 Mobile Device and Data Security Enhancements.

Continue to develop best practices for managing mobile devices and ensuring data security.

Recommended milestone
Ongoing, evolving effort over the next 36 months.

2.9 Wireless Data Services

The SDUA should develop additional capabilities to strengthen wireless data services for incidents in areas that have limited commercial coverage, provide a contingency for damaged infrastructure and for events that create a high demand for access.

Recommended milestone
Identify and implement solutions to strengthen wireless data services within 12-24 months.

2.10 Resource and People Location Services

The SDUA should evaluate opportunities to strengthen the reliability of automatic vehicle locations services and develop regional capabilities to track the location of individual personnel, equipment and assets in near real time that can be displayed in a visual tool. This should include tools that would support family reunification and witness location services.

Recommended milestone
Identify and implement a Resource and People Location system within 24-36 months.

2.11 Palantir

Provide all interested law enforcement agencies in the SDUA with the necessary training and access for use of the Palantir application.

Recommended milestone
Provide the necessary training and access to interested law enforcement agencies within 12-24 months.

Challenges

- Identifying best long term technical path forward on CAD interoperability.
- FirstNet implementation is likely to take several years to implement.
- Development of data standards.
- Constantly evolving mobile operating system changes.
- Meeting requirements for both IOs and Android.
- Funding sources for initiatives.
- Implementation and training impacts on new technology capabilities.
- Developing the right expertise for cyber security issues.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

7. GOAL 3—INTEROPERABLE GEOGRAPHICAL INFORMATION SYSTEMS

The SDUA should continue to provide and improve the regions interoperable geographical information systems and capabilities. Most data has a geospatial connection and can be referenced to a real-life location on the ground. Data maintained in this manner is more valuable because it provides the user with the ability to analyze the relationship to that of other data or features on the ground. Geographic information systems provide the capability not only to look at feature locations, but also to analyze their spatial relationships.

A comprehensive regional emergency geospatial information network increases the capacity for risks to be assessed and prepared for; assets to be positioned and managed; people to be warned; personnel to be deployed; damage to be assessed; rescue efforts to be targeted; and restoration activities to be tracked. Geospatial technology allows for multiple sets of information to be analyzed, modeled and correlated in order to find patterns that can lead to improved strategies for prevention, response and mitigation. Perhaps the most important role of geospatial information and geospatial technologies is that of an information integrator, providing both a canvas on which to post information from a wide variety of sources, and the tools to combine, visualize and make sense of the data. In this way, geospatial capabilities are a key component to decreasing or mitigating risk by providing the common operating picture needed by Public Safety personnel to see the whole situation simultaneously and develop an appropriate, coordinated response. In addition, geospatial technology allows aspects of that common operating picture to be shared with the media in order to prepare the public, keep them informed and seek their assistance.

Accomplishments and Current Activities

Regional Public Safety Geodatabase Program (RPSG)

The RPSG program has provided a regional approach to development of public safety GIS needs. This includes many aspects:

- Created single repository for the public safety geodatabase (Chula Vista server and Amazon Web Services)
- A regional data schema for public safety geospatial data has been developed and implemented. This includes data such as streets, addressing, routing, preplan templates and map books.
- Completion of 2,500 Digital Target Hazard Preplans (Fire Preplans) in a common, regional template format.
- Completion of 70 high priority Wildland Urban Interface Fire Emergency Response Plans.
- Geodatabase Synchronization Phase 1 (analysis) of data with SanGIS.
- Common Operating Data Services Developed ready to use GIS services that are interoperable and can be easily shared as a single source of information.
- SanMAPS Group Implemented ArcGIS Online tool to create a GIS data sharing group.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

- Acquired high resolution aerial imagery for the SDUA.

Situational Awareness Mapping Applications

An assessment of options for situational awareness mapping options for the SDUA was completed in 2015. Recommendations were provided and adopted by the Unified Disaster Council. The recommendations included focusing on the use Next Generation Incident Command System (now SCOUT) and development of the SanMAPS Emergency Operations Center (EOC) Incident Template. The SCOUT solution is in the process of deployment and the EOC Incident Map has been developed and is ready for use.

InSIDeR

InSIDeR, operational as of March 2015, is a geographical viewer application accessible through the secure SDLaw portal. InSIDeR is a repository of infrastructure information that can assist first responders during tactical response, crisis management, search and rescue efforts, and emergency planning. The viewer displays a digital map with facilities in San Diego County that can be selected to retrieve information that may be imperative during emergency response

InSIDeR includes the following types of products:

- Fire Preplans/Floor Plans – digitized fire preplans, digitized facility floor plans, or other types of digitized facility plans
- Virtual Walkthroughs – digital product that first responders can use to view the interior and exterior spaces of a facility using 360 degree panoramic photos and existing floor plans or fire preplans. The virtual walkthroughs are a "snapshot in time" and not a real-time product.
- SWAT Tactical Surveys – produced by law enforcement and provide information that may be needed during tactical response. Information included in the survey can include utility shutoffs, building composition, door construction, obstacles/hazards on-site, etc.
- First 30-Minute Guides – Provides information about a facility that may be needed by first responders during the initial response phase. Information includes facility contact information, gate codes or Knox box locations, max persons on-site, law enforcement initial perimeter posts, hazmat on-site, critical nodes such as utility shutoffs and electrical control rooms, and aerial maps of the facility.

Capability Gaps

Remaining high priority Digital Target Hazard Plans

The SDUA has approximately 1,000 high priority infrastructure sites that do not have a site plan completed in the regional database format.

Geodatabase synchronization between RPSG and SanGIS

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Due to the differences in mission objectives, the GIS data layers in SanGIS and the Regional Public Safety Geodatabase or Computer Aided Dispatch Systems have developed differences on available data and how the data is stored and identified. Where possible, these two databases should be as close to the same as possible. In order to accomplish this synchronization of data, an effort to fix or accept the differences is necessary.

Operationalize Situational Awareness Mapping Tools

In 2015, the SDUA decided to focus situational awareness mapping efforts around two applications. They are the ArcGIS suite of software and the Situational Awareness Collaboration Tool (SCOUT) hosted by California Office of Emergency Services.

While these tools have been developed, the process of operationalizing the tools into the work flow is still a work in progress. Progress can be made through training efforts, exercising the tools and inserting the tools into workflows.

San Diego Multiple Agency Public Safety Services (SanMAPS)

In 2015, the SDUA began using the ArcGIS Online Group called SanMAPS to share common data services that are found in GIS format. A user guide and initial training has been developed. Additional training on use of SanMAPS is necessary to make further progress in developing this sharing method across the SDUA.

ARJIS GIS Support Services

The increased use of geospatial tools has created a need for additional technical support to implement the capabilities. Many local law enforcement agencies do not have the necessary GIS expertise to develop GIS tools to support their mission. It is critical to ensure the regions data is validated properly using SanGIS and a standard geo-coding service to ensure consistency among the various law enforcement agencies. Without the necessary technical support, many of the geospatial capabilities are under-utilized. ARJIS is positioned to provide GIS support services to its members with the addition of GIS analyst.

Next Generation 911 GIS Data

The Next Generation 911 system will be greatly dependent on a statewide aggregated GIS data service for geospatial routing of 911 calls. The SDUA must develop a plan for how the region will create and maintain a regional GIS system necessary to support the Next Generation 911 system requirements.

The SDUA has not made a decision on how to best meet the future requirements of an aggregated geodatabase for the Next Generation 911 system.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

InSIDeR Plans
In order to complete the InSIDeR plans for the high priority sites in the SDUA, there is a need for the continuation of collection and production of fire preplans, SWAT Tactical Surveys, First 30-Minute Guides, and Virtual Walkthroughs to be included in InSIDeR for first responder awareness and preparedness. Gaps include agreed upon priority assets, which is ultimately determined by individual agencies, and the inclusion of that information in InSIDeR. Currently, Virtual Walkthroughs are not able to be viewed on a mobile device. The ability to view Virtual Walkthroughs on a mobile device would be beneficial for first responders.

Initiatives

3.1 Digital Target Hazard Plans (Fire Preplans).
Complete the remaining high priority site plans.

Recommended milestone
Complete the remaining high priority plans within 36 months.

3.2 Synchronization of data between Regional Public Safety Geodatabase and SanGIS.
Complete the process of analyzing the differences in databases and develop an ongoing business process of synchronizing.

Recommended milestone
Complete the synchronization of the databases within 12-24 months.

3.3 Situational Awareness Mapping Tools.
Provide additional training and tools to operationalize situational awareness mapping tools.

Recommended milestone
Provide the additional training and tools within 12-24 months.

3.4 SanMAPS
Provide additional training, exercises and development operational policies and procedures for all stakeholders in the SDUA.

Recommended milestone
Provide the additional training, exercises and policies and procedures within 12-24 months.

3.5 ARJIS GIS Services
ARJIS is positioned to develop GIS tools including mobile applications that can be used to support local law enforcement agencies perform their mission. These tools can be developed on the existing regional

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

platforms utilizing ARJIS GIS support staff. This will significantly increase the region's geospatial capabilities.

Recommended milestone
Provide GIS support to law enforcement agencies over the next 36 months.

3.6 Next Generation 911 GIS Requirements.

Develop a plan for how the San Diego Operational Area will meet the GIS requirements of the Next Generation 911 system.

Recommended milestone
Develop the plan and make policy decisions on implementation within 12-24 months.

3.7 InSIDeR Plans

The law enforcement community should complete an InSIDeR plan for the remaining high priority sites in the SDUA. This includes the collection and production of information for inclusion on a day-to-day basis, coordinating with participating agencies throughout San Diego County to identify assets that individual agencies determine to be priority for their area of responsibility for inclusion into InSIDeR and manage allocation of resources to collect and produce products for InSIDeR. This also includes the development of technology to view Virtual Walkthroughs on a mobile device.

Recommended milestone
Complete the high priority sites and develop additional mobile capabilities within 36 months.

Challenges

- Creation of Fire Preplans must be supported with resources from the individual agencies to get them completed,
- Significant effort is required to get through the initial RPSG/SANGIS synchronization process.
- Common operating data services require ongoing maintenance to ensure functionality and accuracy.
- Operationalizing of situational awareness mapping tools will require significant training efforts.

8. GOAL 4 – GOVERNANCE

The SDUA will need to identify long term solutions for maintenance and sustainment of those projects that will be ready to transition to a program. Many of the current technology projects that were created through the use Homeland Security funding do not have clear plans for where they will be supported in the future. In the interim, many of these projects have developed operational, technical or executive steering

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

committees with regional representation. As these projects transition to programs and the possibility of reduced grant funding, the region must identify a solution that is capable of supporting the required maintenance and sustainment funding.

Accomplishments and Current Activities

Regional Public Safety Geodatabase (RPSG) Governance
The Unified Disaster Council accepted the governance role for RPSG project.

Regional CAD Interoperability Governance
The RCIP Memorandum of Understanding expired and a transition of governance to the Unified Disaster Council was approved.

3C's Public Safety Data Network Transition
The internet protocol based microwave backhaul equipment has been transferred and repurposed where possible by the City of San Diego SafetyNet and the Regional Communications System. This transition has allowed for the dissolution of the 3C's Memorandum of Understanding.

