Public Safety Communications Board Meeting

Date: Wednesday, December 4, 2019
Time: 10:00 a.m.
Location: Board Room

Agenda

1) Call to Order and Introductions
2) Approval of September 25, 2019 meeting summary
3) SirenGPS/911 RTA
4) CCTA Communications Study
5) 911 Legislation Update
   • Federal
   • State
   • Local
6) Missouri 911 Service Board Report
7) Kansas 911 Coordinating Council
8) Cost Share Requests:
   • Independence
   • Cass County host move request
9) PSAP Updates:
   • Douglas County Implementation
   • Atchison County Membership
10) Public Safety Program Updates:
    • Training
    • Technical Services
    1) Router Project Update
    • Database / Mapping
11) Other Business

12) Adjournment

**Future Meeting Dates:**
- PS Communications Board @ 10:00 am in MARC Boardroom
- March 11, 2020
- July 8, 2020
- September 9, 2020
- December 16, 2020
Public Safety Communications Board Meeting
October 2, 2019
Meeting Summary

Agencies Present:
Marie Athearn, Johnson County Kansas - Emergency Communications
Anthony Avery, Platte County Sheriff’s Office
Jim Bagley, North Kansas City Police Department
Ed Brundage, Kansas City Missouri Police Department
Paul Davis, Johnson County Kansas Med Act
Mark Francisco, Kansas City Missouri Police Department
Dan Haley, Kansas City Missouri Police Department
Simon Happer, Overland Park Police Department
Steve Hoskins, Kansas City Missouri Police Department
Eric Houston, Overland Park Police Department
Jennifer Jones, Kansas City Missouri Police Department
Steven Mailand, Johnson County Kansas Sheriff’s Office
Mark Owen, Platte County Sheriff’s Office
Rance Quinn, Kansas City Kansas Police Department
Maury Thompson, Johnson County Kansas Manager’s Office
Robin Tieman, Cass County Emergency Services Board
Kris Turnbow, City of Raymore
Don Ward, Overland Park Police Department
Ellen Wernicke, Johnson County – Emergency Management and Communications

MARC Staff: Eric Winebrenner, Mike Daniels, Hassan Al-Rubaie, Hannah Ankenbauer, Saralyn Hayes, Sally McGraw, Marlene Nagel, Pam Opoka, Nikki Thomas

1. Call to Order and Introductions
Maury Thompson called the meeting to order and self-introductions were made.

Winebrenner reported that Kansas City Fire Department had announced that Donna Maize is their new Chief and Nathan Dugan would be her designee. Kansas City Kansas has an Interim Chief, Michael York and his designee will be Rance Quinn.

2. Approval of June 26, 2019 Meeting Summary

A motion was made to approve the June summary and seconded. The meeting summary was approved with no opposition.

3. 2020 Regional 911 Budget – Eric Winebrenner

- The way the budget is being presented has been changed for it fit more easily into the overall MARC budget.
The training program was moved underneath the Government Training Institute (GTI) last year as a contract. It is being moved back into this year’s Public Safety budget. Pam Opoka has been working on some online trainings. She will possibly be signing a contact with Power Phone who offers eighteen online 911 related trainings.

- **Consortium Fees** – Daniels did a study on how consortium fees are collected and how this worked with our training system. He put together some numbers on how this would look rolled into the monthly allocation fees. Those outside the MARC region would be required to pay $200 per year, per person membership fee. Wernicke asked how the cost would be allocated and Daniels said it would be based on county population. Owen felt counties would be taking an increase. Daniels explained that in his reviewing of the way funding was being handled; he learned that it would not provide the regional training funds needed in the future. Avery noted that their county does online for all disciplines and they must have a medical doctor approve everything. Daniels will review the outside training that agencies are paying for to see if that could be included and/or if our region could get a discount for having a larger group. Then, counties would not have an additional training cost.

- **911 Maintenance** – Winebrenner – The contact with Commenco increases by 18%, RAMBIS increases by 5% and Training Coordinator position has been added back into the Public Safety budget which adds 1%.

- **Capital Project**
  - **Routers** – When they are paid for and we will have $458,000 left.
  - **Workstations** - Increasing the number of workstations being replaced annually from 48 to 60 is being recommended since hard drives are only lasting about four years. Also, Windows 7 support from Microsoft expires at the end of this year and they will no longer provide software security patches. With 97% of our region’s machines on 7, it is believed that increasing the number of machines replaced each year would be the most cost-efficient way to handle this. This project would take approximately four-years to complete.
  - **Cybersecurity** – Tested this with Douglas County but now there is a need for test servers that match our environment. Once this testing is completed, it will be put on the live environment. This cost has been included in the budget.
  - **Vesta Software Support** – There is a need to extend this until some of the older workstation’s replacement project is completed. This is also included in the budget.
  - **Seculore** – This company is being recommended to contract with for cybersecurity. Going with a company that provides cybersecurity or hiring an internal person to handle this was explored and it was decided contracting with a company was the most cost-efficient. This company provides monitoring, training, policies and emergency support should we have an attack.
  - **Firewalls** - Funding for this is included in the budget. These will be installed in front of all our PSAP connections to provide more security.

> A motion was made by Kris Turnbow to approve the whole budget. It was seconded. The motion passed with one nay.

Winebrenner asked for the Board’s permission to start working with Seculore.

> A motion was made by Mark Owen to approve MARC to begin work with Seculore. It was seconded. The motion passed with no opposition.

4. **911 Legislation Update** – Eric Winebrenner

- **Federal**
  - **HR1629** bill was introduced. This bill reclassifies PSAP personnel from clerical to public safety. It has moved to the Senate.
  - **HR2760** and **HR1479** are the same bill which would provide $20 million in grant funding over a five-year period for states to modernize their 911 equipment. These are assigned to the committee but no legislation yet.

- **State**
  - **Missouri SB 291** - Signed July 9 and went into effect immediately. Winebrenner shared everything included in this bill.
  - **911 Service Board** – They voted that state charter counties would get 65% of the pre-paid paid in their counties returned to them. All other counties will get 40% back. Work is being done to get these funds sent back electronically. Counties that opted out previously will receive letters explaining the new process and offering an opportunity for them to opt in by November 19.
- **Kansas** – Passed their .90 tax.

- **Local**
  - **Jackson County** – The 911 subscriber tax will go on the ballot in August 2020. An agreement with the City of KC on the sharing of revenues and costs has to be in place before this issue is placed on the ballot.

5. **Missouri 911 Service Board – Eric Winebrenner**
   - This Board has been working and are in the process of filling positions and identifying a state 911 Director. Have discussed federal grant awards which will be administered by them and the Public Safety Board. They are awaiting final award notices before they proceed with dividing it up funding.
   - Kansas region’s intentions to apply for state funding for their microwave overlay project. There is a 40% match which is of concern on how the smaller counties would be able to do the match.
   - Regional Coordination Centers are set. This will be voted on at the Missouri Public Safety Conference in October.

6. **Kansas 911 Coordinating Council - Eric Winebrenner**
   - There has been contact with this council about their grant. The intent is to also apply for funding as a region for our microwave overlay project. Wernicke shared that it was her believe that both the region and Kansas entities could both apply. Winebrenner noted that this was also his belief.

7. **RAMBIS – Hassan Al-Rubaie**
   - **Radio use** – Al-Rubaie shared background information on RAMBIS. There is a pending upgrade for Motorola radio systems that is not believed to be a good use of funds. It is being recommended that MARC Public Safety no longer be responsible the voice radio channels on RAMBIS. Cannot turn RAMBIS totally off since there are 3 entities using NPSPAC channels in their radios. Robin Tieman suggested having the three that are using the NPSPAC channels meet and create a plan before an actual cutoff date is set. Steve Hoskins added that the recommendation from the Users Board meeting was for RAMBIS to be moved underneath the MARRS committee. Daniels shared that what happened with the Users meeting motions was a little confusing. He believes the intent of the Users committee was to have the Board decide if the voice decisions related to RAMBIS should be moved to the MARRS Management Council and let the Council come up with a plan for the RAMBIS radio side. This will be tabled until the three entities have meet and bring back their thoughts on this item.

   - **Continued maintenance requirements**

8. **Cost Share Requests - Eric Winebrenner**
   - **Independence** - Work is still being done on identifying a third position that could be relocated to Independence.
   - **Cass County** – Two positions have been ordered. An additional request to move a PSAP from one host to another was received. The cost for this will be worked up and shared at the next committee meeting.

9. **PSAP Updates – Hassan Al-Rubaie**
   - **Douglas County Implementation** – Work on both Douglas County and KU is moving forward.
   - **Atchison County Membership** – Circuits were started last week on Kansas City side and should be finished today. On Atchison side, AT&T is projecting they will not be completed until late November. So, Atchison may not join the system until after the first of the year.
   - **Kansas City Kansas Fire and Police departments have been upgraded to Vesta.**
   - **Vesta upgrades are complete and hardware upgrades will start next year.**

10. **Public Safety Program Updates**
    - **Training - Pam Opoka**
      - A training advisory committee was established with one representative from each of the regional counties. This committee is assisting in the development of the 2020 training curriculum which is set up in four tracks (Fire/EMS, Police, Wellness & combined). Also, 18 online trainings will be rolled out next year.
      - Peer Support was recognized at NENA as a national model for their Peer Support policies. They were also asked to attend the Standards of Best Practices conference in January as panel experts to assist that wellness workgroup with their peer support piece.
The Commander Peer Support team will be turned over to the commander co-chairs with Opoka serving as a consultant.

**Technical services – Hassan Al-Rubaie**
- **Router Project Update** – This project is moving forward, and routers are expected in six weeks. A Vesta upgrade was done, and he shared what would be seen on the consoles. Reports have been received regarding a change in the emergency and waiting callback functions. This will be reviewed.
- **Accidental Calls** – Crash calls or Vehicle assist system issues have been reported. MARC staff reached out to Ford Assist and are working on changes they suggested. Please contact MARC with any issues you may have by calling or emailing 911techs@marc.org if it is not urgent. Providing the date/time would be very helpful when researching issues.
- **Microwave** – Have a new microwave link. Some of the T-1 links are being monitored for timing issues. There is an antenna that needs a new cover. Received a request from Lee’s Summit Police for 10 megs of bandwidth.

**Database / Mapping – Saralyn Hayes**
- In the next couple of weeks, dispatchers will see another layer on their maps which will be the hazardous materials or Tier II data. There will be two categories 1) extreme hazardous substances (EHS) and 2) risk management plan (RMP) sites. Opoka and Hayes are working on a mapping component that will be on the 911 Intranet.
- Maria Walser from MARC’s database team conducted a wireless side audit with Sprint and found 8900 mini site cells. These cells were previously using data and was changed over to voice without any notification to MARC. Hayes noted that some 911 wireless calls will show “ON POLE” or “ON UTILITY POLE” as part of the ANI/ALI display. Information on this was sent out in yesterday’s ***Training Tip Tuesday***.
- Keri’s Law was signed previously but does not go into effect until February 2020. This is where on a multi-line telephone system you will no longer be required to dial a digit for an outside line when calling 911. There have been questions regarding what is needed for this change. So, a page is being developed on the MARC website that will provide what you need to do/what are requirements and how this will work. MARC’s Public Affairs staff will be sending out information regarding this change/requirement to businesses, hospitals, schools, Chamber of Commerce, etc.

11. **SirenGPS - Eric Winebrenner**
- Winebrenner shared background information on a map that MARC Research Services created. He then, turned the floor over to Paul Bushore, MARC Research Services. Bushore shared a PowerPoint map that was built using 911 monthly call data. He noted that other feeds could be added that would show a dashboard of calls within a timeframe such as weather issues.