ARJIS Acceptable Use Policies
ARJIS has developed and approved regional acceptable use policies for the License Plate Reader and Facial Recognition capabilities.

Privacy impact assessments
Completion of privacy impact assessments for technologies such as license plate readers, facial recognition and live video sharing of Metropolitan Transit Systems cameras with local law enforcement agencies,

Capability Gaps

Regional Public Safety Geodatabase Sustainment
The long term solution for providing services and sustainment needs to be determined.

RCIP Sustainment
A governance document for sustainment and funding needs to be completed by the fire communications centers.

Regional Technology Partnership (RTP) Support Services
The type of services and method for maintaining RTP support services needs to be determined and procured.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

New Technology Policies and Procedures
New technologies will continue to require development of policies and procedures. This includes issues such as records retention, privacy impact assessments, data sharing agreements and best practices for new technologies.

Initiatives

4.1 GIS Program Sustainment

Identify the long term solution for providing services and sustainable funding.

Recommended milestone
Identify the long term solution for providing services and sustainable funding within 12-24 months.

4.2 RCIP Program Sustainment

Develop and adopt a governance document that supports sustainment and funding between the fire communications centers.

Recommended milestone
Develop and adopt a governance document within 12 months.

4.3 Regional Technology Partnership (RTP) Services

Identify the types of services, complete procurement and determine future funding needs or sources.

Recommended milestone
Complete the implementation within 12-24 months.

4.4 New Technology Policies and Procedures

Develop new policies and procedures as new technologies are created. The can include privacy impact assessments, acceptable use policies, records management, data sharing agreements and best practices.

Recommended milestone
Ongoing development of policies and procedures over the next 36 months.

Challenges

- The process for procuring services or establishing a recruitment process for program support can be a lengthy and difficult process.
- The SDUA will need to identify alternative funding sources beyond grant funding to sustain new capabilities.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

9. IMPLEMENTATION STRATEGY

The implementation strategy utilizes the eight goals from the San Diego Homeland Security Strategy to organize the region into investment groups. The key stakeholders from each goal have been identified and are represented in the following organizational chart;

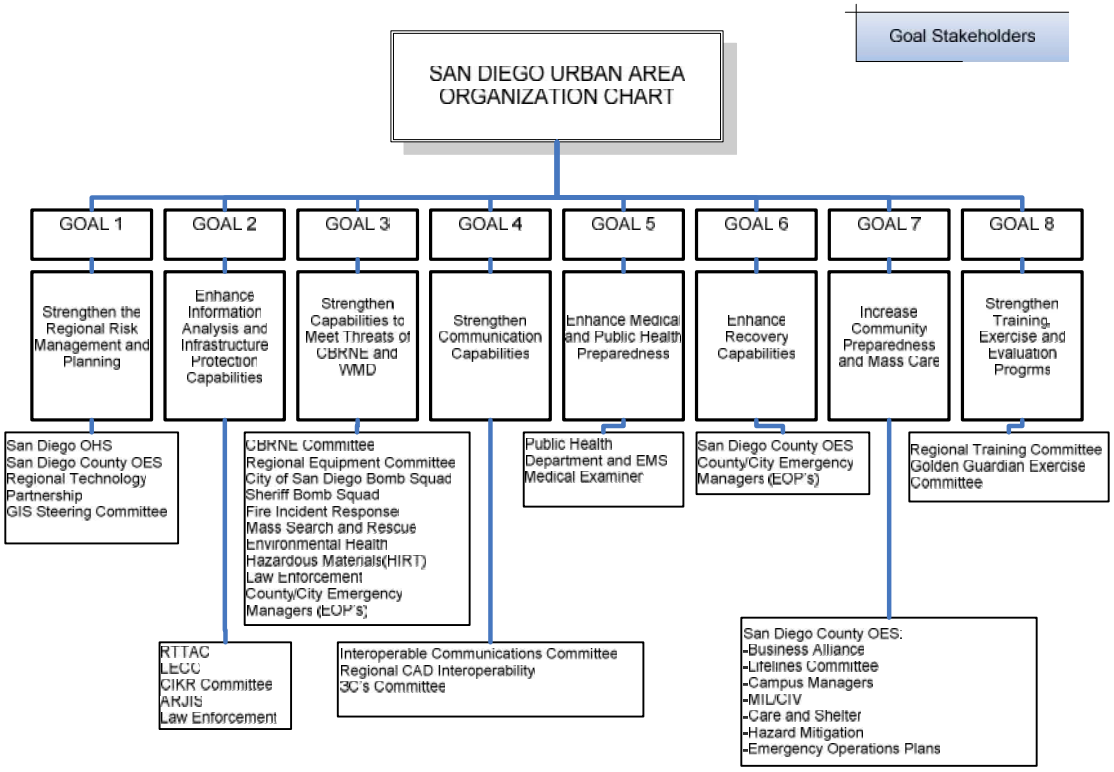


Figure 1—Organizational Chart

Each of these goals has objectives that have been identified through the Security Strategy based upon the identified gaps, risk and capabilities assessment. These stakeholders utilize that information to support investment proposals that can be submitted for consideration. If the Urban Area Security Initiative grant is the funding source, the City of San Diego Office of Homeland Security collects those proposals for the region. For UASI funding, the RTP has been designated as the first level review for prioritizing and ranking projects for funding consideration. The RTP provides recommendations to the Urban Area Working Group on how projects are scored for meeting the needs of the Security Strategy and regional benefit.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

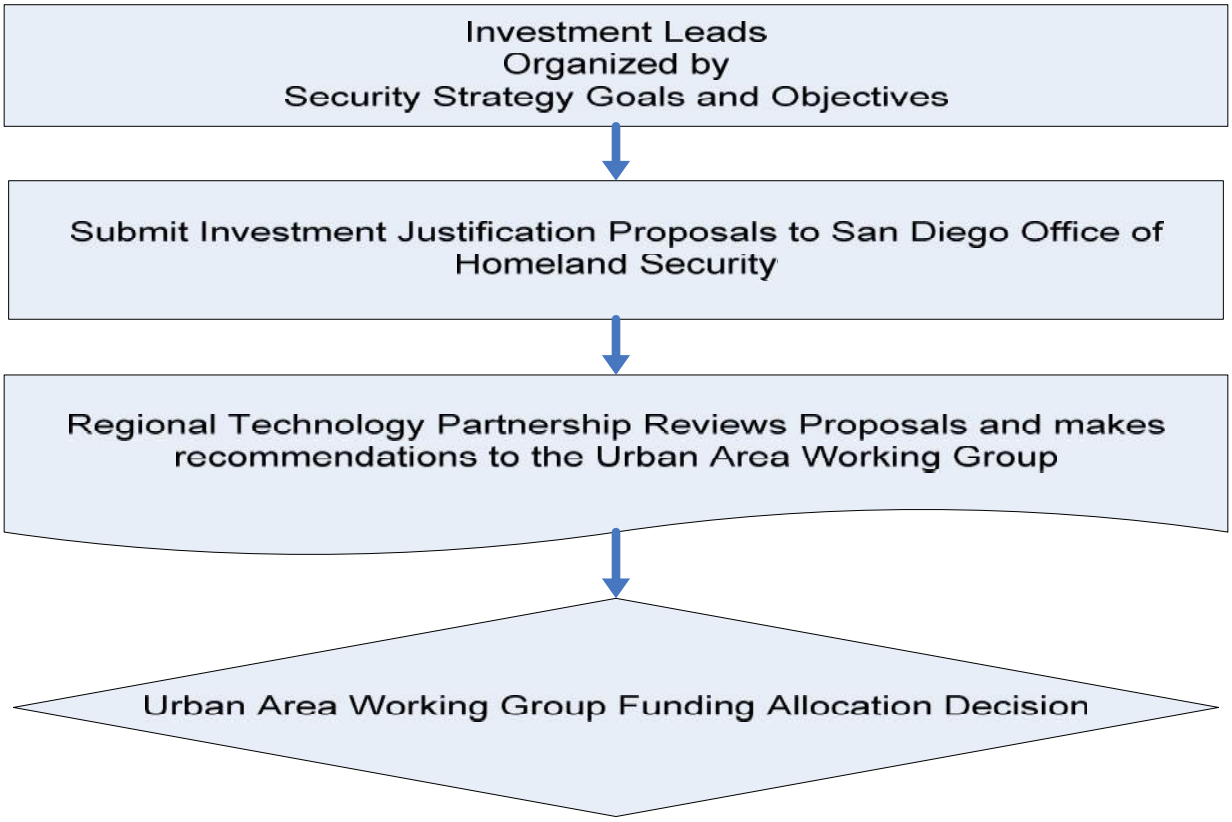


Figure 2—UASI Investment Proposal Process

This process currently only applies to the UASI funding. Consideration should be given to utilizing this process for any additional future regional funding sources.

The remainder of this page is intentionally left blank.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

10. SAN DIEGO URBAN AREA TECHNOLOGY INVESTMENTS

For many years, San Diego has engaged in many regional technology projects to improve their everyday prevention, protection, mitigation, response and recovery through regional interoperability technology solutions. This section provides an overview, status and vision for the End State for several of these projects.

City of San Diego and Regional Communications System Migration to P25 Standard

OVERVIEW

Project 25 (P25) or APCO Project-25 refers to a suite of standards for digital radio communications for use by federal, state/province and local public safety agencies to enable them to communicate with other agencies and mutual aid response teams in emergencies. Agencies in the SDUA share the vision of a standards-based Regional Public Safety Communications System. The migration of the RCS from the current Motorola SmartZone 3.0 architecture, combined with the migration of the City of San Diego from the Motorola SmartZone 4.1 architecture to a P25 system in the SDUA will allow for the highest degree of equipment interoperability, compatibility and economy of scale for all agencies in the region, while leveraging, to the greatest extent possible, the existing infrastructure in both systems.

Project 25 is an open-system technical standard that has been nationally developed for more than 15 years. The P25 Steering Committee sought to establish open system standards so multiple vendors could make competing products that are compatible. Many of the P25 technologies are still privately owned or proprietary. However, the P25 Steering Committee only selected proprietary technologies as a recommended standard when the owners agreed to freely share the technology with other competing vendors. Every aspect of P25 is designed to benefit Public Safety agencies with a new level of performance, efficiency, capability, and quality in two-way radio communications. The four key objectives of the P25 Steering Committee include:

- Enhanced functionality with equipment and capabilities focused on public safety needs.
- Improved spectrum efficiency.
- Assured competition among multiple vendors through Open Systems Architecture.
- Effective, efficient, and reliable intra- and inter-agency communications.

By adhering to these objectives, P25 makes it easier for agencies to make informed decisions when planning to convert from an existing system to a P25 digital system. Agencies are able to compare the direct features and benefits of different vendor systems and equipment. The purpose is to make the procurement process more competitive and fair.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

The P25 standard continues to be developed as the technology evolves and additional parts of the complex standard are addressed. A basic P25 requirement for new digital radio equipment is backward compatibility. This supports a phased migration into mixed analog and digital systems, allowing agencies to gradually trade out radios and infrastructure equipment.

Even though P25 networks will be backward compatible, the current RCS product life is nearing the end of life; therefore, supporting the current infrastructure will become increasingly difficult. The end of the RCS product life cycle increases the importance of planning for the phased upgrade and replacement of the current radio system infrastructure and identifying the funding necessary to transition to a P25 network.

STATUS

Local first responders in SDUA currently operate on two shared 800 MHz radio systems; the RCS and the City of San Diego Radio System (CSDRS) for primary public safety voice communications. Both systems are in the early phases of upgrading to P25.

City of San Diego Radio System

The City has implemented a metro San Diego Motorola Digital 700 MHz P25 trunked radio system which seamlessly links into the existing 800 MHz Analog Motorola SmartZone 4.1 system. The metro San Diego P25 radio system is operational on 20 channels at six radio hi-site locations and two ASR (Intelli-repeater) site locations with approximately 900 subscriber units. Both San Diego PD dispatch and SD Unified Schools PD dispatch are cut-over to P25 7500 consoles and SD Fire Rescue will be cut-over by late 2016. The City completed construction of a Nokia IP/Ethernet MPLS backhaul 1Gig fiber and 200 Mbit microwave system in December 2015. Overall, the metro CSDRS P25 system is currently about 80 percent complete and will be 100 percent complete by December 2017 with an additional hi-site at Otay Mtn.

Regional Communications System

The County has developed a multi-year plan to upgrade RCS to a fully P25 compliant system. In 2013, the County is completed a project to replace the RCS trunked radio proprietary core equipment with a P25 core and interoperable gateways to link the core to the existing Motorola SmartZone 3.0 radio infrastructure. The County then addressed the replacement of the RCS microwave backhaul network with an IP-standards based system (which is required to support a fully P25 compliant system). This project was completed in 2016. The County is currently planning the replacement of the RCS trunked radio system over the next three years.

Another component of this migration is the replacement of portable and mobile radios. Approximately 25% of the current 24,000 devices will need to be replaced by the individual agencies.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

CONVENTIONAL VOICE:
The SDUA has developed a number of sites to provide multi-band gateways between users of these shared systems and other government users who are not equipped to operate on one of these two networks. These systems support both interoperability and mutual aid response to threats in the region and provide backup communications capability. The County is in the process of replacing all of the legacy conventional radios utilized in these mutual aid/gateway systems with P25 capable radios in order to facilitate a future transition to full P25 operations.

VISION OF END STATE
After transitioning to P25 systems, SDUA will be able to link the two systems to provide significantly increased interoperability and potentially increasing network capacity for operating decades into the future. Many of the subscriber radios currently being used on RCS and the City are capable of using both 700 and 800 MHz frequencies. The RCS and the City of San Diego have been allotted sufficient 700 MHz channels for future use in public safety radio communications systems.

Implementation of a Regional network of P25 Radio Systems will provide full digital operation within various spectrums (VHF, 700 MHz and 800 MHz), a higher degree of privacy through improved encryption standards and significantly enhanced user and resource capacity.

The long-range plan for achieving communications interoperability across the SDUA's multi- jurisdictional and multi-agency boundaries includes the long-term convergence of all radio systems to digital, open-standards technology and implementation of the most current version of the P25 standard available at the time of purchase. Project 25 system technologies will allow seamless communication between SDUA Public Safety agencies operating on 700 MHz and 800 MHz spectrum and other P25 Public Safety agencies operating on different spectrum. Federal and State Public system users in the 150 MHz band will have the capability to communicate with SDUA users, since all agencies' users have reciprocal coverage with their radio systems. Through the implementation of the P25 standard, SDUA can achieve seamless interoperable radio communications

VHF Radio Infrastructure

OVERVIEW
As the SDUA transitioned to a trunked radio system, many local government agencies had limited need to maintain their legacy VHF radio infrastructure. As a result, some of the infrastructure sat unused or was allowed to reach its end of life cycle without replacement.

With significant wildland events in 2003, 2007 and 2014, the fire service community has recognized the need to keep a robust VHF radio capability. These events depend heavily on VHF radio systems to support

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

interoperability of mutual aid resources and to meet requirements for communications with aerial firefighting resources.

The county wide power outage and subsequent radio system degradation of the trunked radio system also identified the need to consider backup communications systems, such as VHF.

The availability of VHF radio capability can also assist with system capacity issues on the trunked radio system that can occur during times of high usage. The VHF radio capability allows the opportunity to shift some users off of the trunked radio system, providing additional capacity.

STATUS
In 2012, the County of San Diego Wireless Services Division contracted with Federal Engineering to develop the alternatives and identify the associated costs of additional VHF fire mutual aid resources. While a large scale infrastructure improvement plan was not initiated, small incremental improvements have improved VHF capability in some areas. In 2016, L.R. Kimball was contracted to complete an update on the gaps in VHF capabilities. This report will identify opportunities to improve capacity and coverage and recommend a plan for implementation. The report is scheduled for completion by early fall of 2016.

VISION OF END STATE
The VHF Gap Analysis will provide a road map to developing a robust VHF radio system that can support interoperability during incidents requiring mutual aid resources, provides a backup communications system to the trunked radio system and can provide additional voice communication capacity during times of high use.

Regional Video/Web Conferencing

OVERVIEW
Video and web conferencing solutions have proven to be a useful communications tool when multiple stakeholders are in different locations. In 2006, the SDUA allocated funds to support a video teleconference system to be hosted on the 3C's Public Safety Data Network video teleconference room systems and the necessary infrastructure was deployed to approximately 70 locations in the SDUA.

STATUS
Much of the original equipment provided for as part of the 3C's program is reaching its end of life cycle. In 2015, the RTP Program Manager was tasked with identifying solutions for replacing the existing system. The report recommended transitioning to a cloud hosted solution that could possibly leverage the remaining life on the existing room systems and could be used across a variety of platforms such as desktop computers, laptops, tablets and phones.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

The County Office of Emergency Services has been allocated UASI funding to implement a cloud hosted video/web conferencing solution. This project will provide a cloud hosted service to provide connectivity and interoperability between local and interagency organizations.

VISION OF END STATE
Provide the members of the Unified Disaster Council with a common platform for video and web conferencing.

Regional Tactical Interoperability Communications Plan

OVERVIEW
The Tactical Interoperable Communications Plan (TICP) is designed to allow urban areas, counties, regions, states, territories, tribes, or federal departments and agencies to document interoperable communications governance structures, technology assets, and usage policies and procedures. The TICP is used to clearly define the breadth and scope of interoperable assets available in the area; how those assets are shared and how their use is prioritized; and the steps individual agencies should follow to request, activate, use, and deactivate each asset. Completed TICPs were required for all 2005 Urban Area Security Initiative (UASI) sites and are encouraged for newly designated UASI (and non-UASI) cities, counties, multi-county regions, tribes, and states/territories.

STATUS
In 2014, L.R. Kimball was contracted to update the Regional Tactical Interoperability Communication Plan. This plan is a combination of a Tactical Interoperability Communications Plan and system failure plans, SOP's and strategic planning.

VISION OF END STATE
As radio systems are enhanced or modified, the TICP will require occasional update to reflect the changes.

Regional Community Emergency Notification Systems

OVERVIEW
The SDUA has developed a variety of methods for keeping the public informed before, during and after an emergency. While many of the SDUA communities utilize a variety of methods for communicating with their residents at a local level, the County of San Diego Office of Emergency Services has taken the lead on providing regional emergency notification systems. The County of San Diego Office of Emergency Services utilizes a variety of methods to communicate emergency public information with the region.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

AlertSanDiego

The County of San Diego, in partnership with Blackboard Incorporated., has instituted a regional notification system that is able to send voice, text message, and email alerts and notifications to residents and businesses within San Diego County impacted by, or in danger of being impacted by, an emergency or disaster. This system, called AlertSanDiego, is used by emergency response personnel to notify those homes and businesses at risk with information describing the event and actions (such as evacuation) they are asking them to take. The system utilizes the region's 9-1-1 database, provided by AT&T, and therefore is able to contact landline telephones whether listed or unlisted. It is Teletype/Telecommunication Device for the Deaf (TTY/TDD) capable.

Because the system uses the 9-1-1 database, only landline numbers are in the system. If the resident has a VoIP or cellular telephone and would like to be notified over that device, or if they want to receive a text or email notification, they must register those telephone numbers and/or email addresses for use by the system.

Accessible AlertSanDiego

This service provides accessible emergency public information to residents of San Diego County who are deaf, blind, hard of hearing and deaf/blind. Accessible AlertSanDiego sends accessible alerts and information to Internet and video capable devices, such as computers, cell phones, smart phones, tablet computers and wireless Braille readers. These alerts are offered in American Sign Language (ASL) with English voice and text.

SDEmergency Website

The "go to" source for information online during a disaster is www.SDCountyEmergency.com. This website will be promoted to the media/public as the official disaster information website. The site will include: maps depicting impacted areas; evacuation zones; shelter locations; disaster perimeters; Local Assistance Centers; feeding sites; social media feeds of the primary responding organizations; press releases and resources produced by the County; and other pertinent disaster related information.

The ReadySanDiego site features preparedness local hazard information and educates and empowers residents to make a Family Disaster Plan, build an emergency supplies kit, stay informed with AlertSanDiego, and get involved with emergency response programs such as Community Emergency Response Team (CERT). The SDCountyRecovery site provides specific recovery tools and resources to maximize disaster assistance to eligible public and private entities and residents through various local, state, and federal disaster assistance programs.

Mobile Applications

The SD Emergency App contains disaster preparedness information, interactive checklists for residents to create their emergency plan, build an emergency supplies kit, and when disaster strikes; the SD

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Emergency App will keep them informed with emergency updates, social media feeds, interactive emergency maps and shelter locations and statuses. The SD Emergency app leverages push notification technology to quickly notify app users of new emergency updates.

The County of San Diego Office of Emergency Services (OES) created the SD Emergency App to better prepare and inform San Diego County residents and visitors about disasters. With SD Emergency, the tools they need to plan, prepare and respond in an emergency are right at their fingertips.

Wireless Emergency Alerts (WEA)
OES has partnered with this FEMA administered system that provides alerts and notifications to cell telephones in specific geographical areas. The local integration of WEA included a regional field test in San Diego County to test the system. WEA is accessed through the Integrated Public Alert and Warning System (IPAWS).

Emergency Alert System (EAS)
The EAS system is used to provide emergency information to the public utilizing area radio, television, satellite and digital media. It is a federally designated system that is mandated by the Federal Communications System, all area broadcasters are encouraged to participate. The EAS warning is received by the entire region and not just those in the affected area, therefore an accurate description of the area affected is a required part of the message. The primary EAS station for San Diego County is KOGO AM 600. The secondary station is KLSD AM 1360.

Social Media
Numerous County departments engage residents through social media. During a disaster the OES and County Twitter (@readysandiego, @sandiegocounty), Facebook (ReadySanDiego, sandiegocounty) and YouTube (ReadySanDiego) accounts will be publicized as the “go to” source for information in the social media realm during a disaster. County Communications and/or OES will utilize Tweetdeck, a program which allows us to send one message to multiple Twitter and Facebook accounts. In this way, we will send the same disaster related message out to County, OES, Public Works, HHSA and any other appropriate departmental social media accounts.