Winebrenner said that SirenGPS is a company working on 911 analytics. They have partnered with a couple of small entities to test their product. Winebrenner explained how SirenGPS works. Now, SirenGPS is needing live call data from a larger entity to move on with their concept and have asked if our region would be willing to provide this information. If our region is agreeable, we would receive information for free, but they would sell the product to companies or property owners alerting them to 911 calls pertaining to their property. SirenGPS also has the capability to link to CAD data which would allow individual PSAPs to be able to work with them. Any information our region provided would not be sold, without the written permission of the individual jurisdiction. There was much discussion around this and if it was legal. Al-Rubaie shared that if it was our quest or desire to receive notification, we would have to go with a system like SirenGPS.

A motion was made by Mark Owen to table this discussion until a legal opinion had been received. This was seconded by Robin Tieman and passed without opposition.

12. **Budget update and Outreach report – Mike Daniels**
- A copy of the budget was included in the meeting packets. Daniels reported that what had been collected was spent.
- **Outreach** – Supported several community events with materials. MARC has quite a few Important Tips brochures in English and will have Spanish ones in a couple of weeks. Anyone needing either should contact MARC.
• **911 Day at the “K”** – Over 300 telecommunicators and their family members attending this event.
• **Telecommunicators Appreciation Celebration (TAC) 2020** - Have entered into a contract with the InterContinental Hotel on the Plaza for next year’s event.
• **Cell Phone Sally Program** - Daniels reminded everyone about this program and would be appreciated if those in attendance could get their staff to assist with this program.
• **911 Hero** – He reminded everyone not forget to fill out the form and notify MARC when they received a call from someone deserving of this honor.
• **PSAP Manager’s Orientation** – The next one is scheduled at MARC tomorrow at 1:00 p.m.

13. **Other Business**

   • Mark Whelan’s retirement and a reception is planned for him tomorrow.
   • Rance Quinn shared that when they were at Johnson County there were not nearly enough 911 positions available to handle their Kansas City Kansas (KCK) callers. He asked what needed to be done to get more positions at Johnson County since they are KCK’s backup facility? Al-Rubaie share that Johnson County would need to do a cost-share request for more positions. Hoskins said that Kansa City Missouri had also ran into this issue and this may need to be reviewed for their department as well.

14. **Adjournment**

   With no further discussion, the meeting was adjourned.
**Information from 911 Calls Released to Certain Third Parties and Impact of Missouri Sunshine Law and Kansas Open Records Act:**

Does Missouri or Kansas law prevent MARC from releasing or allowing monitoring of 911 call data by third parties, for the purpose of providing property owners within a certain jurisdiction of incidents occurring on their property, when such property owners will only be informed of limited information from the 911 call data pertaining to incidents, specifically time, location, phone number of contacting party and the nature of the incident? No names of victims or persons involved in the incident will be provided.

- The short answer is, in most cases, no. Both Missouri and Kansas have laws that encourage transparency and the release of public records and the information being released should not divulge protected information and is being released to property owners directly affected by the incidents being reported, so that such property owners can respond and provide information to occupants at the affected properties, all for the safety of persons affected or nearby the reported incidents. The relevant provisions of the Missouri and Kansas laws are discussed below.

- **Missouri.** RSMo §§610.010, 610.100 and 610.150 set forth the relevant portions of Missouri's open records act, referred to below as "Missouri's Sunshine Law". Although no definite determination has been reached by a court under Missouri's Sunshine Law, MARC is likely a “quasi-public governmental body” as defined at RSMo §610.010(f) due to MARC's close relationship with local public governmental bodies.

The next question is what, if any, of the 911 data are accessible to the public. We believe that the data acquired by MARC and the public governmental bodies from the 911 call monitoring that is proposed to be shared with affected property owners is within the definition of a "public record" and open to the public in Missouri.

The following language in Missouri's Sunshine Laws is instructive:

- RSMo §610.100.1(4): defines an "Incident report": "a record of a law enforcement agency consisting of the date, time, specific location, name of the victim and immediate facts and circumstances surrounding the initial report of a crime or incident, including any logs of reported crimes, accidents and complaints maintained by that agency." Each law enforcement agency within Missouri is to maintain records of all incidents reported to the agency, investigations and arrests made by such law enforcement agency, and all incident reports are open records. See RSMo §610.100.2(1).

- While RSMo §610.150 states that information acquired by law enforcement agencies or first responder agencies by way of 911 reports are to be inaccessible to the general public, that section further states that information consisting of the date, time, specific location and immediate facts and circumstances surrounding the initial report of the crime or incident shall be considered to be an incident report and thus an open record under the sections discussed in the prior bullet.

We believe that the information acquired from 911 call monitoring that is to be released to, or monitored by, third parties for the purpose of providing information to affected property owners of the time, location, phone number of contacting party and the nature of the incident, to be within the definition of an "incident report" under Missouri's Sunshine Law. Further, we understand that such information is only being made available to affected property owners for the limited purposes stated above, i.e., so that such property owners can respond
and provide information to occupants at the affected properties, for the safety of the persons affected or persons nearby the reported incidents. If sharing of 911 call information is to be made with other persons or for other purposes, please let us know, as our view could change.

• **Kansas.** The Kansas Open Records Act (the "Act") defines "public record" broadly, as recorded information made, maintained or kept by a "public agency" (which likely includes MARC) and the Act sets forth numerous exceptions to the general rule that public records are to be open for inspection and copying. The relevant exceptions include: medical treatment records; records closed by rules of evidence; criminal investigation records; certain correspondence between a public agency and a private person; public records containing personal information that would clearly constitute an unwarranted invasion of personal privacy; and information that would reveal contact information about an alleged victim of stalking, domestic violence or sexual assault. See KSA §45-221(a) and the numerous subsections therein. The Kansas Attorney General has issued opinions on numerous occasions that the front page of a Kansas standard offense report is considered an open public record, with exceptions for information that could be redacted or otherwise not disclosed (such as information constituting an unwarranted invasion of personal privacy such as victim specific information in a sex offense or addresses of victims when the victim is placed in danger due to disclosure. See KS AG Opinion Nos. 87-25, 92-149 and 98-38 as examples). Social security numbers cannot be disclosed as part of an open record in Kansas, unless federal law requires disclosure. See KSA §75-3520(a)(1) (subject to exceptions listed in the statute). As long as the information gathered in a 911 call and made available to affected property owners is limited to time, location, phone number of the caller and the nature of the incident, so that the affected property owners can respond and provide information to occupants at the affected properties, such disclosures should be permitted under the Act. Just as in Missouri, we are assuming that no names of victims or persons involved in the incident will be provided.

Please let us know if our assumptions are incorrect or if the nature of the information shared changes, as our view could change.

Is there liability for any jurisdiction related to the release or monitoring of 911 call data to some but not all stakeholders?

• No, there is clear precedent from the Supreme Court of the United States that supports public safety agencies decision making related operational policy. Agencies can decide to give information to some stakeholders and not provide information to others for operational needs. *Town of Castle Rock, Colorado v. Gonzales*

Other Questions you might have:

1. What is unique about 911 RTA?
   • 911 RTA uses artificial intelligence to identify large-scale emergency incidents in real time using automated algorithmic analysis research using the location, proximity and frequency of 911 calls from previous active shooter incidents. 911 RTA software can automatically detect a likely large-scale emergency and generate an incident indication 4X faster than dispatch. This service can identify a potential mass casualty incident and send a notification to leadership and special weapons and tactical up to 50X faster than without automation. SirenGPS has been researching and developing this technology since 2012 and holds several patents related to using an analytic process to identify mass casualty incidents.

2. Who are 911 RTA community stakeholder subscribers?
   • SirenGPS is making 911 RTA notifications available as a subscription service to appropriate security and leadership at schools, businesses and places of worship in communities where public safety authorizes distribution of incident notifications. Subscribers can only receive notifications for incidents that impact property they own, control or protect. Revenue generated from subscriptions to community stakeholders makes it possible for SirenGPS to offer the service to public safety without charge.
3. What notifications does 911 RTA distribute and who can receive them?
   • 911 RTA distributes incident notifications when the software identifies a potential large-scale emergency and from dispatcher 911 incident codes. 911 RTA incident notifications provide a description of the nature of the incident and a location for the incident. These notifications are delivered via text, email and/or automated call. Public safety agencies manage 911 RTA recipient lists to send notifications to leadership and appropriate first responders associated with agencies within the same political subdivision, and their mutual aid partners. Where authorized, community stakeholders such as security at a business, school or hospital can subscribe to the service to receive incident notifications for matters that directly impact property they own, control or provide security. Community stakeholder notifications include a timestamp of the 911 call, location of where the call was placed, and incident code where applicable.

4. How does 911 RTA software identify large-scale emergency incidents?
   • 911 RTA software monitors the location, proximity, frequency, and related meta-data for 911 calls to identify potential large-scale emergency incidents in real-time. An algorithmic model has proven to reliably identify active shooter incidents from frequency, location and proximity of 911 calls without access to other information. SirenGPS is working with artificial intelligence and data scientists at St Louis University and the University of Notre Dame to expand 911 RTA’s ability to automatically identify significant emergency incidents.

5. How does 911 RTA protect first responders and the agencies they work for?
   • We appreciate that agencies want to do everything possible to keep first responders safe and limit risks to their agencies -- and we do too. SirenGPS has written our commitment to protecting our public safety partners into the 911 RTA terms and conditions:
     a. 911 RTA alerts are only available to approved commercial stakeholders and only for incidents that impact premises they own, control or provide with security.
     b. Public Safety agencies may restrict distribution of 911 RTA notifications to stakeholders and terminate a subscriber at their discretion.
     c. Public Safety agencies have sole discretion to decide what incident codes, if any, may be sent to stakeholder subscribers.
     d. Public Safety agencies can deny and/or delay 911 RTA notifications to stakeholder subscribers for specific incident types.
     e. Stakeholder subscription agreements include a release of liability for public safety agencies that use 911 RTA.

6. How does 911 RTA decrease the risk of litigation for public safety agencies?
   • Public safety agencies provide most of their services to entities and individuals without any agreement in place that allocates risk. 911 RTA creates an opportunity for public safety entities to benefit from an agreement with community stakeholders that includes a waiver related to requests for emergency information and services.

7. 911 RTA would put more information out in the community about emergency response times. Could this increase the frequency of claims related to response times?
   • There is strong legal precedent supporting public safety agency prerogative to make operational decisions – including even the decision not to respond to 911 calls. This precedent makes claims related to emergency response times unlikely. Because the 911 RTA subscriber agreement includes a waiver that addresses claims related to emergency information and response, the risk of lawsuits filed by subscribers is essentially zero. Moreover, public safety agencies that routinely publish 911 call information report no increase in claim activity. Starting in 2015 law enforcement agencies began participating in the Police Data Initiative, a research collaboration that encourages agencies to publish 911 call information as well as other information about crime and requests for service in cooperation with the United States Department of Justice and various research interests. More than 200 participating agencies regularly publish information and statistics about crime and emergency service requests in their communities. Dozens of cities publish relatively complete 911 call emergency service request
information to public websites daily. The most commonly reported impact on participating agencies is a reduction in the effort required to respond to open records requests.

8. Are public safety agencies that use 911 RTA required to make the service available to every stakeholder?
   - There is clear precedent from the Supreme Court of the United States that supports a public safety agency offering 911 RTA to some community stakeholders and not to others. See Town of Castle Rock, Colorado v. Gonzales, 545 U.S. 748 (2005).

9. Is there a risk of claims that personal information has been exposed?
   - 911 RTA notifications distribute information about incidents, not calls, and the service doesn’t capture any Personally Identifiable information (PII). PII is typically understood to include date of birth, social security number, financial institution account numbers, health information, and other information subject to special protection by law. 911 RTA does not collect any PII. The only information that 911 RTA collects that can reasonably identify an individual is a caller’s telephone number. While telephone numbers do not qualify as Personally Identifiable Information, SirenGPS treats phone numbers as if they were sensitive, personal information. 911 RTA only uses phone numbers to validate data. Phone numbers are never shared with subscribing stakeholders and are encrypted at all times. 911 RTA meets or exceeds all data security requirements in states that have passed regulations prohibiting revealing the identity of 911 callers.

10. Is there insurance for a data breach?
   - While we believe exposure is essentially theoretical, SirenGPS maintains $1M insurance coverage for the benefit of our clients related to 911 RTA data breach. How does 911 RTA protect PSAP data and systems? 911 RTA is fully encrypted and designed to exceed NIST 800-171 security standards. 911 RTA does not monitor agency communications and does not expose any protected information. 911 RTA can only be configured through a direct connection and can only accept authorized communications.

Respectfully,

Michael Daniels
Public Safety Communications
Planning and Administrative Manager
Eric Winebrenner  
Public Safety Program Director  
Mid-America Regional Council  
600 Broadway, Suite 200  
Kansas City, MO 64105-1659

Dear Eric,

Thank you for taking the time to discuss 911 Real-Time Analytics (911 RTA) for the MARC and its partner agencies. Agencies can be confident that 911 RTA will deliver significant benefit, reduce risk, and won’t compromise sensitive information or technology. Recognizing the importance of a strong partnership with public safety, SirenGPS makes the following commitments related to the implementation of 911 RTA:

1. **SirenGPS will not share 911 call information or use that information to send incident notifications without authorization from the agency that “owns” that information.** Unless we have authorization (or are subject to a court order) SirenGPS won’t share 911 call information collected from MARC except with MARC, MARC public safety agency partners, and academic and/or government research partners approved by MARC.

2. **911 RTA public safety agency partners will retain authority over their 911 information.** Distribution of 911 RTA incident notifications to stakeholders must be authorized by the MARC public safety agency partner responsible for the geographic area where the incident(s) occurs (see #3 below). Agencies may later withdraw their authorization.

3. **When an agency authorizes distribution of incident notifications for community stakeholders, that agency retains authority over incident notifications.**
   - 911 RTA stakeholders may only subscribe to receive notifications for incidents that impact or originate from a commercial or public property that the subscriber owns, controls, or for which the subscriber provides professional security services.
   - MARC public safety agency partners will receive quarterly reports of 911 RTA subscribers with property located within the partner agency’s geographic area.
   - 911 RTA stakeholder subscription agreements include a waiver that extends to MARC and MARC agency partners for claims related to the service, and for 911 RTA subscription payments in the event that an agency withdraws authorization.
   - 911 RTA stakeholder subscription agreements require non-disclosure to keep incident information in confidence except by court order.

These commitments are written into our terms and conditions, available for download from https://sirengps.com/misc/contract-documents. We also include an FAQ that provides references to each of these commitments in the 911 RTA terms and conditions.

Thank you for your consideration,

Paul Rauner
SirenGPS, Inc.
9-1-1 Real-Time Analytics Support Proposal for MARC

Overview

MARC is evaluating a new innovative real-time 9-1-1 analytics solution from SirenGPS. For analytics to be computed, the SirenGPS system needs a real-time feed of all 9-1-1 call locations as they are received at PSAPs across the MARC region. Sources of 9-1-1 call location include 9-1-1 Automatic Location Information (ALI) and supplemental Device Based Hybrid Location (DBHL) received from an external clearinghouse such as RapidSOS. The 9-1-1 ALI interfaces at MARC are complex, as there are three host sites each containing A and B sides and each side containing multi-port ALI controllers. MARC PSAPs currently utilize a GeoComm web browser based PSAP mapping application hosted within this environment. The GeoComm mapping system is already connected to this complex ALI environment, as well as to RapidSOS, and thus provides a good mechanism for concentrating 9-1-1 call location information to a single location and brokering real-time messaging to the SirenGPS analytics appliance. This approach also minimizes risks and eliminate costs associated with deploying and connecting new interfaces directly to the ALI controllers. To support MARCs investigations into real-time 9-1-1 call location analytics with SirenGPS, GeoComm proposes to implement a 9-1-1 call location interface between the GeoComm and SirenGPS systems for no cost to MARC.

Proposed Approach

The GeoComm system deployed at MARC includes “ALI Connect” software from GeoComm. Each port on each ALI controller is connected to an “ALI Connect” instance. “ALI Connect” sends received call location data to a GeoComm Mapping System API that is used by the internally hosted GeoComm web browser based PSAP mapping application. The GeoComm “ALI Connect” software can POST call location data to multiple REST endpoints. To achieve the desired region-wide call location data centralization, GeoComm proposes to configure each “ALI Connect” at each host site with an additional REST endpoint to POST received 9-1-1 call location data to. GeoComm will provide a new API that can be deployed to a new server or PC at each host site. The new API will receive 9-1-1 call location data from the “ALI Connects”, augment with additional DBHL data from RapidSOS, and send the resultant event and location information to the SirenGPS appliance via the SirenGPS PGA Incident Message API. A summary of the proposed approach is:

- MARC would deploy a new Microsoft Windows server at each of the three host sites (one server per site). For networking, each of the new servers needs to connect to the “ALI Connects” at its host site as well as to the SirenGPS analytics appliance, which presumably may be at a different physical location in the network. In addition, each of the new servers will require an Internet connection in order to query the RapidSOS clearinghouse. The new servers and networking would be a MARC responsibility. Server compute and storage capacity requirements will be
minimal as the GeoComm software running on these servers is only brokering messages between systems and not storing data or performing analytical operations.

- The GeoComm Support Team will remotely configure each “ALI connect” with an additional new REST endpoint to send caller location data to. As this operation touches the live 9-1-1 call mapping system, GeoComm will utilize the standard Change Control process in place between GeoComm and MARC to plan and execute the configuration change.

- The GeoComm Innovation Team will develop, deploy and support a new GeoComm API hosted on each of the three new servers for concentrating ALI from the “ALI connects” at each host site, augmenting with DBHL from RapidSOS, and sending data to the SirenGPS PGA Incident Message API. GeoComm application installation and configuration will be accomplished by remote connection to each of the three new servers.

- SirenGPS will deploy, test and support integration of its communication gateway appliance with GeoComm’s “ALI connects” service. SirenGPS has agreed to provide this service at no cost to MARC and the Kansas City Police Department in order to facilitate initial deployment of the service as part of a research proposal co-sponsored by the University of Notre Dame. The integration to be implemented as described in this proposal in accordance with the following documentation submitted with this proposal:

  1. PSAP Gateway Appliance Installation Guide (911RTA-PGA1-IG-1.0.1)
  2. PSAP Gateway Incident Message API (911RTA-TD-PGA-IM-API_1.0)
  3. 911 RTA Gateway Appliance Test Protocol
  4. Research Project Description

**Proposed Schedule**

Should MARC desire to proceed, GeoComm will work with MARC to create Change Control document covering the existing GeoComm PSAP mapping system configuration change, testing and activation as well as a no-charge purchase order for the new GeoComm to SirenGPS API. GeoComm could accomplish the configuration change, interface implementation, and integration testing in Q4 2019 (October – December).
Public safety agencies considering 911 Real-Time Analytics (911 RTA) to distribute incident notifications often ask questions related to understanding how 911 RTA works, what benefits the service provides, and whether there is any risk. The following provides some frequently asked questions and answers.

1. **What is unique about 911 RTA?**

   911 RTA uses artificial intelligence to identify large-scale emergency incidents in real time using automated algorithmic analysis research using the location, proximity and frequency of 911 calls from previous active shooter incidents. 911 RTA software can automatically detect a likely large-scale emergency and generate an incident indication 4X faster than dispatch. This service can identify a potential mass casualty incident and send a notification to leadership and special weapons and tactical up to 50X faster than without automation. SirenGPS has been researching and developing this technology since 2012 and holds several patents related to using an analytic process to identify mass casualty incidents.

2. **Who are 911 RTA community stakeholder subscribers?**

   SirenGPS is making 911 RTA notifications available as a subscription service to appropriate security and leadership at schools, businesses and places of worship in communities where public safety authorizes distribution of incident notifications. Subscribers can only receive notifications for incidents that impact property they own, control or protect. Revenue generated from subscriptions to community stakeholders makes it possible for SirenGPS to offer the service to public safety without charge.

3. **What notifications does 911 RTA distribute and who can receive them?**

   911 RTA distributes incident notifications when the software identifies a potential large-scale emergency and from dispatcher 911 incident codes. 911 RTA incident notifications provide a description of the nature of the incident and a location for the incident. These notifications are delivered via text, email and/or automated call. Public safety agencies manage 911 RTA recipient lists to send notifications to leadership and appropriate first responders associated with agencies within the same political subdivision, and their mutual aid partners. Where authorized, community stakeholders such as security at a business, school or hospital can subscribe to the service to receive incident notifications for matters that directly impact property they own, control or provide security. Community stakeholder notifications include a timestamp of the 911 call, location of where the call was placed, and incident code where applicable.

4. **How does 911 RTA software identify large-scale emergency incidents?**

   911 RTA software monitors the location, proximity, frequency, and related meta-data for 911 calls to identify potential large-scale emergency incidents in real-time. An algorithmic model has proven to reliably identify active shooter incidents from
frequency, location and proximity of 911 calls without access to other information. SirenGPS is working with artificial intelligence and data scientists at St Louis University and the University of Notre Dame to expand 911 RTA’s ability to automatically identify significant emergency incidents.

5. **How does 911 RTA protect first responders and the agencies they work for?** We appreciate that agencies want to do everything possible to keep first responders safe and limit risks to their agencies -- and we do too. SirenGPS has written our commitment to protecting our public safety partners into the 911 RTA terms and conditions:
   a. 911 RTA alerts are only available to approved commercial stakeholders and only for incidents that impact premises they own, control or provide with security.
   b. Public Safety agencies may restrict distribution of 911 RTA notifications to stakeholders and terminate a subscriber at their discretion (¶ 6.5).
   c. Public Safety agencies have sole discretion to decide what incident codes, if any, may be sent to stakeholder subscribers (¶ 6.5).
   d. Public Safety agencies can deny and/or delay 911 RTA notifications to stakeholder subscribers for specific incident types (¶ 6.5).
   e. Stakeholder subscription agreements include a release of liability for public safety agencies that use 911 RTA (¶ 5.7).

911 RTA terms and conditions available for download at https://sirengps.com/misc/contract-documents

6. **How does 911 RTA decrease the risk of litigation for public safety agencies?**

   Public safety agencies provide most of their services to entities and individuals without any agreement in place that allocates risk. 911 RTA creates an opportunity for public safety entities to benefit from an agreement with community stakeholders that includes a waiver related to requests for emergency information and services.

7. **911 RTA would put more information out in the community about emergency response times. Could this increase the frequency of claims related to response times?**

   There is strong legal precedent supporting public safety agency prerogative to make operational decisions – including even the decision not to respond to 911 calls. This precedent makes claims related to emergency response times unlikely. Because the 911 RTA subscriber agreement includes a waiver that addresses claims related to emergency information and response, the risk of lawsuits filed by subscribers is further diminished.