211 San Diego - 2-1-1 provides a 24/7 hotline connected to a highly trained team providing the up-to-date information in an emergency. Vital information about conditions and services such as road closures, evacuation routes, shelters and more.

STATUS
The SDUA has supported a regional approach to emergency notification systems. This approach is especially effective when an emergency is multi-jurisdictional and impacts many agencies. At the same time, through an MOU, local agencies are given training and limited access to utilize the alerting systems at

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

a local level. This allows a more effective approach and eliminates duplication of effort for emergency notification systems.

The Office of Emergency Services has expanded the mobile application resource by adding links to each of the interested cities in SDUA. This again provides a resource of information for preparedness from a regional approach and avoids duplication of effort.

VISION OF END STATE
The SDUA will continue to enhance the methods for communicating information to the public before, during and after emergencies. The Office of Emergency Services is the natural lead for a regional approach to this function. While local agencies will continue to manage communication with their jurisdictions at their own local level, they should continue to leverage the regional resources to avoid duplication of effort. These emergency notification systems go well beyond the early concepts of calling landlines for alerts and notifications. They now include methods such as texting, social media, emails, cell phones and mobile applications. Of special interest will be the Wireless Emergency Alerts (WEA) System that will be able to send emergency notifications to all WEA capable cell phones based on the user's geographical location.

Regional Computer Aided Dispatch Interoperability Project

OVERVIEW
The Regional CAD Interoperability Project (RCIP) allows SDUA Fire Communications Centers' CAD systems to seamlessly exchange data between each system where appropriate, regardless of the manufacturer. The solution is flexible enough to accommodate future CAD interoperability requirements and provide for growth to accommodate additional public safety agencies and functions as needed. Integration with selected third party systems, such as ambulance and utility companies has also been implemented.

Through a competitive bid process, Thinkstream Inc. was selected and contracted to implement this capability in 2009.

To support this project, a Memorandum of Understanding (MOU) was executed by the interested parties. The MOU provided for governance through an Executive Committee, Steering Committee and Technical Group.

STATUS
By 2012, four Fire Communications Centers were connected and utilizing the system to allocate fire and EMS response resources across communications centers jurisdictions. This capability greatly reduced the time required to request resources from contiguous agencies by performing what used to be a manual function into an automatic function, without the need for a required phone call. The communications centers

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

included San Diego Fire Rescue, North County Dispatch, Heartland Communications and CALFIRE Monte Vista.

The remaining local government Fire Communications Center is the City of Escondido. Escondido is a combination law and fire dispatch facility. Due to CAD vendor and Thinkstream challenges, this connection has not yet been completed.

In addition, some efforts were made to connect the San Diego Harbor Police to the system due to their interaction with San Diego Fire resources. This connection was not completed.

The original MOU document governing the project was valid for five years. Rather than executing or extending the document, a recommendation was made and approved for transition to a program under the Unified Disaster Council.

In 2015, Thinkstream was forced into a bankruptcy process. This process had a significant impact on any ongoing efforts to add additional connections. As a result of the bankruptcy process, the company's assets were acquired by Thinkstream Acquisition. The new owners of the company have committed to support and maintain the RCIP capability. The City of San Diego Office of Homeland Security executed a short term agreement for maintenance and support through November 2016.

The current effort is focused on completing the Escondido connection and maintaining the system. There is currently no ongoing effort to complete any law enforcement connections.

With the primary focus on fire communications centers only, the governance model under the Unified Disaster Council is under review. A recommendation has been made to transition to a MOU type arrangement between the fire communications centers. Additionally, the procurement of maintenance and support services will transition to a fire communications center for execution and managing. A scope of work to support a request for proposals is under development for the procurement of services after November 2016.

VISION OF END STATE

It is anticipated that the level of interoperability capability between disparate CAD systems will improve over time. In the meantime, a CAD integrator like RCIP is mission critical to allowing communication between disparate CAD systems. The focus in the short term is to maintain the capability, fix bugs and respond to necessary changes that occur as a result of CAD upgrades. In the long term, the Fire Communications Centers will need to identify the best solution for maintaining the capability.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Regional License Plate Reader (LPR) Project

OVERVIEW
In use nationally for the past decade, LPR systems have been regarded as effective tools for identifying and recovering stolen vehicles, and/or vehicles that are wanted in conjunction with a crime, to include AMBER alerts. LPR systems consist of specially designed high-speed cameras combined with sophisticated computer algorithms capable of randomly capturing an image of a license plate and converting the plate characters into computer-readable data. The text files can then be sent to a computer and compared against pre-existing data files, such as 'hot lists' containing records of stolen or wanted vehicles as well as vehicles associated with AMBER alerts, missing persons, wanted subjects or other criteria. If a match is found, the LPR user (law enforcement officer or agency) is notified by an audible alert and an associated notation on the user's computer screen.

STATUS
In 2008, San Diego County law enforcement agencies began procuring their own LPR systems. During this same time, ARJIS partnered with the National Institute of Justice (NIJ) to develop a national LPR standard for sharing LPR data between agencies. In 2009, Urban Area Security Initiative (UASI) funds were awarded to ARJIS to procure a regional server to share LPR data among its member agencies. From calendar year 2009-2014, 11 ARJIS member agencies continued to expand their number of LPR cameras and develop interfaces to send their LPR reads in real-time to the regional server.

Regional LPR statistics gathered from 2009-2014, demonstrated the effectiveness of LPR with the stolen vehicle recovery rate for San Diego County (percent recovered out of the total stolen) improving significantly each year, from 57 percent of the region's stolen vehicles being recovered in 2009 to 82 percent in 2014.

A management report from the San Diego Police Department's Eastern Division highlighted results on one of their LPR vehicles. Those statistics include 407 alerts on stolen vehicles and 202 stolen vehicle recoveries over a 2 ½ year period.

Agencies have reported many other success stories, from carjacking, to sexual assaults, homicides, and felony hit and run incidents that were solved due to LPR data.

The LPR project is a system that captures pictures and data from license plates. The License Plate Reader can be fixed or mobile (handheld or on a vehicle). The value of the LPR systems includes locating and recovering stolen vehicles, solving cases, linking crimes, providing investigative leads and a force multiplier. This project includes the deployment of UASI funded mobile and fixed LPR systems and the

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

regional collection of data. Recognizing that regional data would provide the ability to use LPR data to identify offenders and solve crimes across jurisdictions, and assist agencies by supplying a storage option, ARJIS, at the request of the San Diego HIDTA, partnered with ONDCP to fund a regional server for sharing and accessing cross-jurisdictional LPR data

In 2015, the SanDAG Public Safety Committee approved the Acceptable Use Policy for the Regional License Plate Reader System. The purpose of the Acceptable Use Policy for the Regional License Plate Reader (LPR) System is to outline the responsibilities of ARJIS in its role as a law enforcement information technology provider for the regional LPR server. ARJIS, in cooperation with local, state, and federal law enforcement agencies, maintains the regional LPR data repository in support of law enforcement efforts to improve public safety.

Operational protocols for how the LPR technologies are utilized by law enforcement agencies are dictated by those individual agencies, and must be consistent with the Regional License Plate Reader Operational Protocol (currently in development by the County Chiefs' and Sheriff's Association) California Law Enforcement Telecommunications System Policies, Practices, Procedures, and Statutes (published by the California Department of Justice), and the Criminal Justice Information Services Security Policy (published by the Federal Bureau of Investigation).

The initial LPR policy created in 2012, broadly governed both the technical and operational aspects of license plate reader technology. As this project has now been fully implemented, staff in collaboration with stakeholders developed a dedicated policy focusing solely on the role of ARJIS as the service provider for the project. As an "acceptable use" policy, this document sets forth rules restricting how the system may be accessed and defining how it is maintained. To ensure ARJIS policies are consistent with those at the state and federal levels, ARJIS has collaborated with the International Association of Chiefs of Police (IACP) in the development of the proposed policy.

VISION OF END STATE

As the integration of the regional license plate reader programs continues, a substantial amount of records will be available. Enhancements to the current mapping dashboard will provide geo-analytical tools for LPR to identify trends and patterns. In addition, automated notifications on suspicious vehicles within predefined critical infrastructure and other geo-fenced areas of interest will be developed.

CalCOP-Haystax Risk Management Software

OVERVIEW

The CalCOP-Haystax risk management software combines several modules to create a variety of information for analysis. The modules include;

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

- Asset management - Allows the region to identify and document infrastructure assets.
- Survey assessment tools – Allows the users to develop their own forms for doing security assessments.
- Threat and Hazard Manager – Enables the user to view and adjust threat and likelihoods and combine with asset information for a picture of the threats and hazards in their jurisdiction.
- Capabilities Assessment – Enables users to perform detailed capabilities assessments for the region.
- Risk Analysis Center –Provides default threat and hazard likelihood, vulnerability and consequence data and combines it with the asset catalog to create a risk analysis of an asset, jurisdiction, sector and sub-sector.
- Situational Awareness Map Viewer – Provides map viewer to display information within the system and feeds from outside data sources.

STATUS

While the software has several capabilities, the SDUA has focused on infrastructure asset management, capabilities assessments, threat and hazard manager and the risk analysis center.

The SDUA has entered approximately 5,000 infrastructure assets into the system. The initial upload was accomplished in 2009. The users continue to adjust the threat and hazard levels based on current intelligence information and continue to refine the data. This infrastructure information has been used to understand what infrastructure may be at risk for a variety of threats. While the data in the system provides a good picture of the regions infrastructure assets, some sectors of infrastructure have limited information and the database could be more accurate with an update effort.

A more complete picture of the regions assets would require a substantial effort to update the data. If the SDUA desires a more complete, up to date picture of the infrastructure assets, resources will need to be committed.

The SDUA stakeholders have participated in two workshops that included subject matter experts to provide input on the regions core capabilities. This process assists with identifying the regions strength's and weakness in the core capabilities.

The Risk Analysis Center and Threat and Hazard Manager tool continues to support the development of the San Diego Urban Area Security Strategy.

The funding required to maintain and enhance the software has been provided by the State of California through the use of State Homeland Security Grant Funds, The City of San Diego OHS manages that contract on behalf of the 8 UASI's.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

VISION OF END STATE
The CalCOP-Haystax risk management software will continue to provide a means to catalog infrastructure assets, understand the threats and hazards, complete a capabilities assessment and provide a risk analysis. To maintain an up to date and accurate picture of infrastructure assets and the SDUA core capabilities, the SDUA will need to commit resources to update.

The long term funding picture for this capability is unclear. At this point, the State of California is providing the funding on a year to year basis for the all California UASI's.

NetRMS Interfaces

OVERVIEW
Through a collaborative effort with the Sheriff, ARJIS has developed stable real-time interfaces to agencies, NetRMS systems. Additional agencies have implemented or are in the process of implementing NetRMS. Each agency needs an interface to ARJIS which requires ARJIS staff to program, test, validate, & classify agency data for standardized regional UCR Reporting. Project funds will provide support for the NCPD, CBPD, Sycuan interfaces & a property and evidence module for all of the agencies in the region.