   Moreover, public safety agencies that routinely publish 911 call information report no increase in claim activity. Starting in 2015 law enforcement agencies began participating in the Police Data Initiative, a research collaboration that encourages agencies to publish 911 call information as well as other information about crime and requests for service in cooperation with the United States Department of Justice and various
research interests. More than 200 participating agencies regularly publish information and statistics about crime and emergency service requests in their communities. Dozens of cities publish relatively complete 911 call emergency service request information to public websites daily. The most commonly reported impact on participating agencies is a reduction in the effort required to respond to open records requests. Lists of participating agencies and data sets are available online at policedatainitiative.org.

8. Are public safety agencies that use 911 RTA required to make the service available to every stakeholder?

There is clear precedent from the Supreme Court of the United States that supports a public safety agency offering 911 RTA to some community stakeholders and not to others. See Town of Castle Rock, Colorado v. Gonzales, 545 U.S. 748 (2005).

9. Is there a risk of claims that personal information has been exposed?

911 RTA notifications distribute information about incidents, not calls, and the service doesn’t capture any Personally Identifiable information (PII). PII is typically understood to include date of birth, social security number, financial institution account numbers, health information, and other information subject to special protection by law. 911 RTA does not collect any PII. The only information that 911 RTA collects that can reasonably identify an individual is a caller’s telephone number. While telephone numbers do not qualify as Personally Identifiable Information, SirenGPS treats phone numbers as if they were sensitive, personal information. 911 RTA only uses phone numbers to validate data. Phone numbers are never shared with subscribing stakeholders and are encrypted at all times. 911 RTA meets or exceeds all data security requirements in states that have passed regulations prohibiting revealing the identity of 911 callers.

10. Is there insurance for a data breach?

While we believe exposure minimal, SirenGPS maintains $1M insurance coverage for the benefit of our clients related to 911 RTA data breach.

11. How does 911 RTA protect PSAP data and systems?

911 RTA is fully encrypted and designed to exceed NIST 800-171 security standards. 911 RTA does not monitor agency communications and does not expose any protected information. 911 RTA can only be configured through a direct connection and can only accept authorized communications. The 911 RTA Communication Gateway Appliance Specification explains 911 RTA system security features in more detail and can be downloaded at https://sirengps.com/content/911-rta-communication-gateway-appliance-specifications.
Public safety agencies strive to serve and protect their communities to the limits of their capabilities. In the effort to achieve that mission, leadership is often forced to contend with limited resources and the potential for litigation. It is helpful in evaluating risk associated with how a public safety agency goes about its business to understand that there is a clear boundary between decisions related to what services a public safety agency will provide to the community, and how services are provided in a specific intervention. A duty to act and standard of care are obligations that typically apply only once a public safety intervention begins (or is promised to a specific individual). For operational decisions not related to providing services to a specific individual, public safety agencies have broad latitude to decide what services will be provided, when, and for whom, including in regard the selection of technology and services. The difference lies in law that relieves public safety from the duty to act. This is perhaps best described by saying that a public safety agency’s duty is to serve and protect the community, but not any specific individual in that community.

Legal safeguards for public safety decisions are rooted in a tradition that recognizes the hazards of being responsible for making a community safe – a task that can never be completed.

Courts have uniformly held that until an emergency intervention begins, responding to a request for services remains the prerogative of the public safety agency receiving the request. The US Supreme Court considered claims alleging failure to prevent harm where public safety agencies exercised the discretion to not perform services they typically provide in the course of standard operational protocols. In Town of Castle Rock, Colorado v. Gonzales, 545 U.S. 748 (2005) the Castle Rock Police Department declined to take action to enforce a restraining order – an action that the department had made a commitment to include in the course of typical operations. Shortly after the department declined to enforce the order, the claimant’s children were murdered by the subject of the order. While tragic, Castle Rock illustrates the extent of discretion applicable in the performance of public safety operations.

The Castle Rock Court explained that law enforcement cannot operate under a mandate to protect citizens from harm in the context of constitutional due process claims alleging failure to safeguard life, liberty and property. The Castle Rock claimant had obtained a restraining order on behalf of herself and her three daughters against her estranged husband. Id. at 751. The preprinted text on the back of the form included a notice to law enforcement that stated law enforcement "SHALL" use every reasonable means to enforce the restraining order, including arrest or seeking a warrant when law enforcement had information amounting to probable cause that the restraining order had been violated. Id. at 752.

When the claimant’s estranged husband took her three daughters in violation of the restraining order, claimant contacted police numerous times, showed them a copy of the order, requested

---

1 Some states have instituted “Duty to Respond” statutes that require an agency that receives a 911 call to take reasonable steps to respond to the request for emergency service. However, this is the exception to the general rule and the obligation these statutes create is limited to the specifics of the statute in question. State courts have uniformly followed the rule of law articulated in Castle Rock and states have also codified this rule in statutes explicitly limiting the duty of first responders to provide services. See Warren v. District of Columbia, 444 A.2d 1, 4 (D.C. 1981), Souza v. City of Antioch, 62 California Reporter, 2d 909, 916 (Cal. App. 1997); Ford v. Town of Grafion, 693 N.E.2d 1047 (Mass. App. 1998); California Government Code, § 845; Mass. Gen. Laws Ann. Ch. 258 § 10(h).
that it be enforced, and asked the officers to find her children. Id. at 753-54. The police told Plaintiff to wait until later in the evening and did not make a reasonable effort to enforce the court order. Id. Late that night the husband arrived at the police station and opened fire on police. Officers returned fire, killing him. Shortly thereafter the bodies of all three daughters were discovered in the husband’s vehicle, murdered." Id. at 754. Claimant alleged pursuant to 42 U.S.C. § 1983 that the town of Castle Rock, Colorado, ("the Town") violated the Due Process Clause of the Fourteenth Amendment when its police officers, acting pursuant to official policy or custom, failed to respond properly to her repeated reports that her estranged husband was violating the terms of a restraining order. Castle Rock, 545 U.S. at 751 754. Contest regarding these claims resulted in grant of certiorari to the United States Supreme Court.

The Supreme Court considered whether the Claimant had a property interest in police enforcement of the restraining order and whether the Town deprived her of this property without due process by having a policy that tolerated non-enforcement of court orders. Castle Rock, 545 U.S. at 755. The Supreme Court stated that the “‘procedural component of the Due Process Clause does not protect everything that might be described as a benefit’”. Id. at 756. To have a property interest, a person clearly must have more than an abstract need, desire, or expectation. Claimant must, “‘instead, have a legitimate claim of entitlement to it.’” Id. at 756 (quoting Roth, 408 U.S. at 577). The Supreme Court recognized that entitlements are not created by the Constitution, but “are created and their dimensions are defined by existing rules or understandings that stem from an independent source such as state law.” Castle Rock, 545 U.S. at 756 (quoting Paul v. Davis, 424 U.S. 693, 709 (1976) and Roth, 408 U.S. at 577).

The Supreme Court reviewed the court order, which included language that dictated the officers "shall use every reasonable means to enforce a restraining order" and Colorado law, in which the legislature made clear its intent to have restraining orders enforced. Castle Rock, 545 U.S. at 759-60. Recognizing a well-established tradition of police discretion, the Supreme Court found that a true mandate for action would require stronger language than "shall use every reasonable means." Id. at 160-61. The Supreme Court found: "Such indeterminacy is not the hallmark of a duty that is mandatory. Nor can someone be safely deemed ‘entitled’ to something when the identity of the alleged entitlement is vague." Id. at 763. The Supreme Court held that even if the Colorado laws and court order created an entitlement to enforcement of the court order, that entitlement would still not constitute a property interest for purposes of the Due Process Clause. Id. at 766 768.

Due Process does not confer an affirmative right to governmental aid to protect an individual's rights, even where such aid may be necessary to secure life, liberty, or property interests of which the government itself may not deprive the individual. DeShaney v. Winnebago County Dept. of Social Services, 489 U.S. 189, 196 (1989); Johnson v. City of Seattle, 474 F.3d 634, 639 (9th Cir. 2007). "If the Due Process Clause does not require the State to provide its citizens with particular protective services, it follows that the State cannot be held liable under the Clause for injuries that could have been averted had it chosen to provide them." DeShaney, 489 U.S. at 196-97. In addition, the Due Process Clause is not implicated by an official's negligent act that results in unintended loss of or injury to life, liberty, or property. Daniels v. Williams, 474 U.S. 327, 328 (1986); Alfrey v. U.S., 276 F.3d 557, 568 (2002).
Legal safeguards to public safety agencies’ operational prerogative are based in both discretion and sovereign immunity. Clear, compelling precedent supports public safety agencies exercising discretion in whether to provide or withhold services, and in what services they provide. The extent of this discretion is such that there is no cause of action where an agency does not safeguard citizens from harm – and that public safety has no obligation to do so. Public safety agencies have the legal prerogative to perform, or to not perform services, even where the action required to protect citizens from harm is an action that a public safety agency often performs but chooses in the instant not to perform – even where there is actual knowledge of a likely harm that might be prevented.

This Due Process precedent is helpful in the context of considering what services public safety agencies choose to provide, and how they provide them, including with respect to choices made regarding technology. The law acknowledging the validity of public safety discretion appropriately recognizes that safeguarding a community necessarily involves competing interests in pursuit of an unattainable goal.

In addition to the protection afforded by Castle Rock and similar cases, Missouri public safety agencies are protected by the doctrine of sovereign immunity. When Missouri public safety exercises discretion in the course of fulfilling their obligations, they cannot be subject to tort claims related to those decisions. This immunity is broad and is only subject to exceptions specifically enumerated by the legislature. There are currently only two exceptions to this immunity, which are for claims related to motor vehicle accidents and for claims related to maintaining inherently dangerous conditions on government property. See MO 537.600.1.

While Kansas has not adopted Missouri’s broad interpretation of sovereign immunity, the Kansas legislature and courts arrive at the same result through other means. Instead of Missouri’s broad prohibition on claims (immunity) with a few exceptions, Kansas enacted a broad allowance for claims against government entities (an enabling statute), with a laundry list of “exceptions”. Each of the exceptions extends immunity to an identified activity. The Kansas Police and Fire Protection exception to the general rule enabling claims against public entities extends essentially the same sovereign immunity to Kansas agencies available in Missouri. See K.S.A 75-6104(n). This provision of the claims allowance statute carves back certain activities, in this case protecting agencies from claims related to operational decisions. See Beck v. Kansas Adult Authority, 241 Kan. 13, 24, 735 P.2d 222 (1987) (“The determination of how to provide police protection is immunized.” Determination of how to provide police protection at a hospital emergency room.); Gragg v. Wichita State Univ., 261 Kan. 1037, 1060–61, 934 P.2d 121 (1997) (Determination of the nature and type of police protection to provide at a special event—no liability on claim that inadequate personnel at event to dissuade gang violence.); and Keiswetter v. State, 304 Kan. 362, 372–73, 373 P.3d 803, 805 (2016) (Determination of how to supervise a work crew of inmates mowing grass outside the confines of a correctional facility.)

Under Kansas law an individual may sue public safety if a duty owed to that individual is breached. However, Kansas law also provides that there is no duty related to the provision of public safety services to any individual derived from services rendered to the public. Under the public duty doctrine, a plaintiff suing a governmental entity in negligence cannot establish the duty element for a claim when the duty is a public one, i.e., owed to the public at large and not to
any particular individual. *Keiswetter v. State*, 304 Kan. 362, 365, 373 P.3d 803, 805 (2016). In Kansas a claim against an agency is permissible, but only where public safety has made an express promise to perform that is specific to the claimant, exclusive of any other obligation.

Kansas grants public safety immunity from liability on claims by individuals arising from the performance or nonperformance of an officer's general duties such as enforcement of law and crime prevention. Liability arises only where public safety breaches a specific duty owed to an individual. Put another way, an officer must owe an affirmative duty to an individual before s/he may be held liable.” *Hendrix v. City of Topeka*, 231 Kan. 113, 120, 643 P.2d 129 (1982). Public safety generally owes its duty to the public at large rather than to any individual. *Lamb v. State*, 33 Kan.App.2d 843, 847, 109 P.3d 1265 (2005). Indeed, Kansas public safety officials retain immunity where they withhold services that are normally offered. See *Potts v. Board of County Commissioners of Leavenworth County, Kansas*, 39 Kan.App.2d 71, 176 P.3d 988 (2008) (EMS attendants had no special duty to transport an elderly woman to the hospital against her wishes despite demand of daughter with power of attorney.), *Lovitt v. Board of Commissioners of Shawnee County, Kansas*, 43 Kan.App.2d 4, 221 P.3d 107 (2009) (Dispatcher has no special duty to a citizen who calls for emergency assistance in absence of a promise by the dispatcher to assist and detrimental reliance by the citizen.) and *Cansler v. State*, 234 Kan. 554, 571, 675 P.2d 57 (1984); *Washington v. State*, 17 Kan.App.2d 518, 525, 839 P.2d 555, rev. denied 252 Kan. 1095 (1992) (Correctional officers do not owe a duty to specific individuals because their duty to keep offenders separate from society is owed to the public at large.) In fact, under Kansas law public safety must make an affirmation of an obligation for a duty to exist respective to an individual. Special duty arises under three specific circumstances: (1) When gov’t has custody/care of wrongdoer; (2) When gov’t has custody/care of the injured person; or (3) When gov’t took affirmative action causing injury; or made a specific promise or representation creating justifiable reliance by the person injured. *Williams v. C-U-Out Bail Bonds, LLC*, 54 Kan.App.2d 600, 608, 402 P.3d 558 (2017); *Potts v. Board of Leavenworth County Comm'r's*, 39 Kan.App.2d 71, 81, 176 P.3d 988 (2008).

While careful consideration of the pros and cons of any new technology or service is always a good idea, public safety agencies have legal protection that provides significant latitude when making operational decisions. The Supreme Court and state law make it clear that public safety agencies in Kansas and Missouri have legal protection to exercise discretion in making operational decisions. Agencies in Missouri and Kansas are free to exercise this prerogative in regard to the services offered and to the manner in which those services are provided. Agencies are free to determine whether a service should be offered, whether a generally available service should be extended in a given circumstance, to whom the service should be made available, and to withhold services.
On February 14, 2018 a former student entered the Marjory Stoneman Douglas High School and started shooting at students, faculty and staff, killing 17 and injuring 17.

By the time law enforcement arrived the shooter had fled the scene.

### Marjory Stoneman Douglas High School Attack Timeline

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:21:18</td>
<td>[00:00] Armed suspect enters building 12 MSD</td>
</tr>
<tr>
<td>14:21:33</td>
<td>[00:15] First shots fired</td>
</tr>
<tr>
<td>14:22:49</td>
<td>[01:31] First 911 Call</td>
</tr>
<tr>
<td>14:23:26</td>
<td>[02:08] Possible Shots Fired radio call</td>
</tr>
<tr>
<td>14:25:00</td>
<td>[03:42] Dispatcher confirms active shooter at MSD</td>
</tr>
<tr>
<td>14:28:14</td>
<td>[06:56] Active Shooter All Units radio call</td>
</tr>
<tr>
<td>14:31:00</td>
<td>[09:42] First SWAT Callout via SMS</td>
</tr>
</tbody>
</table>

First responder communication milestones indicate situational awareness

Resource escalation for the attack was 15% faster than average, but officers still arrived too late to stop it.
Situational awareness enables a faster response

911 Real-Time Analytics would have identified the attack and sent alerts 10 seconds after the first 911 call.

Marjory Stoneman Douglas High School Attack Timeline

- 14:21:18 [00:00] Armed suspect enters building 12 MSD
- 14:21:33 [00:15] First shots fired
- 14:22:49 [01:31] First 911 Call
- **14:22:59 [01:41]** 911 Real-Time Analytics Triggered
- 14:23:26 [02:08] Possible Shots Fired radio call
- 14:25:00 [03:42] Dispatcher confirms active shooter at MSD
- 14:28:14 [06:56] Active Shooter All Units radio call
- 14:31:00 [09:42] First SWAT Callout via SMS

911 RTA automates incident identification enabling faster emergency response.

- 4X faster than the first radio call.
- 50X faster SWAT alert.
SirenGPS
911 Real-Time Analytics

PSAP Gateway
Incident Message API

911RTA TD-PGA-IM-API

Version 1.0
June 25, 2019
0 Document Management

0.1 Purpose

The SirenGPS PSAP Gateway web services Application Programming Interface (API) is a backend interface that allows PSAP call handling systems, e.g. Computer Aided Dispatch (CAD), Call Routing (CR), and Geographic Information Systems (GIS), to send incident messages to the SirenGPS 911RTA Service.

0.2 History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Amendment</th>
<th>Amended By</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/04/2019</td>
<td>1.0a</td>
<td>Initial draft</td>
<td></td>
</tr>
<tr>
<td>06/25/2019</td>
<td>1.0</td>
<td>Added GIS as a source type. v1.0 Final.</td>
<td>BM</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

0 DOCUMENT MANAGEMENT ............................................................................................................2
  0.1 PURPOSE .................................................................................................................................2
  0.2 HISTORY .................................................................................................................................2
1 SESSION SECURITY .......................................................................................................................4
2 SCHEMA VALIDATION ..................................................................................................................5
3 SEND MESSAGE ..........................................................................................................................6
1 Session Security

**POST** /psapi/security/session

**Implementation Notes**

Authenticates the caller using PSAP ID and authorization key credentials. If the login attempt is successful it returns back a SessionToken which can be used in subsequent calls to identify the user and demonstrate that authentication and authorization has been completed. All other calls require a valid SessionToken to be passed in a header named PSAPI-Session-Token.

**Response Class (Status 200)**

```json
{
    "sessionExpiration": "string",
    "sessionToken": "string"
}
```

Response content type: application/json

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Data Type/Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessionCredentials</td>
<td>Session credentials</td>
<td>body</td>
<td>{&quot;type&quot;: &quot;string&quot;, &quot;vendor&quot;: &quot;string&quot;, &quot;product&quot;: &quot;string&quot;, &quot;version&quot;: &quot;string&quot;, &quot;psapId&quot;: &quot;integer&quot;, &quot;authorizationKey&quot;: &quot;string&quot;}</td>
</tr>
</tbody>
</table>

**Response Messages**

<table>
<thead>
<tr>
<th>HTTP Status Code</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Unsupported generator. The vendor product version is not supported by the interface.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized.</td>
</tr>
<tr>
<td>405</td>
<td>Method not allowed (only POST requests supported).</td>
</tr>
<tr>
<td>429</td>
<td>Too many requests (no more than 1 request/second/requester IP address permitted).</td>
</tr>
<tr>
<td>500</td>
<td>Internal server error.</td>
</tr>
</tbody>
</table>
2 Schema validation

**POST** /psapi/schema

**Implementation Notes**

Defines the XML schema (XSD) for the incident messages that are generated by the source system and sent to the 911RTA PSAP Gateway Appliance.

**Response Class (Status 200)**

None.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Data Type/Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSAPI-Session-Token</td>
<td>A unique identifier which is issued by 9011RTA as a result of a successful authentication to the Session Login API by an authorized Third Party.</td>
<td>header</td>
<td>string</td>
</tr>
<tr>
<td>Content-Type schema</td>
<td>Content type Incident message XML schema (XSD).</td>
<td>header</td>
<td>“application/XML”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>body</td>
<td>XSD (application/XML)</td>
</tr>
</tbody>
</table>

**Response Messages**

<table>
<thead>
<tr>
<th>HTTP Status Code</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Session token missing</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
</tr>
<tr>
<td>403</td>
<td>Session token expired</td>
</tr>
<tr>
<td>405</td>
<td>Method not allowed (only POST requests supported).</td>
</tr>
<tr>
<td>406</td>
<td>Bad XSD schema</td>
</tr>
<tr>
<td>500</td>
<td>Internal server error</td>
</tr>
</tbody>
</table>
3 Send message

**POST** /psapi/message

**Implementation Notes**
Send incident message.

**Response Class (Status 200)**
None.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Type</th>
<th>Data Type/Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSAPI-Session-Token</td>
<td>A unique identifier which is issued by 911RTA as a result of a successful authentication to the Session Login API by an authorized Third Party.</td>
<td>header</td>
<td>string</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Content type</td>
<td>header</td>
<td>“application/XML”</td>
</tr>
<tr>
<td>message</td>
<td>Incident message XML.</td>
<td>body</td>
<td>XML (application/XML)</td>
</tr>
</tbody>
</table>

**Response Messages**

<table>
<thead>
<tr>
<th>HTTP Status Code</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Session token missing</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
</tr>
<tr>
<td>403</td>
<td>Session token expired</td>
</tr>
<tr>
<td>405</td>
<td>Method not allowed (only POST requests supported).</td>
</tr>
<tr>
<td>406</td>
<td>Schema validation error</td>
</tr>
<tr>
<td>500</td>
<td>Internal server error</td>
</tr>
</tbody>
</table>
911 Real-Time Analytics

PSAP Gateway Appliance
Installation Guide
# Contents

- **Security Features** ................................................................. 3
- **Hardware and Network Setup** ................................................. 4
  - Unpack Your Gateway Appliance ........................................... 4
  - Front Panel ............................................................................. 5
  - Rear Panel ............................................................................... 5
  - Position Your Gateway Appliance ......................................... 6
  - Cable Your Gateway Appliance ............................................. 6
  - Network Topology .................................................................... 8
- **Provision the Gateway Appliance** ......................................... 9
  - Connect to the Management Port ......................................... 9
  - Connect to the PSAP Network ............................................ 10
  - Connect to PSAP CAD/CR System ..................................... 11
- **Supplemental Information** .................................................... 14
  - Factory Defaults ................................................................. 14
  - Technical Specifications ..................................................... 15
  - Support .................................................................................. 16
The 911RTA PSAP Gateway Appliance has been designed with security as a top priority. The appliance runs the 911 Real-Time Operating System (911RTOS), a proprietary operating system developed by SirenGPS.