The information is regularly used in both investigative and interdicted efforts thereby supporting both law enforcement and homeland security functions. Effective data sharing allows agencies to fully utilize the information systems as a force multiplier by focusing resources more effectively. It also enhances homeland security effectiveness by aiding in the identification of people/vehicles frequenting critical infrastructure and linking those who may be involved in planning activities.

STATUS
The San Diego Sheriff's Department negotiated a contract on behalf of the region that allows jurisdictions to implement NetRMS records management system at their police agencies. A key requirement in the implementation of NetRMS was to ensure the data captured in NetRMS could be configured into ARJIS for standardization and regional access. To address this requirement, an interface was developed from the Sheriffs NetRMS to the ARJIS Enterprise database to include record types such as crime cases, field interviews, traffic accidents and citations. There are several law enforcement agencies that have completed their implementation. They include:

- El Cajon
- Oceanside
- Chula Vista
- Escondido
- Carlsbad
- San Diego Harbor PD

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

- La Mesa
- Sheriff

Additional agencies in the process of transitioning:

- Coronado
- San Diego
- Sycuan
- San Diego Metropolitan Transit System

Each agency's interface requires customization from ARJIS staff to ensure the data is mapped correctly, standardized for regional UCR reporting and for use in the ARJIS suite of tools.

There are currently seven local agencies that have implemented or in the process of implementing NetRMS. Two additional agencies, National City and Carlsbad have initiated implementations but do not have the resources to fund ARJIS for the required assistance. In addition, the Sycuan Tribe was recently approved by CAL-DOJ and the Sheriff's Department to become a member of ARJIS. Sycuan has requested to contribute records to ARJIS via NetRMS. This is a significant effort as this will be the first time tribal data is shared throughout the region via ARJIS. Without the aforementioned interfaces to ARJIS, agencies would not be able to share the data that resides in each agency NetRMS with the rest of the region. In addition, agencies wouldn't have the capability to use ARJIS tools such as the Dashboard and COPLINK for accessing the data.

VISION OF END STATE

The successful integration of NetRMS data from multiple police agencies to the ARJIS Enterprise database will have a positive impact on the region by facilitating real-time automated entry, validation and classification of crime incidents throughout the region. This results in a much more robust and efficient data exchange mechanism whereby full report narratives, photos and other data elements will interface to ARJIS in near-real time without intervention by data entry clerks. Finally, the timeliness of the data will greatly enhance the investigative capabilities of the ARJIS query tools.

ARJIS Dashboard

OVERVIEW

The ARJIS Regional Mapping Dashboard allows users to organize and analyze geographic information on regional incident data. The Dashboard displays county-wide police incident and officer notification information from agencies that contribute data to ARJIS, crime reporting, critical infrastructure plans, license plate reader data and the ability to perform crime analysis.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

STATUS
During Phase 1, the application was procured, customized, tested, and deployed to ARJIS member agencies and trainings were held throughout the region. While the feedback from users has been positive, there have been requests for an additional phase to deploy enhancements to the application.

The recommended enhancements were compiled and included in a Phase 2 proposal that was submitted to the Urban Area Working Group (UAWG). Responsible for prioritizing the region's proposed UASI projects, the UAWG rated the Mapping Dashboard Phase 2 as a high enough priority for inclusion in the FY 2014 UASI grant application. The Phase 2 enhancements include new mapping layers for the region's critical infrastructure layers such as school floor plans, additional information on the addresses of parolees and high-risk probationers, and the plotting of CAD 911 calls for service.

ARJIS has built a platform for law enforcement regional situational awareness using the Omega software. Law enforcement users can visualize data in a dashboard and geospatial format to improve their situational awareness in near real-time. Information includes recent calls for service, crime reporting, critical infrastructure plans, license plate reader data and the ability to perform crime analysis.

VISION OF END STATE
The ARJIS Dashboard provides a powerful tool for law enforcement personnel to view incident data in near real time and provide access to other data such as LPR and infrastructure site plans. An aggregated view of information across multiple jurisdictions will greatly improve situational awareness. The goal is to have as many ARJIS members providing data and using the tools as possible.

ARJIS Mobile

OVERVIEW
The initial goal of this project was to provide Terrorism Liaison Officers (TLO) capability to access critically needed Public Safety data on a near real-time basis in a mobile environment. Providing the TLO's with mobile data devices with access to Public Safety applications enhanced cross jurisdictional sharing of information and enabled timely officer notifications and alerts. This enhanced the ability to identify suspicious activity and potentially disrupt terrorism and other criminal activities.

ARJIS has taken the lead to provide project management for this technology. ARJIS supported the selection and purchase of the mobile data devices and configured the devices to connect to several sources of information that are useful for law enforcement to have access to in a mobile environment.

STATUS
ARJIS has extended the capability beyond the original TLO's and have been assisting law enforcement agencies with deploying their own mobile devices using the infrastructure that has been built. To date, a

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

total of 456 devices have been deployed to 35 agencies. These mobile devices have access to a variety of applications, including;

- State, Regional Federal Enterprise Retrieval System (SRFERS)
- Mobile Field Interview
- Facial Recognition
- COPLINK

In 2015 Sheriff's Department began large scale deployment of the mobile devices (phones and tablets). To date the Sheriff's Department has deployed over 1800 mobile devices. These devices provide our users with secure and seamless access to a variety of resources. Access is based on the user's role within the Department.

VISION OF END STATE

The ARJIS Mobile environment continues to develop capabilities such as a public safety application store where law enforcement personnel can add applications that are user friendly on mobile devices. The next major initiative will be the ARJIS Mobile ID. The ARJIS Mobile ID is a capability that will allow officers to read individual's identification barcode (i.e.; Driver's License, Military ID) rather than having to type in a name, DOB and/or driver's license number to confirm an individual's identity. More than 200 unique DMV and other ID barcode formats to include every state and military branch, all Canadian provinces and select Mexico states will be able to be authenticated immediately. Information returned on individuals will pre-populate ARJIS applications to query information on wants, warrants, officer notifications and potential terrorists and criminal records.

The Sheriff Department's mobile device infrastructure is designed to be a secure extension of all the service and applications available to the user at their desk. Compatibility with the Department's mobile device infrastructure is required with any new application that the Department implements. Additionally, several existing applications are getting upgraded to be compatible with the mobile devices.

The use of mobile devices by law enforcement personnel is expected to continue to grow. The ARJIS Mobile capability and the Sheriff's mobile device infrastructure provides a secure environment for law enforcement tools that is available to all authorized users in the SDUA.

ARJIS Network and Data Center

OVERVIEW

ARJIS has undergone significant changes in their network and data center through the implementation of the Enterprise project and the City of San Diego dissolving the San Diego Data Processing Center

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

(SDDPC), which served as the data center for ARJIS computers and provided a complete array of IT services, staffing and support to ARJIS.

STATUS
The transition for the network and data center has included:

- A split of the technology environment that was housed at SDDPC into two locations; the network that moved to 401 B Street, San Diego and the data center that was relocated to the National Law Enforcement Telecommunications System in Phoenix.
- Replacement of physical servers with an entirely virtualized server environment
- Executing a contract with Xerox to move the data center and associated connections for 82 member agencies and provide 24/7 support and maintenance of the secure network.
- The addition of servers and storage physically located at SANDAG to provide a failover capability for the Phoenix data center.
- Significant updates to the server environment, including moving to current state of the practice operating systems and software suites.

VISION OF END STATE
This accomplishment of these changes for the network and data center positions ARJIS to begin to enhance offerings available to agencies and their users. The changes also allow ARJIS to continue to improve the technology environment and support a broader mobile solution.

Palantir

OVERVIEW
The San Diego Law Enforcement Coordination Center has implemented the Palantir Software solution. Palantir brings together data from multiple sources, displays and models data from disparate other IT systems, enables real time updates of information, manages access to the data for security and privacy, visualizes the relationships of data and assists the discovery of connections, trends and patterns in support of law enforcement investigations.

STATUS
Currently, 11 local law enforcement agencies are utilizing the software to support crime analysis and law enforcement investigations.

VISION OF END STATE
The goal of this effort is to continue to enhance the available data sources in the system and to maintain the current capabilities. All authorized law enforcement agencies should have access to this analytical tool.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

ARJIS CAD Interfaces

OVERVIEW
ARJIS has developed CAD interfaces that allow real time display of calls for service in the ARJIS Dashboard. This allows law enforcement personnel the ability to easily visualize trends.

STATUS
ARJIS has completed three Computer Aided Dispatch interfaces that send data to the ARJIS Dashboard (Omega) to display near real time display of current or recent calls for service. The El Cajon, La Mesa and San Diego Police Departments are currently connected.

VISION OF END STATE
The goal is to complete as many CAD interfaces as possible. The more connections completed, the more complete the regional picture becomes.

ARJIS Net Portal

Overview
ARJIS has implemented a 'one stop shop' portal for the regions law enforcement personnel to access a variety of resources in one location. The portal allows users to access the 20+ applications maintained by ARJIS as well as other state, regional and federal systems used daily be officers and investigators throughout the region. 'Be-On-the-Lookout' bulletins are posted daily to assist officers in sharing information about high profile cases, officer safety notifications and regional crime trends. Access to policies, user guides and other relevant material can be found on the site, as well as training videos and tips and tricks for using ARJIS applications. Users are able to re-set their passwords via the Security Center module or submit helpdesk tickets to assist with system issues.

STATUS
The web based portal is available to all 4,500+ authorized law enforcement personnel. As new applications, capabilities and policies are developed, they are added to the portal.

VISION OF END STATE
An interactive training page is being developed to allow ARJIS users to sign up for trainings on regional systems as well as a forum for users to communicate about the various systems. Completing the implementation of 'single sign on' to all ARJIS applications via the ARJIS Security Center, along with federated identity management for all other public safety applications, will eliminate the need for multiple logons and passwords.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Law Enforcement Coordination Center (LECC) Cyber Security

OVERVIEW
The San Diego Law Enforcement Coordination Center (LECC) maintains a Cyber Unit which provides unique cyber programs for various Federal, State, Local Law Enforcement agencies as well as regional partners. These cyber programs have been carefully created to benefit regional partners by providing:

- Intelligence
- Awareness
- Training
- Incident Response
- Information Sharing
- Special Programs
- Regional Cyber Leadership and Outreach

STATUS
Intelligence
The LECC is a leader in the cyber intelligence community and has closely worked with organizations such as FBI, DHS, US-CERT, MS-ISAC, the State Threat Assessment System (STAS) and various national Fusion Center partners to produce several joint cyber products. The LECC has provided the region 16 unique Cyber Intelligence Products, with various partners such as FBI, DHS Computer Emergency Response Team (US-CERT), MS-ISAC as well as various "pass through" products from several partners.

The regional impact of LECC Cyber Intelligence Products and "pass-through" products has been instrumental in situational awareness, hardening network security posture and remediation and mitigation of malicious activity. Since October 2014 to December 2015 the LECC has provided cyber intelligence products to cyber partners, but also specific San Diego municipalities requesting intelligence on topics such as APT, Crypto-Wall/Crypto-Locker, Phishing, Vshing, DDoD, DOXing, Email compromise, DHS Blacklist IP addresses to assist their internal remediation attempts.