Key security features of the gateway appliance include:

- Solid-state, fanless, and approximately the size of a book, the gateway appliance is built by SUPERMICRO®, a leading manufacturer of server and IoT server solutions, for industry leading reliability.
- A minimal Ubuntu 18.04 LTS installation is a secure operating system “out of the box”.
- Information collected through the gateway appliance is encrypted subject to confidentiality requirements and limited to non-sensitive data categories such as location, timestamp, incident code and number(s).
- Communication with PSAP systems is typically limited to passing data from PSAP systems to the gateway appliance, without information or instructions communicated from the gateway appliance to PSAP systems.
- Root login access to the gateway appliance from the network/internet is disabled.
- The ability to boot the gateway appliance from USB-attached devices is disabled.
- System BIOS access is password protected in compliance with NIST 800-171 security standards and can only be configured through a direct connection to the MGMT port.
- Access via the MGMT port to configure for operation is restricted to a single source IPv4 address (10.0.0.2) and the admin web interface (port 443) only. No other services are accessible via this interface.
- Access to a gateway appliance connected to PSAP systems is restricted to inbound requests that can only come from the configured CAD/CR system IPv4 address or authorized and authenticated SirenGPS 911RTA service.
- Access from all public or unauthorized LAN IP addresses is prohibited.
- All unplanned server reboots, network outage, communication and configuration of the gateway appliance is logged offsite in real-time.
This chapter covers the following topics:

- Unpack Your Gateway Appliance
- Front Panel
- Rear Panel

Unpack Your Gateway Appliance

Your package contains the following three items.

- Gateway appliance
- Cross-over Ethernet cable
- Power adapter

Figure 1. Package contents
Front Panel

The gateway appliance power button is shown in the following figure.

![Gateway appliance front view](image)

**Figure 2. Gateway appliance front view**

Rear Panel

The gateway appliance connections are shown in the following figure.

![Gateway appliance rear view](image)

**Figure 3. Gateway appliance rear view**
The following table lists and describes each connection on the rear panel of the gateway appliance.

**Table 1. Rear Panel Connections**

<table>
<thead>
<tr>
<th>Connection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>Power adapter input.</td>
</tr>
<tr>
<td>USB</td>
<td>Reserved. Do not connect peripherals to these ports.</td>
</tr>
<tr>
<td>HDMI</td>
<td>Reserved. Do not connect peripherals to this port.</td>
</tr>
<tr>
<td>LAN</td>
<td>Ethernet LAN port. Connect this port to the PSAP local area network.</td>
</tr>
<tr>
<td>MGMT</td>
<td>Management LAN port. This port is used for initial setup and configuration of the gateway appliance only. Do not connect this port to a local area network.</td>
</tr>
</tbody>
</table>

**Position Your Gateway Appliance**

The gateway appliance is a solid-state, fanless, computer that may get warm during normal operation. It should be placed off the floor in a well-ventilated space at room-temperature or in a cooled server room or cabinet. Do not let dust accumulate on or around the appliance as this may affect how hot it gets and impact the performance and stability of the gateway.

**Cable Your Gateway Appliance**

Your gateway appliance must be provisioned and configured before it can connect to the 911RTA service. During the initial setup of the device, you will need to connect a desktop or laptop computer to the MGMT port using the supplied cross-over Ethernet cable. After the provisioning of the gateway appliance has been completed you can disconnect the cable from the MGMT port as it is not required during normal operation.

*Note:* Do not discard the supplied cross-over Ethernet cable as you may need to use this if you need to run the setup again or to update the service.
Cable the Gateway Appliance

The gateway appliance must be able to connect to both the PSAP Computer Aided Dispatch (CAD) and/or Call Routing (CR) system as well as the Internet over the PSAP network.

To cable your gateway appliance:

Connect the LAN port on the gateway appliance to the PSAP network using a Gigabit Ethernet (1000baseT) capable switch using a standard Cat6 Ethernet cable (not provided).

1. Connect the power adapter provided in the package to the gateway appliance and then plug the power adapter into an electrical outlet.

   **Note:** Use an uninterruptable power supply (UPS) whenever possible to minimize downtime and potential damage to the gateway appliance in the event of brief power surges or outages.

2. Press the **Power On/Off** button on the front panel of the gateway appliance.

   **Note:** Never unplug or switch off your appliance unless instructed to do so by SirenGPS technical support staff. Doing so may result in damage to the gateway appliance.
Network Topology

The gateway appliance must be able to establish a connection to the PSAP CAD/CR server to receive incident information and to the Internet to connect to the 911RTA service. While the gateway appliance has a built-in firewall to ensure that only authorized inbound and outbound communication from and to the 911RTA service can be established over the Internet and from the configured PSAP CAD/CR server, typical PSAP installations will have their own hardware firewalls in place for network security.

The figure below describes a typical network configuration where the gateway appliance is behind a firewall relative to the PSAP CAD/CR server(s).

![Network diagram](image)

**Figure 5. Typical network configuration**

**DMZ 101**

“DMZ” is a military term for a “demilitarized zone” separating hostile parties. A network DMZ is a secure space between the public internet – and hackers – and an internal critical resources network. The internal network is not connected directly to the internet, relying on services in the DMZ to communicate with the outside world. A firewall between the internal services and the DMZ limits communication to authorized services running in the DMZ. Another firewall protects systems in the DMZ from outside attacks.

Installed in a PSAP DMZ, the gateway appliance maintains a secure, encrypted, internet connection with SirenGPS 911 Real-Time Analytics to identify significant incidents. The gateway appliance is, by design, unable to accept unauthorized communication or to be re-configured remotely, frustrating attacks from would be hackers.
Provision the Gateway Appliance

This chapter contains the following sections:

- Connect to the Management Port
- Connect to the PSAP Network
- Connect to the PSAP CAD/CR System

Connect to the Management Port

Before the gateway appliance can connect to either the PSAP CAD/CR system or the 911RTA service it must be configured to access the PSAP local area network and, if required, set appropriate credentials to access the PSAP CAD/CR system and 911RTA service.

Configuration of the gateway appliance is done by connecting a computer to the MGMT port on the gateway (as described above) and using a browser to access the provisioning portal on the gateway.

➢ To access to your gateway appliance:

1. With your computer connected to the gateway appliance MGMT port using the provided cross-over Ethernet cable (see above), configure the network settings on the computer to use the following manual network address:

   IPv4 Address: 10.0.0.2
   Subnet Mask: 255.255.255.252
   Router: 10.0.0.1 or none

   **Note:** The IP address of the MGMT port is configured to be 10.0.0.1 and cannot be changed by the user. Computers connected to the port must use the IP address 10.0.0.2 as the MGMT interface is configured to allow only one host to be connected to it for security reasons. Similarly, you should not connect the MGMT port to a network switch to avoid unauthorized access.

2. Launch a web browser.

3. Type **https://10.0.0.1** into the address bar of the browser and press Enter/Return.

   A login page is displayed.
4. Enter the gateway appliance username and password.

5. The user name is **admin**. The password will have been provided to you in your welcome email. The username and password are case-sensitive.

   **Note:** If you do not have your password, please contact SirenGPS customer support at support@sirengps.com.

6. The gateway appliance Home Page displays. You can now complete configuration and provisioning of your gateway appliance.

## Connect to the PSAP Network

By default, the gateway appliance will attempt to obtain an IP address for the LAN port using Dynamic Host Configuration Protocol (DHCP). If the PSAP network does not provide DHCP services then the gateway appliance LAN port will need to be configured manually using a static IP address or, if available, BOOTP.

With your computer connected to the gateway appliance MGMT port using the provided cross-over Ethernet cable (see above) and logged into the admin web interface, configure the network settings on the gateway appliance to access the PSAP network.

- **To connect to the PSAP network:**
  1. Select the **Manage** view from the top menu bar.
  2. Select **Network** from the sidebar menu to display the current network configuration settings.
  3. Select the correct IPv4 address configuration method from the **Configure IPv4** dropdown select box and complete any necessary fields with the correct settings for your network.
  4. When all changes have been made, click **Accept** to save and update the network configuration. This may take a few moments while the appliance applies the new configuration.
Connect to PSAP CAD/CR System

Your gateway appliance supports connection to PSAP CAD/CR systems that include the following vendors:

Table 2. Supported CAD Systems

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Public Safety</td>
<td>TAC.10 CAD</td>
</tr>
<tr>
<td>CentralSquare Technologies</td>
<td>CentralSquare CAD</td>
</tr>
<tr>
<td>Motorola Solutions</td>
<td>PremierOne CAD</td>
</tr>
</tbody>
</table>
### Vendor and Product

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hexagon Safety &amp; Infrastructure</td>
<td>Intergraph I/CAD</td>
</tr>
<tr>
<td>Tyler Technologies</td>
<td>New World Enterprise CAD</td>
</tr>
<tr>
<td>Harris Computer</td>
<td>Global CAD</td>
</tr>
<tr>
<td></td>
<td><a href="https://globalsoftwarecorp.com/">https://globalsoftwarecorp.com/</a></td>
</tr>
</tbody>
</table>

### Table 3. Supported CR Systems

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorola Solutions</td>
<td>Vesta® 9-1-1</td>
</tr>
<tr>
<td>West Corporation</td>
<td>Call handling Suite</td>
</tr>
</tbody>
</table>

*Additional vendor integrations are in progress and on demand. Please let us know if you need integration with a service provider that is not listed here.*

CAD and CR system products can connect to the gateway appliance through a push or poll interface depending on the particular vendor product implementation.

If the selected CAD/CR system product provides a push API whereby 911 incident events are sent to the gateway appliance, then the CAD/CR system software may require configuration to send event messages to the IPv4 address configured in the PSAP network settings.

If the selected CAD/CR system product provides a poll API whereby the gateway appliance must log into the CAD/CR system and retrieve a list of new event messages, then a form will be displayed below the product selection dropdown box for you to enter the necessary network address and login credentials for the selected CAD system product.
To connect to a “push” PSAP CAD/CR system:

1. Select the Manage view from the top menu bar.
2. Select CAD/CR System > Product from the sidebar menu to display the current CAD/CR system configuration settings.
3. Click the Add CAD/CR button to add a new CAD/CR system to the configuration.
4. Select your PSAP CAD/CR system vendor from the Vendor dropdown select box.
5. The supported products will be displayed in the Product selection drop-down select box. If only one product is supported, then no further selection is necessary.
6. Click Accept to save your selections.

To connect to a “poll” PSAP CAD/CR system:

1. Select the Manage view from the top menu bar.
2. Select CAD/CR System > Product from the sidebar menu to display the current CAD/CR system configuration settings.
3. Click the Add CAD/CR button to add a new CAD/CR system to the configuration.
4. Select your PSAP CAD/CR system vendor from the Vendor drop-down select box.
5. The supported products will be displayed in the Product selection drop-down select box. If only one product is supported, then no further selection is necessary.
6. Enter the IPv4 address and Port number of the CAD/CR system interface to which the gateway appliance will connect.
7. Enter the Username and Password credentials required for access to the CAD/CR system.
8. To test whether the values entered are correct, click Test Connection. A status message will be displayed if a successful connection is made or if there is an error.
9. Click Accept to save your selections.
Supplemental Information

This appendix includes the following sections:

- Factory Default Settings
- Technical Specifications

Factory Defaults

Table 4. Factory Defaults

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway appliance login</td>
<td></td>
</tr>
<tr>
<td>User login URL</td>
<td><a href="https://10.0.0.1">https://10.0.0.1</a></td>
</tr>
<tr>
<td>User name (case sensitive)</td>
<td>admin</td>
</tr>
<tr>
<td>Password (case sensitive)</td>
<td>Provided in welcome email</td>
</tr>
<tr>
<td>LAN Network</td>
<td>LAN IP</td>
</tr>
<tr>
<td></td>
<td>Supplied by DHCP</td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
</tr>
<tr>
<td></td>
<td>Supplied by DHCP</td>
</tr>
<tr>
<td>MGMT Network</td>
<td>MGMT IP</td>
</tr>
<tr>
<td></td>
<td>10.0.0.1</td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
</tr>
<tr>
<td></td>
<td>255.255.255.252</td>
</tr>
</tbody>
</table>
## Technical Specifications

The following table describes the technical specifications for the gateway appliance.

### Table 5. Technical Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power adapter</td>
<td>40W lockable 12V DC power adapter</td>
</tr>
<tr>
<td>Physical</td>
<td>Width: 5.82&quot; (148mm)</td>
</tr>
<tr>
<td></td>
<td>Height: 1.72&quot; (44mm)</td>
</tr>
<tr>
<td></td>
<td>Depth: 4.64&quot; (118mm)</td>
</tr>
<tr>
<td></td>
<td>Package: 5.5&quot; (H) x 9.5&quot; (W) x 8&quot; (D)</td>
</tr>
<tr>
<td></td>
<td>Weight: Gross Weight: 3.52 lbs (1.6 kg)</td>
</tr>
<tr>
<td></td>
<td>Net Weight: 2.2 lbs (1 kg)</td>
</tr>
<tr>
<td>Environmental</td>
<td>Operating Temperature: -20°C to 50°C (-4°F to 122°F)</td>
</tr>
<tr>
<td></td>
<td>Non-operating Temperature: -40°C to 70°C (-40°F to 158°F)</td>
</tr>
<tr>
<td></td>
<td>Operating Relative Humidity: 8% to 90% (non-condensing)</td>
</tr>
</tbody>
</table>
Support

Thank you for subscribing to the SirenGPS 911RTA service. You can visit www.sirengps.com/about/support to get help, access the latest downloads and user manuals, and join our community. We recommend that you use only SirenGPS support resources.

Trademarks

© SirenGPS, LLC., SirenGPS, the SirenGPS Logo, 911RTA, and the 911RTA Logo are trademarks of SirenGPS, LLC. Any non-SirenGPS trademarks are used for reference purposes only.

Updated April, 2019
The 911 RTA Gateway Appliance is emulated in a test environment to enable remote testing. The following provides guidance on executing communication testing against the 911 RTA REST API test service as described in the API documentation, 911RTA TD-PGA-IM-API. Expected results as seen from the message producer end are provided below.

Authorization Key, IP Address and port information for the test service will be provided in a separate communication.

API communication follows the steps detailed in the API specification document 911RTA TD-PGA-IM-API as follows:

1. Establish a session,
2. Submit an XSD schema, and
3. Send messages.

**Session initialization**
The first step is to get a session token. Submission of the authorization key initiates a session request by passing the parameters specified in the API. The system will respond with an HTTP code of 200 together with a session token and expiration to be used in subsequent calls to the API. The default expiration of the token is 4 hours.

**Schema submission**
The XSD schema must be submitted before messages can be sent (you’ll receive an error otherwise). The API does some simple validation of the schema to make sure it is well-formed. HTTP code 200 is returned on successful schema submission (no data is returned). See the API documentation for an explanation of error codes.

**Message submission**
Once the XSD has been submitted, the service will accept messages. On successful message submission, an HTTP code of 200 is returned (no data is returned). Unsuccessful submission will return an error code. The most likely errors are failure to validate the XML against the XSD or an expired session token (in which case you’ll need to request a new session token, no need to resubmit the XSD if it hasn’t changed).
Every second counts

Presented to Mid-America Regional Council
SirenGPS submits the following for your consideration

SirenGPS proposes to partner with MARC to deploy **911 Real-Time Analytics (911 RTA)** a software service designed to enhance situational awareness in emergencies.

---

**Who we serve**

- **Public Safety**
- **Community Stakeholders**

---

**Our software**

**911 Real-Time Analytics**
Patented artificial intelligence designed to rapidly identify large-scale emergency incidents, capable of sending incident notifications 50x faster than without automation.

---

**Our offer**

SirenGPS would like to deploy **911 RTA** interoperable incident notification software with MARC and its partner agencies as follows:

- No charge to MARC or partner agencies
- Public safety retains control of their information
- Subscription terms that protect public safety
- Agencies may withdraw without penalty
The challenge responding to large-scale emergencies

Rapid escalation of emergency response resources is critical in large-scale emergencies.

**Recognizing the Need:**
During an attack it typically takes 10 minutes to activate special weapons and tactical (SWAT) and to start making mutual aid calls.

**Most attacks are over in less than 15 minutes**
[Blair & Schweit (2014); ALERRT (2018); National Threat Assessment Center (2019)].

**Golden hour: 60 minutes for trauma intervention**
[Kotwal, et al. (2015); Pham et al. (2017)].
Situational awareness milestones illustrate an opportunity for improvement

Resource escalation for the MSD attack was 15% faster than average -- but was still not fast enough.

On February 14, 2018 a former student entered the Marjory Stoneman Douglas High School and started shooting at students, faculty, and staff, killing 17 and injuring 17.

By the time law enforcement arrived the shooter had fled the scene.

Marjory Stoneman Douglas High School Attack Timeline

14:21:18 [00:00] Armed suspect enters building 12 MSD
14:21:33 [00:15] First shots fired
14:22:49 [01:31] First 911 Call
14:23:26 [02:08] Possible Shots Fired radio call
14:25:00 [03:42] Dispatcher confirms active shooter at MSD
14:28:14 [06:56] Active Shooter All Units radio call
14:31:00 [09:42] First SWAT Callout via SMS
911 RTA supports faster situational awareness in large-scale emergencies

911 RTA monitors 911 call location, proximity, frequency, and related information to automatically detect 911 call patterns identified in previous active shooter incidents.

911 RTA is designed to monitor the 240 million 911 calls that occur in the US each year to identify large-scale emergency incidents.
Distributing situational awareness to enable a faster response

911 RTA would have identified the MSD attack and sent alerts 10 seconds after the first 911 call.

Marjory Stoneman Douglas High School Attack Timeline

14:21:18 [00:00] Armed suspect enters building 12 MSD
14:21:33 [00:15] First shots fired
14:22:49 [01:31] First 911 Calls
14:23:26 [02:08] Possible Shots Fired radio call
14:25:00 [03:42] Dispatcher confirms active shooter at MSD
14:28:14 [06:56] Active Shooter All Units radio call
14:31:00 [09:42] First SWAT Callout via SMS

911 RTA automates incident identification to enable a faster emergency response.

- 4x faster than the first radio call
- 50x than the first SWAT call-out
Escalating the response faster with real-time information

SirenGPS’ 911 RTA software automatically detects active shooter incidents, terrorist attacks, and other large-scale emergency incidents. SirenGPS has been issued several patents for this software.

**Example:** 911 RTA determines that 911 calls coming from a school indicate an active shooter.
Notifications indicating an elevated risk of a large-scale emergency incident are sent automatically to:

- Public safety leadership
- Mutual aid agencies
- SWAT
- Additional ambulance and fire services
- School leadership
- The school resource officer on site
Automated notifications distribute incident information

**911 RTA** delivers automated notifications of incidents across agency boundaries and jurisdictions with normalized, plain language incident descriptions – without affecting work-flow or protocols.

Manage contact distribution lists to receive notifications triggered by:

- Incident “10 codes” assigned by 911 to identify the emergency
- Large-scale emergency incidents identified by 911 RTA

Notifications delivered through multiple, parallel pathways:

- SMS
- Email
- Call
- Delivery to incident management software
911 is available without charge to public safety to enable a more efficient response to large-scale emergency incidents.

- Delivers faster recognition of mass casualty incidents to start the coordination of resources across a region
- Shares critical information about an incident across disciplines and jurisdictions
- Normalize incident codes across a region without any change at the PSAP
- Requires very limited set up and no training
- **Free of charge to public safety**

“During life saving operations, preparations and recovery efforts, it’s important that members of emergency management teams communicate with one another in real time.” – Pre-Disaster Recovery Planning Guide for State Governments (FEMA) November 2016
Community stakeholder value proposition for 911 RTA

Large-scale emergencies occur in the businesses, schools, hospitals, and places of worship in our communities. With 911 RTA implemented with public safety, these stakeholders can subscribe to the service.

- Community Stakeholders have a compelling set of interests that include protecting their employees, students, clients, property, and reputation
- These stakeholders are the first line of defense and need to know about an attack as it happens
- Situational awareness enables community stakeholders to take appropriate action to protect their interests and support first responders

“70% of active shooter incidents resolve without police intervention.”
— Active Shooter Study Federal Bureau of Investigation (FBI) 2017
Participating agencies retain control of their information

SirenGPS is committed to partnering with public safety and has written safeguards into 911 RTA subscription agreements that put protecting public safety operations, information, and first responders first.

- Community stakeholders may only subscribe to 911 RTA for notification of incidents that impact or originate from a commercial or public property that the subscriber owns, controls, or for which the subscriber provides professional security services.

- MARC public safety agency partners will receive quarterly reports of 911 RTA subscribers with property located within the partner agency’s geographic area.

- Stakeholder subscription agreements include a waiver that extends to MARC and MARC agency partners for claims related to the service, and for 911 RTA subscription payments in the event an agency withdraws authorization.

- 911 RTA stakeholder subscription agreements require non-disclosure to keep incident information in confidence except by court order.
911 RTA setup is simple and secure

911 RTA integrates seamlessly with PSAP operations using a secure gateway appliance.

A secure deployment plan has been cooperatively developed by MARC’s technology team, SirenGPS, and GeoComm, the vendor that provides call routing and GIS services for MARC. Once approved, this plan can be completed in just a few weeks.

Integration with PSAPs that MARC serves can further enhance situational awareness across the MARC’s service area.
Every second counts

Thank you

For more information call 800.570.3807 or visit sirengps.com
911 RTA R&D Introduction

The following provides a brief summary of the potential benefit in rapidly identifying large-scale emergencies like active shooter incidents, and provides general technical explanation for technology that addresses this challenge.

911 RTA Software Automatically Identifies Mass Casualty Incidents in Real Time

911 Real-Time Analytics software (911 RTA) monitors 911 call proximity, frequency, and related data in real-time to identify incidents likely to require an escalated level of emergency response. When 911 RTA identifies a likely mass casualty incident, it automatically notifies leadership, special services and other appropriate stakeholders.

The window of opportunity for law enforcement to intervene in an active shooter incident is typically less than 15 minutes. [Blair & Schweit (2014); ALERRT (2018); National Threat Assessment Center (2019)]. After an attack ends, the demand for first response resources escalates still further as achieving medical intervention for the victims of trauma in the first 60 minutes is critical. [Kotwal, et al. (2015); Pham et al. (2017)]. Despite the urgency of timely escalation of the emergency response, timely incident recognition of mass casualty incidents and the communication of requests for mutual aid and special weapons and tactical (SWAT) takes significantly longer than it would if that process were automated. Based on examination of the timelines for numerous mass casualty incidents, calls for mutual aid and SWAT typically occur ten (10) minutes after the inception of an attack. [Braziel et al. (2018); Lombardo (2018); Tony (2018)].

Recent advances in accurate device location for 911 have made automated incident identification possible for the first time. [Washington Post (2019)]. Where the accuracy of 911 location services for mobile calls is sufficient to identify a precise location, automated threat identification and notification can achieve situational awareness milestones necessary for an escalated emergency response within the first minutes of an attack. 911 RTA can reduce the time it takes to activate SWAT, request help from other agencies, and call for additional emergency medical services, sending an initial incident alert as much as fifty (50) times faster.

911 RTA is deployed by installing a secure communication appliance at the Public Safety Access Point (PSAP) where 911 calls are answered. (See device specifications submitted with this proposal 911RTA-PGA1-IG-EN_1.0.1) The 911 RTA communication appliance transmits 911 call data in real time to the 911 RTA cloud service for analysis. 911 RTA manages this data stream, analyzing incoming information to detect emergent threats, incorporating call information into an experience model that makes the service more efficient in performing threat analysis over time. 911RTA has been developed as a scalable service capable of managing real-time analysis of every 911 operation in the United States, delivering threat notifications to appropriate first responders and stakeholders in real time.