Awareness and Training
The LECC Cyber Unit provides cyber awareness and training to private sector partners through its involvement with the FBI's InfraGard program. The LECC maintains the active role as IT Sector Co. Chief. The program reaches out to provide public and private sector partners responsible for security and emergency management with an awareness of threats to critical infrastructure such as terrorism, espionage, cyber-attacks, and natural disasters through the Infrastructure Liaison Officer (ILO) program. The LECC provides assistance for the ILO program by creating, updating and teaching the Cyber curriculum. Since October 2014 to December 2015 LECC has provided the Cyber Curriculum for three ILO

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

classes equating to three plus hours of cyber training to over 81 private partners throughout San Diego and Imperial Valley regions.

Incident Response

The LECC Cyber Intelligence Unit is assisting the Governor's Office of Emergency Services to establish the California Cyber Security Integration Center (CAL-CSIC) which will be responsible for strengthening the state's cybersecurity strategy and improving interagency, cross sector coordination to reduce the likelihood and severity of cyber-attacks. The CAL-CSIC will also be a multi-agency cyber incident response team to serve as the state's primary unit to lead cyber threat detection, reporting and response in coordination with public and private entities across the state.

The Cyber Intelligence Unit is the Cyber Disruption Response Team (CDRT) lead, the focal point for coordination for all matters concerning the response to cyber disasters for the entire San Diego County area. This position is in response to a newly created annex to the Unified San Diego County Emergency Services Operational Area Emergency Plan. The Cyber Intelligence Unit is working closely with the San Diego County Office of Emergency Services (OES) to construct the Cyber Disruption Response Planning Annex, hand select participating members and act as the team lead/coordinating body during the event of a cyber-disaster.

The recent success of the LECC's Cyber Intelligence Unit as the CDRT Team Lead was highlighted during the May 2015 SD County OES Cyber exercise where, LECC Cyber Intelligence Unit lead a diverse team of 25 cyber professionals ranging from Federal, State and Local Law Enforcement and various Public/Private sector partners. This event highlighted the SD County's ability to mitigate a 12 hour cyber disaster scenario.

The LECC's partnership/leadership provided to SD County Office of Emergency Services through the LECC's Cyber Intelligence Unit's participation provided keen insight on situational awareness, intelligence dissemination, analytic troubleshooting, technical review and suggestions for consideration during a malicious attack, as well as the ability to triage and escalate malicious cyber activity to the proper federal channels and outreach.

Information Sharing

The LECC's Cyber Intelligence Unit maintains a position as a Co-Chair on the Information Sharing subcommittee of the California Cyber Security Taskforce, a program created in 2013 and pioneered by California's Governor's Office of Emergency Services (CALOES) to develop a Cyber Incident Response Plan for the state of California.

With the new amendment of Assembly Bill No. 1172, as it pertains to cyber security, which was effective January 1, 2016, the existence of the California Cyber Security Task Force is continued while granting the

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Task Force the responsibility to complete/issue a report of policy recommendations to the Governor's office and the Legislature on an annual basis.

The Cyber Intelligence Unit has afforded regional partners with actionable and timely intelligence which is verified and reported to the State Threat Assessment System (STAS) to improve visibility and increase situational awareness for our region concerning various cyber topics; the STAS is the collection of six California fusion centers who all participate with cyber awareness in our respective areas of responsibility (AOR) as it concerns cyber events, awareness and remediation discussions.

The LECC Cyber Intelligence Unit maintains the role of the Western Regional Coordinator for the Cyber Threat Intelligence (CTI) subcommittee for the National Fusion Center Association and is leveraged as an information pool of cyber analysts from around the United States during major incidences to assist in the mitigation of current cyber issues.

The LECC facilitates the outreach to private sector partners via the Cyber Intelligence Unit's role as the IT Sector Chief of the San Diego Chapter of InfraGard. The program reaches out to provide public and private sector partners who have undergone a FBI back ground check and are responsible for security and emergency management with an awareness of threats to critical infrastructure such as terrorism, espionage, cyber-attacks, and natural disasters.

Special Programs

Detect and Deter (DND) is a joint cyber security program between the LECC and the San Diego Federal Bureau of Investigation (FBI) created in 2013. The primary goal of the DND program is to enhance the information security posture of the program's participants by detecting indicators of malicious activities on the participants' networks, and to provide timely feedback regarding indicators of malicious activity found on those networks so as to deter further activity.

The DND program maintains over 20 regional partners and performs a log analysis quarterly. As of October 2014 to December 2015 the DND program has uncovered three major APT compromises of "highly valued" participating partners and provides considerations for remediation. This program provides benefit back to SDUA by providing the access to classified indicators (IP addresses and DNS addresses) and identifies anomalies which may require federal assistance.

The LECC has recently increased responsibility and commitment to the DND program by assisting FBI Computer Scientist with the parsing (reorganization) of data files and database correlation of log files (which requires LECC access to FBINET) at San Diego FBI's main office.

The Threat Analytic Platform (previously Automated Threat Information Exchange, ATIX) is a California statewide UASI funded program, created to deliver timely and actionable cyber intelligence for the state of

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

California, through the implementation of network monitoring devices (IPS/IDS) which have the ability to inspect malware in a "detonation chamber" to ascertain intelligence data on the malware and their origin.

The LECC and State Threat Assessment System (STAS), through the TAP project, have been provided FireEye hardware and software network appliances for various cyber sensitive locations throughout the state of California. The hardware and software network appliances assist the San Diego county area and the state of California with malware identification, malicious traffic prevention and actionable intelligence, identifying and highlighting potential Indicators of Compromise (IOCs).

The hardware and software appliances collect non-personal network data, at each appliance location and provide those details to a state wide dashboard. The aggregated indicators for the San Diego area partners and those partners located throughout California provide a state wide "landscape picture" of malicious traffic and potential malicious campaigns. The aggregated data will be utilized as actionable intelligence and distributed through products to better provide situational awareness and network security posture for the LECC and San Diego/ Imperial Valley areas as well as provide a threat landscape for the State of California. These hardware and software appliances are provided to select SDLECC partners at no cost.

As of December 2015, the LECC, through the collection of malicious traffic from various TAP appliances has detected over 100 variants of malicious content and has assisted with the remediation of major network infections requiring Incident Response for TAP partner's compromised with Cryptowall 4.0.

The LECC Cyber Intelligence Unit has recently purchased Rapid 7 Vulnerability Assessment software to perform Vulnerability Assessment for select regional partners. The LECC's Cyber Intelligence Unit is attempting to reduce regional cost associated with vulnerability assessments which can exceed 5-10K per assessment (cost can vary greatly depending upon the size of the network); five regional partners have requested LECC assistance with assessments and various regional partners have expressed interest in this service.

It is important to note, as of Jan 1, 2016, Assembly Bill 670 will:

"Impose a duty on the office to require it to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office at least once every 2 years and would maintain the requirement that the state agency, department, or office being assessed fund the costs of the independent security assessment."

<u>Cyber Tabletop and Cyber Training Exercises</u>
As of December 2015, the LECC has participated in SD County Office of Emergency Services (OES) Cyber Exercise; DHS Cyber Guard 2015 Prelude; FEMA/Sempra Cyber Exercise GridEX III; InfraGard Cyber Tabletop Exercise; InfraGard Red teaming Cyber Tabletop.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

VISION OF END STATE
The SDUA should continue to develop their capabilities in the cyber security environment. The nature of this necessary capability, suggests the need for a more robust set of resources to support the SDUA.

San Diego Regional Public Safety Geodatabase

OVERVIEW
The Regional Public Safety Geodatabase (RPSG) project was established to solve traditional regional interoperability issues. The project began as a fire service driven initiative to standardize map features, attributes and symbology, resulting in the development of a common-use geospatial language for emergency responders. Prior to the project, most fire agencies had hard copy, run books and dispatch systems that stopped at their jurisdictional or district boundaries. Each agency used a different set of symbols to represent features on their map pages.

Over the last few years, significant effort has been put forth to identify opportunities to share the resource capabilities with law enforcement and emergency management stakeholders.

Over time the objectives for the RPSG have grown and been further refined. The key components of the RPSG are:

- A regional data schema for public safety geospatial data has been developed and implemented including data such as streets, addressing, routing, preplan templates and map books.
- A centralized server infrastructure to support the SDUA.
- Digital Target Hazard Preplans (Fire Preplans) in a common, regional template format.
- Wildland Urban Interface Fire Emergency Response Plans in a common, regional template format.
- System security enhancements.
- Participation in regional acquisition of aerial imagery.
- Geodatabase synchronization with SanGIS.
- Common Operating Data Services that are interoperable and can be easily shared as a single source of information.
- SanMAPS Group Implemented ArcGIS Online tool to create a GIS data sharing group

STATUS
Efforts are on-going with the Unified Disaster Council Advisory Committee, GIS Steering Committee and Regional GIS Working Group to develop policy, make funding decisions, develop strategic plans, continue to refine the designs of regional symbology, digital target hazard pre-plan templates and reports as well as wildland/urban interface emergency response plan templates and reports. These bodies meet on a monthly basis. The GIS Steering Committee is comprised of one GIS, technical and operations representative from

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

each of the four zones. The Regional GIS Working group is open to any interested party that would like to help develop regional standards.

Regional Database
A regional data schema for public safety geospatial data has been developed and implemented. This includes data such as streets, addressing, routing, preplan templates and map books. Procedures have been developed for quality assurance.

Centralized server infrastructure to support the SDUA
Implemented a GIS server at the City of Chula Vista and deployed an Amazon Web Services instance of the GIS software and services.
Digital Target Hazard Preplans (Fire Preplans)
The SDUA has completed 2,500 digital target hazard plans, also referred to as fire preplans.

Wildland Urban Interface Fire Emergency Response Plans
Several agencies within the SDUA have developed WUI Emergency Response Plans. These plans reside on local computers or in hard copy versions in command vehicles or with local first responders. Funding has been allocated to develop a standard GIS data model for the WUI Emergency Response Plans. This will provide a standard template for all agencies to develop plans that can be stored in the San Diego Regional Public Safety Geodatabase. After a regional standard has been developed for the WUI Emergency Response Plans, the required information will be collected by a SME and placed into the San Diego Regional Public Safety Geodatabase. Storing these plans in the regional database will allow opportunities to distribute the plans and make them available to all public safety agencies in real time during emergencies. A total of 70 high priority plans have been completed.

System Security
An Enterprise GIS Security Architecture Workshop for the RPSG was held in October 2015. The review was conducted by Esri Professional Services and included security best practice guidance, ArcGIS architecture recommendations as well as identifying current security risks, requirements and constraints. The primary goal of the security review was to improve the security posture of the existing GIS and determine architecture to securely support future use cases within RPSG. In addition, a security roadmap was developed to ensure efforts are prioritized to efficiently manage overall security risk.

Aerial imagery
In 2012 and 2014, SDUA in collaboration with United States Geologic Services, San Diego Association of Governments, SanGIS and other local governments partnered to purchase aerial imagery for the region. The region should continue to pursue this type of collaborative effort that reduces the cost for aerial imagery for all parties.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Geodatabase analysis and synchronization with SanGIS
An analysis of the differences between the RPSG and SanGIS has been completed to identify areas to be addressed. A working group has been established to review the differences and to make policy decisions on how to handle those differences. After those policy decisions have been made, an effort to modify the data will be undertaken.

Common Operating Data Services
Multiple services have been developed, are interoperable and can be easily shared as a single source of information to support situational awareness for EOC's and DOC's.

SanMAPS Group
Implemented ArcGIS Online tool to create a GIS data sharing group

VISION OF END STATE
All public safety agencies will need to continue to develop their GIS capabilities. Many of these GIS capabilities and needs are shared across multiple jurisdictions and disciplines. The ability to have a centralized system of GIS capabilities offers a high degree of interoperability and opportunities for economies of scale to support.

There are many examples of how the regional public safety geodatabase will serve the SDUA. They include:

- Common database standard
- Centralized server for storage, access and updating
- Seamless data for map books
- Standardized format for emergency preplans
- Shared common operating data services in a secure, cloud hosted environment that all stakeholders can access.
- Shared costs for high resolution aerial imagery
- Shared costs for staffing or support services.
- Provide an option for meeting the Next Generation 911 GIS requirements.

Situational Awareness Mapping

OVERVIEW
One of the most effective tools available to support a common operating picture is the use of map viewers for situational awareness. There are many variations of map viewers available that can support a version of situational awareness. Due to the variety of map viewers available and solutions that agencies have

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

invested in, it can be difficult to narrow the options that may be used from a regional perspective. Over the last several years, as many as 10 different types of map viewers were in use by various agencies.
In 2015, the RTP tasked the RTP Program Manager with providing a Situational Awareness Map Assessment. The SDUA at that time was using a variety of tools for situational awareness mapping. One of the primary objectives of the report was to provide recommendations on where the SDUA should focus their regional efforts.

The assessment provided the following four recommendations for the SDUA:

- Continue to develop the ArcGIS Online solution for creating a shared library of common operational data.
- Continue to utilize the NICS application for tactical situational awareness.
- Develop an ArcGIS based regional situational awareness map solution to support emergency operations centers and public information sharing.
- Support a high level of collaboration between the all appropriate solutions to make sure all parties have access to common operational data.

STATUS
<u>SanMAPS -ArcGIS Online Group.</u>
The SDUA has implemented the use of the ArcGIS Online solution to create the San Diego Multiple Agency Public Safety Services (SanMAPS) Group. The ArcGIS Online solution is a cloud-based mapping platform for organizations. From anywhere on any device, web browser, or desktop application, users get access to dynamic, authoritative content to create, collaborate, catalog, and share maps, data, and applications with members of their organization, other organizations or the general public. Organizations can subscribe to this secure platform and use it to manage, create, store, and access hosted services, maps and applications.

For the purpose of supporting regional public safety stakeholders, the following key capabilities are provided in ArcGIS Online.

- Provides a cloud-based storage location that is available from any internet browser support device.
- Ability to organize map services, web maps, web mapping applications.
- Ability to create and control functional, invitational only groups for collaboration of non-public geospatial data and products.
- Ability to publish map products to the public (open url, website embed)
- Ability to serve various types of users. Includes the range from GIS professional to public viewers.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

As of June 2016, there are over 100 members in the SanMAPS Group from fire, law and emergency manager disciplines. A user guide has been developed and training sessions are being delivered during the summer of 2016.

Situational Awareness and Collaboration Tool (now SCOUT, formerly NICS).
In 2015, the State of California, Office of Emergency Services began the deployment of the NICS software 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 for small to extreme scale homeland security incidents, such natural disasters, technological hazards, intentional attacks, and human-caused emergencies.

The objective was to make the application available to State and Local government public safety agencies as a tool for situational awareness. To accomplish the objective of implementing the California hosted version, a transition working group with representation from State and Local agencies was created. This group was tasked with creating a business requirements document, a concept of operations document and user acceptance testing. The State of California also procured services for implementation and support services on a cloud hosted server.

It is anticipated that that SCOUT will be available to use for incident management in June 2016.

Situational Awareness Map for Emergency Operations Centers
For the purpose of supporting emergency operations centers, the ArcGIS software provides the highest level of interoperability, scalability, redundancy, portability and functionality. Using the ArcGIS suite of tools, a situational awareness map application was developed with emergency manager and operations staff input. This map application is called "SanMAPS EOC Incident Map Template." This template provides the SDUA emergency operations centers with a situational awareness mapping tool that is ready to use and easy to use when an event occurs.

Interoperable GIS Data
The final recommendation encourages the sharing of data with any other appropriate map viewers in use by agencies. This begins by insuring that GIS data is developed based on open geospatial standards such as what is available in the ArcGIS Online – SanMAPS library. The capability for interoperability should be further supported as a requirement for any procurement process involving geospatial capable software. This approach will allow for the continued use and collaboration with other applications, improve interoperability and ensure stakeholders are using the same information to support decision making.

This concept has been demonstrated through integration of the common operating data services with applications such as SCOUT, CalCOP, Insider and Omega Dashboard.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

VISION OF END STATE
The ability to share common operational picture intelligence or information in a situational awareness map application provides a valuable capability for decision makers. The SDUA has focused its efforts on the SCOUT application and the use of ArcGIS to create tools like the SanMAPS EOC Incident Map Template.

In order to embed these tools in the emergency management business process, ongoing training and exercises are necessary. Users are more likely to utilize the tools if they are comfortable with the tool and see the value that it provides. The goal is to have as many emergency managers using the same tools or at least have the ability to see the same information.

InSIDeR

OVERVIEW
InSIDeR, operational as of March 2015, is a geographical viewer application accessible through the secure SDLaw portal. InSIDeR is a repository of infrastructure information that can assist first responders during tactical response, crisis management, search and rescue efforts, and emergency planning. The viewer displays a digital map with facilities in San Diego County that can be selected to retrieve information that may be imperative during emergency response

InSIDeR includes the following types of products:

- Fire Preplans/Floor Plans – digitized fire preplans, digitized facility floor plans, or other types of digitized facility plans
- Virtual Walkthroughs – digital product that first responders can use to view the interior and exterior spaces of a facility using 360 degree panoramic photos and existing floor plans or fire preplans. The virtual walkthroughs are a “snapshot in time” and not a real-time product.
- SWAT Tactical Surveys – produced by law enforcement and provide information that may be needed during tactical response. Information included in the survey can include utility shutoffs, building composition, door construction, obstacles/hazards on-site, etc.
- First 30-Minute Guides – Provides information about a facility that may be needed by first responders during the initial response phase. Information includes facility contact information, gate codes or Knox box locations, max persons on-site, law enforcement initial perimeter posts, hazmat on-site, critical nodes such as utility shutoffs and electrical control rooms, and aerial maps of the facility.

InSIDeR is a regional tool that relies on several regional agencies to prioritize and collect data, ensure quality control, and maintain the database. Law enforcement participation and providing of information to

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

produce products is essential, individual facilities providing information or updated floor plans, fire agencies providing fire preplans, individual facilities providing floor plans, and SD-LECC virtual walkthrough hardware and software to produce the virtual walkthroughs. Additionally, the SD-LECC and the Sheriff's Department IT is essential for preparation and uploading of the data into SDLaw into InSIDeR. Law enforcement participation for the collection and production of products to include in InSIDeR is reliant upon grant funding.

STATUS
InSIDeR is an ongoing project to include information on infrastructure assets throughout all of San Diego County and will require continual maintenance and quality control checks as facilities and information changes.

VISION OF END STATE
The goal is to have an InSIDeR plan completed for all high priority sites in the SDUA.

Regional Public Safety Geodatabase (RPSG) Governance

OVERVIEW
RPSG began as a pilot project to develop the capability to share GIS data and services amongst multiple agencies. This effort in the beginning was largely an informal collaborative effort amongst interested stakeholders. The stakeholders created a working group and steering committee that represented the four fire zones. Each fire zone provided representatives from the operational, communications center and GIS professionals to help steer the effort.

In order to provide a sustainment for the project, a sustainment model with more formal governance needed to be identified.

STATUS
In 2015, a recommendation for the Unified Disaster Council to assume the role of the governing body was approved. The UDC was recommended as the most appropriate governing body because of its representation model (18 cities and County) and its public safety mission. As part of that recommendation, an advisory committee was established to provide recommendations to the full UDC membership. The advisory committee is represented by:

- Emergency Management

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

- Fire Operations
- Fire Communications
- Law Enforcement Operations
- Law Enforcement Communications

This advisory committee has been meeting on a regular basis to discuss important policy and funding issues such the UASI Grant investment proposal, exploration of collaboration opportunities with SANGIS, update of the Strategic Plan and options on how to provide support services in the future.

VISION OF END STATE

All public safety agencies in the SDUA will need to continue to develop their capabilities for GIS. Some of those efforts will be centered on the individual agency's needs, using their own resources. A good portion of the effort provides opportunities to leverage regional, shared efforts. The economies of scale of shared regional support make a strong case for the UDC to continue to sustain the program for shared benefit.

A significant portion of the funding for this project has come from Homeland Security grants such as UASI. As the program transitions from a capability building phase into a maintenance mode, the funding source is likely to also transition. The use of general fund monies through member assessments formula is a likely path for sustainment.

Regional CAD Interoperability Project (RCIP) Governance

OVERVIEW

The RCIP was developed through a Memorandum of Understanding (MOU) amongst the interested stakeholders in 2009. The MOU provided for representation through an Executive Committee and created a steering committee for the policy and procedure development. The agreement also provided details on future costs for maintaining.

In order to provide sustainment for the project, a sustainment model with more formal governance was necessary.

STATUS

The RCIP MOU had an expiration date of five years from when the parties signed the agreement. In 2015, a recommendation for the Unified Disaster Council to assume the role of the governing body was approved. The UDC was recommended as the most appropriate governing body because of its representation model (18 cities and County) and its public safety mission. As part of that recommendation, an advisory committee was established to provide recommendations to the full UDC membership.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Due to the bankruptcy issues of the vendor Thinkstream and a limited interest by law enforcement to utilize the RCIP capability, it has been decided that the project will remain a fire based capability for the short term. As a result of this decision, the use of the UDC as the governing body is under review. The current recommendation is for the fire communications center community to develop an MOU amongst themselves to determine how it will be sustained and governed.

VISION OF END STATE
The San Diego County Fire Chiefs – Fire Communications Section has assumed the lead in developing a plan for sustaining the capability of CAD interoperability. This capability is mission critical in how it serves the community and should continue to be sustained in one form or another. As technology evolves and CAD systems interoperability improves, there may be additional methods to maintain the capability.

3C's Public Safety Data Network Transition

OVERVIEW
The internet protocol based microwave backhaul equipment has been transferred and repurposed where possible by the City of San Diego SafetyNet and the Regional Communications System. This transition has allowed for the dissolution of the 3C's MOU.

STATUS
In 2015, the 3C's Operations Advisory Committee supported a staff recommendation to dissolve the program at the end of the MOU term scheduled for June 2016. As part of that process, it was decided that the video teleconference system would no longer be supported through the 3C's program. The capability for the system to host a network connection for the RCIP and CALID has been maintained for those two capabilities.

A plan has been developed to repurpose where possible the microwave backhaul equipment by absorbing the assets into the City of San Diego Radio System and the Regional Communications System. Portions of the equipment have reached their end of life cycle and will not be repurposed or continue to be used.

VISION OF END STATE
The 3C's program was dissolved inf June 2016. The equipment will be absorbed and repurposed where possible by the City of San Diego and the Regional Communications System.

ARJIS Acceptable Use Policies

OVERVIEW

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

As new technology such as license plate readers and facial recognition systems have been deployed, there have been public policy and privacy impact questions on appropriate use of these technologies.

STATUS
ARJIS has developed and approved regional acceptable use policies for the License Plate Reader and Facial Recognition capabilities

VISION OF END STATE
ARJIS should continue to support the regions law enforcement agencies in the development of acceptable use policies for new technologies. The development of model policies and procedures for use of new technologies on a regional basis helps create a common approach to deployment of new capabilities. This is especially important for those technologies that are deployed region wide and where agencies share responsibility for acceptable use.

Privacy Impact Assessments

OVERVIEW
Privacy impact assessments are important tools in the development of acceptable use policies and procedures.

STATUS
ARJIS has completed privacy impact assessments for technologies such as license plate readers, facial recognition and live video sharing of Metropolitan Transit Systems cameras with local law enforcement agencies.

VISION OF END STATE
Continue to complete privacy impact assessments as necessary to inform the development of acceptable use policies and procedures.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

11. Reference to San Diego Urban Area Security Strategy

Initiative 1.1 – Migration of radio systems to Project 25 Standards	
SDUA Security Strategy Objective	**Description**
4.1 – P1	Assess regional public safety communications requirements. Develop plans, requirements documents, specifications and strategy to migrate to APCO P25 voice communications throughout the region.
4.1 – E2	Increase interoperability by providing two-way access to already existing shared communications systems among agencies.
4.1 – E5	Enhance regional medical response by upgrading obsolete medical and hospital analog radios with APCO Project-25 compliant subscriber units and accessories.
4.1 – E6	Improve regional public safety communications by procuring and installing P25 infrastructure equipment and supporting transport/backhaul equipment.
4.1 – E7	Procure APCO Project-25 compliant radios and accessories for regional law enforcement and fire-rescue personnel to increase communications operability and interoperability.
4.1 – E8	Strengthen regional communications infrastructure by installing APCO Project-25 network operations center management equipment.

Initiative 1.2 – VHF Radio Infrastructure	
SDUA Security Strategy Objective	**Description**
4.1 – P6	Assess viability of additional communications sites to mitigate coverage gaps and improve regional communications interoperability.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

4.1 – E1	Improve backup systems (e.g., VHF infrastructure, cache radios, system redundancy) for tactical communications through equipment upgrading and additional investment for large regional "task forces" providing recovery assistance to disasters and other emergencies.

Initiative 1.3 – Cloud hosted video/web conference solution

SDUA Security Strategy Objective	Description
1.3 – E4	Update EOC communications equipment and technology to include video teleconferencing systems, Local Area Networks for internet access, and enhanced wireless internet access systems.

Initiative 1.4 – Regional Tactical Interoperability Communications Plan

SDUA Security Strategy Objective	Description
4.1 – P4	Regularly test and update the region's existing TIC-P to ensure that it is up-to-date and readily employable within the region during an event.

Initiative 2.1 – Regional CAD Interoperability

SDUA Security Strategy Objective	Description
4.1 – P2	Develop and introduce standards and planning requirements for data centers to share dispatch operations data to foster real-time, interoperable data communication among parties in the region.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Initiative 2.2 – Mobile Data Devices

SDUA Security Strategy Objective	Description
2.1 – E2	Develop database systems that are linked and compatible across agencies to facilitate rapid transmission and processing of pertinent information. This is will require development and implementation of data standards, agreements among agencies for information sharing, and adoption of either new interoperable systems or bolt-on measures for existing systems.
2.1 – E4	Implement back-up and redundant systems and processes for disseminating necessary information and/or intelligence among relevant parties.
2.1 – E3	Despite the inconstant linkages and compatibility between existing database systems, ensure that all future equipment and systems procured or implemented are interoperable across agencies and jurisdictions. In addition, take measures to build such interoperability onto previously existing systems.

Initiative 2.3 – ARJIS Dashboard

SDUA Security Strategy Objective	Description
2.1 – E2	Develop database systems that are linked and compatible across agencies to facilitate rapid transmission and processing of pertinent information. This is will require development and implementation of data standards, agreements among agencies for information sharing, and adoption of either new interoperable systems or bolt-on measures for existing systems.
2.1 – E4	Implement back-up and redundant systems and processes for disseminating necessary information and/or intelligence among relevant parties.
2.1 – E3	Despite the inconstant linkages and compatibility between existing database systems, ensure that all future equipment and systems procured or implemented

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

	are interoperable across agencies and jurisdictions. In addition, take measures to build such interoperability onto previously existing systems.

Initiative 2.4 – ARJIS Data Enhancements	
SDUA Security Strategy Objective	**Description**
2.1 – E3	Despite the inconstant linkages and compatibility between existing database systems, ensure that all future equipment and systems procured or implemented are interoperable across agencies and jurisdictions. In addition, take measures to build such interoperability onto previously existing systems.

Initiative 2.6 – Cyber Security	
SDUA Security Strategy Objective	**Description**
2.4 – P3	Conduct an in-depth cyber risk analysis across the region to include an asset catalogue.
2.4 – P4	Conduct an in-depth cyber capability assessment across the region.
2.4 – P5	Develop a regional cyber security/preparedness strategy
2.4 – P6	Develop an Operational Area cyber incident response plan or annex.
2.4 – O1	Develop a cyber security/preparedness working group or equivalent organization to manage the region's cyber security/preparedness program.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Initiative 2.7 – Risk Analysis Center

SDUA Security Strategy Objective	Description
2.2 – P1	Update the SDUA CIP to include current accounting of all CIKR assets, both public and private, within the region.
2.2 – P2	Within the updated CIP Plan, develop regional sector-specific plans (for all 18 sectors, or those sectors at highest risk) or annexes to the core CIP Plan. Such plans will provide additional detail to the unique characteristics and security stakeholders of each sector, as well as the corresponding framework to ensure integration of the various sector stakeholders.

Initiative 2.10 Resource and People Location Services

SDUA Security Strategy Objective	Description
1.4 – E1	Enhance interoperable resource management and tracking software in all jurisdictions. Software should include a database of resources by type and include private sector assets.
7.2 – P6	Develop processing, registration, and tracking systems for incoming evacuees to include necessary forms and materials, and trained staff.

Initiative 3.1 – Digital Target Hazards

SDUA Security Strategy Objective	Description
3.6 – P6	Continue implementation of the Digital Target Hazard Plans for the pre-incident planning and regional sharing of information.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

3.6 – E2	Develop a GIS layer depicting locations of businesses required to have hazardous materials business plans.

Initiative 3.2 – Data Synchronization between RPSG and SanGIS

SDUA Security Strategy Objective	**Description**
2.1 – P3	Introduce data standards, agreements between agencies, and an interoperable, searchable, and scalable information sharing utility such that gathered information may be organized, linked, searched, and easily retrieved across disparate agencies.

Initiative 3.3 Situational Awareness Mapping Tools

SDUA Security Strategy Objective	**Description**
1.1 – P1	Identify a geospatial solution for a regional common operating picture or decision support system to track resources, active incidents, target hazard plans, wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions
1.3 – O4	Re-establish the geospatial regional common operating picture or decision support system working group as a means to facilitate regional understanding of the system and related policy and use issues.
1.3 – E4	Acquire necessary geospatial and other equipment necessary for regional common operating picture/decision support system to track resources, active incidents, target hazard plans, wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions.
1.3 – T6	Provide training to first responders, public safety agency command staff and emergency managers on use of a geospatial regional common operating picture or decision support system to track resources, active incidents, target hazard plans,

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

	wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions.

Initiative 3.4 – SanMAPS Common Operating Data Services

SDUA Security Strategy Objective	**Description**
1.1 – P1	Identify a geospatial solution for a regional common operating picture or decision support system to track resources, active incidents, target hazard plans, wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions
1.3 – O4	Re-establish the geospatial regional common operating picture or decision support system working group as a means to facilitate regional understanding of the system and related policy and use issues.
1.3 – E4	Acquire necessary geospatial and other equipment necessary for regional common operating picture/decision support system to track resources, active incidents, target hazard plans, wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions.
1.3 – T6	Provide training to first responders, public safety agency command staff and emergency managers on use of a geospatial regional common operating picture or decision support system to track resources, active incidents, target hazard plans, wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions.

Initiative 3.5 – ARJIS GIS Services

SDUA Security Strategy Objective	**Description**

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

3.3 – P5	Acquire additional GIS technician personnel to ensure future availability, increased capacity, and the ability to provide for appropriate work/rest cycles during major incidents.
3.3 – T1	Develop a SOP to train and instruct GIS technicians regarding potential computer network conditions to ensure continual mapping support.

Initiative 3.6 – Next Generation 911 GIS Services

SDUA Security Strategy Objective	**Description**
1.1 – P1	Identify a geospatial solution for a regional common operating picture or decision support system to track resources, active incidents, target hazard plans, wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions
1.3 – E4	Acquire necessary geospatial and other equipment necessary for regional common operating picture/decision support system to track resources, active incidents, target hazard plans, wildland urban interface plans, special hazards, water supply systems, street and address information and current weather conditions.

Initiative 4.1 – GIS Program Funding and Support Services

SDUA Security Strategy Objective	**Description**
3.3 – P5	Acquire additional GIS technician personnel to ensure future availability, increased capacity, and the ability to provide for appropriate work/rest cycles during major incidents.
3.3 – T1	Develop a SOP to train and instruct GIS technicians regarding potential computer network conditions to ensure continual mapping support.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.

Initiative 4.3 – RTP Program Management	
SDUA Security Strategy Objective	**Description**
1.1 – P2	Integrate regional and state/local strategic plans with one another to facilitate cross-jurisdictional and consistent planning.
1.1 – O2	Maintain a regional advisory organization to assist in capability needs prioritization, requirement validation, and goal and objective achievement monitoring.
1.1 – O3	Maintain a support center for regional interoperability assessments to monitor individual technology projects for alignment with regional strategies, to conduct special projects as assigned, and for technology evaluation through operational testing in exercise and actual events

Initiative 4.4 – New Technology Policies and Procedures	
SDUA Security Strategy Objective	**Description**
2.1 – P5	Develop and implement content and template standards to be applied across disciplines and jurisdictions to ensure uniformity of reported information.
2.1 – P15	Data standards and systematization should be required across jurisdictions and agencies to allow for organized, linked, searchable, and easily retrievable information by all parties involved.

FOR OFFICIAL USE ONLY (FOUO)
All portions of the attached document are deemed by the City of San Diego Office of Homeland Security to be records of homeland security preparedness and are exempt from public disclosure by Section 6254(aa) of the California Government Code.