911RTA Key Research and Development Project Objectives

Commercialization of the 911RTA service requires deployment of learning software to evaluate live 911 call data in real time to facilitate the research, development, testing, and commercialization of this technology.
Successful completion of the project will achieve the following technical objectives:

1. Deployment of Prototype Algorithms: Initial development and testing indicates successful threat identification with prototype algorithms that identify potential mass casualty incidents based on the frequency, proximity and location of 911 calls, the history of calls for the caller’s location and for the location type, as well as other factors.

2. False Positive Filters: The project includes deployment and testing of prototype algorithms that apply human checks to filter false positives to less than 5% for calls made from highways and similar heavy traffic areas that tend to generate high call volume for relatively trivial incidents.

3. Consistent Outcomes: Research and development of learning software that enhances human checks to produce more reliable outcomes, exploring the correlation between call location information and call-outs for mutual aid and special weapons and tactical (SWAT).

4. Publication of Test Results: Test results will be prepared in an academically rigorous manner suitable for publication, supporting adoption of the service by public safety agencies.

5. Development of Commercial Sales Portal: Parallel to development and testing of the analytic service, a web portal that allows community stakeholders to manage subscription to the service has also been developed.

**911RTA Commercialization: Technical and Commercial Validation**

911RTA software analyzes 911 calls for patterns in the frequency, timing, and proximity, with calculations that take into consideration certain environmental information. Initial research demonstrates that an algorithmic process can rapidly identify emergent incidents and can be used to generate notifications to facilitate more efficient response outcomes. The purpose of this project is to commercialize this service, supporting a more efficient response in mass casualty incidents.

The technical feasibility of the project has been validated with historic data used to apply algorithmic analysis to past incidents. Initial testing has been performed using simulated data obtained through public records requests submitted to agencies that have answered emergency service calls during incidents identified as “active shooter” attacks by the United States Justice Department Federal Bureau of Investigations (FBI). Agencies were asked to provide a data inventory of twelve months of 911 calls that include the calls for at least one active shooter incident, and to also provide incident documentation sufficient to identify a timeline for situational awareness milestones.

By way of example, Nashville, TN 911 calls were modelled for a period of twelve months from September 24, 2017, a data set which includes two active shooter incidents identified in FBI research. The 911 calls in this data are reasonably well modelled by a time-varying
inhomogeneous spatial Poisson process. The time-varying aspect displays daily and weekly trends. The resulting model was applied to incident call data from other jurisdictions confirming the positive test results.

In order for the identification of an emergent incident to have commercial value to current first responder communications operations, the models are restricted to detecting patterns that are localized in time intervals of five minutes or shorter. This interval represents approximately 50% of the typical time interval required for a 911 dispatch operation to identify that an active shooter incident is occurring and communicate that information to mutual aid and special weapons and tactical (SWAT). The working assumption is that reducing the time to identify and communicate a mass casualty incident as a means of providing a meaningful benefit in view of the ten minutes it takes to achieve the same outcome using current technology. This assumption has been validated through research on past incidents and through presentation to state of the art PSAP operations in sample communities that provide 911 services for populations ranging from 100,000 to 2,500,000 residents.

911RTA Commercialization: Research and Development Timeline

Multiple 911 agencies have been engaged to participate in deployment and testing of the 911 RTA service. The project began by deploying the data collection and cloud services enabled to submit data to test prototype algorithms.

The project will be completed over a period of six months to include concurrent development and of two analytic models implemented through four overlapping software development phases:

1. Initial Implementation: Stand-up of data collection, data environment and analytic process sandbox. (four weeks)
2. Algorithm Model Development: The initial analytic process will be deployed into a real-time data environment with the capability of processing test simulations. Human false positive controls will be implemented. (eighteen weeks)
3. Learnable Model Development: Development and testing of learning models for false positive filtering and active threat identification. (fourteen weeks)
4. Commercial Portal: (six weeks)

The data collection tasks included in the initial implementation of the project were completed in advance of the start of the research phase as implementation with agencies is aligned through negotiation and integration with vendors and agency personnel. While refinement of the models is ongoing, the initial deployment and testing was completed in November of 2019.

Primary Research and Development Activities

The research and development project’s goals fall into a wide area of pattern recognition and classification, in which incoming patterns in the data must be classified (in this case in real time) into categories of events, given a classification model. Addressing all calls corresponding to actual incidents is of paramount importance, with simultaneous minimization of a number of false positives.
Contemporary classification problems are solved effectively by models from two main categories: the so called “hand-crafted” approaches, which incorporate human expertise and knowledge about the task into the classifier’s design process, and “data-driven” (or “learnable”) models, which approximate the classification functions directly from data, often without strict assumptions on the classification boundaries (like in -- recently popular -- deep learning). While there is debate regarding which models are best in general, there is some consensus that for pattern recognition solutions like this one an ensemble approach that incorporates a hand-crafted model with a learnable model is the superior approach.

Classifiers put into ensemble may work independently in a multi-expert framework, in which all experts’ opinions are fused (usually through voting) to make a final decision [Kuehlkamp-etal-TIFS-2019]. However, a particular case of ensemble classification, which proved to be extremely effective in computer vision, is stacking the classifiers into a cascade [Viola-and-Jones-CVPR-2001]. While the first model in the cascade is designed in isolation, the next tiers make use of the output of the preceding classifiers. This organization of classification pipeline into tiers allows for gradually eliminating false positives.

The cascaded classification approach is a fit for processing 911 call information as this approach aligns with the real-time development of 911 call information. The first element of a cascade will deploy a statistical model tuned to reliably identify 911 calls that need to be quickly processed, with a higher probability of returning false positives. The second stage in the cascade will be based on learnable model that will accept the initial output and will be trained to filter out false positives more effectively. The introduction of learning capability enables the system to adapt on-line to changing circumstances in real-time.

In addition to alignment with the data structure, a cascaded framework has relatively low implementation risk: it has been researched for almost two decades, executes fast enough to provide real-time output, and has proven successful deployed in various commercial pattern recognition tasks.

The goal of the first element of the cascaded classification approach is to identify call patterns which are highly localized in both time and space to an extent which is statistically unlikely based on the historical intensity function associated with the Poisson process. As indicated above, for the identification of an emergent incident to have commercial value, the models are restricted to detecting patterns that are localized in time intervals of five minutes or shorter. However, the proposed algorithm is robust to modifying this interval. Application to historic incident data suggests that the process can achieve incident identification four (4) times more quickly than is typically achieved using current technology and protocols, delivering situational awareness alerts to activate SWAT and mutual aid fifty (50) times more quickly.

The initial analytic process partitions the geographic space domain into small regions where it is unlikely that many 911 calls will originate from that region in a five minute (or shorter) period. Calls in a region are flagged as a potential incident if the number of calls in a given period is greater than a threshold. The initial size of regions and threshold are determined by assuming that the underlying process for generating calls is Poisson. It is important to estimate the intensity function accurately in order to obtain accurate regions and thresholds. The size of regions may
vary over time, because the regions need to be constructed in such a way that the threshold frequency of 911 calls is highly unlikely.

Each incident that is flagged as unlikely will then be passed through a human generated check to identify false positives based on observational information and/or third-party information. These checks are likely to include lists of known automated alarm calls, the National Oceanic and Atmospheric Administration (NOAA), the US Geologic Survey (USGS) and similar reliable sources of real-time information on natural disasters, tornados, earthquakes and other risks, as well as controls to limit false positives from highway traffic incidents and alarm systems, any of which could be responsible for generating a high volume of 911 calls.

Flagged incidents not identified as false positives by human generated checks will be passed on to a learning false positive identification model as the next stage of the classification cascade. Several classifiers may be considered at this stage, including recurrent neural networks (due to their inherent capabilities of processing time series data) and shallow convolutional neural networks. Popular deep architectures will be evaluated as a tertiary alternative for this project, since the training of such structures that would prevent overfitting (i.e., would offer good generalization on unknown incidents) requires more data about past incidents than available for this task. Highly imbalanced class representations are anticipated, for instance the number of active shooter incidents is expected to be smaller than the number of car accidents. The team at the University of Notre Dame has a substantial research record in addressing classification problems for unbalanced data, using techniques such as SMOTE [Chawla-et al-JAIR-2002], which will be considered in this project, if appropriate.

In the course of further development, it is anticipated that dynamic parameters may be required to partition a given 911 area into sub-regions such that localized calls in time are unlikely for each sub-region separately. Unbounded partition creation could result in some instances where localized calls are unlikely in any sub-region. The working assumption is that partitions aligned with property use will result in optimal outcomes. We have proven a theoretical result that if the overall rate of the Poisson process is $\Lambda$, and we partition the spatial region into $N$ sub-regions, each with rate $\Lambda/N$, then the probability of observing $r$ or more events in any of the sub-regions behaves like $N^{1-r}$. In particular, we have theoretical guarantees that we can control the system-wide false positive rate, as long as $r$ is at least 2; that is, as long as our flags consist of two or more calls in a time period.

Second, we estimate the intensity function of the spatial Poisson process. Based on initial analysis of the data, we use different estimates for the intensity function for each hour period of the week, totaling up to 168 estimates. In particular, we assume that the intensity function is constant across each hour period. We anticipate that not all 168 estimates will be significantly different. We will also hand create models for holidays days such as July 4 that have historically shown an impact on 911 call behavior. With the assumption that intensity does not vary over each hour period, this enables estimation of the intensity function on that hour period by locating all calls during that hour period and using standard techniques, e.g. Gaussian smoothing, wavelets [Donoho-et al-AS-1996] or other multi-scale estimation, or k nearest neighbors [Ellison-et al-JABES-2014], to estimate the intensity associated with those points. Computationally, a dyadic partition alternating vertical and horizontal splits into a set of sub-regions with approximately equal equal rates will be the first method implemented. Other methods that require more
steps to both accurately estimate the intensity function and split into sub-regions with equal rates in a computationally efficient way will be developed as necessary. Multiple models will enable cross-validation and simulated data to select for superior model(s).

Because it is very unlikely that 911 call data will conform to pure Poisson process, the potential for deviance from Poisson will also be explored. Many times, when differences exist, they exist in the tails of the distribution. Incident tails will be flagged for further analysis and development of controls. This process will involve cross-validation with simulated and live data to minimize the false positive rate, determining sub-regions that are large enough to likely contain all calls from a single active shooter incident. While it is anticipated that a limited rate of false positives will survive this this stage in the development of the detection algorithm, initial testing indicates that an operationally reliable level of incident identification will be achieved.

**Further Potential Investigation Activities**

As mentioned above, a two staged research and development path to deployment of the cascaded analysis approach described will include learnable models and is expected to achieve a commercially appropriate discrimination between actual events and false positives. Further investigation of the flagged events may be appropriate to eliminate a higher percentage of false positives, and to enable the learning model to account for environmental information.

An issue anticipated to develop more fully in live data is that, while the overall trend of 911 calls is approximately Poisson, tail events are significant. These often follow a different distribution than the general trend, making it more difficult to accurately control the false positive error rate. It may be necessary to adjust the sub-area partition based on data coming in so as to minimize the false positive rate. A later stage analysis will consider flagging calls in order to characterize urgency. This analysis will be based on geo-location data, the FBI database of likely targets, and by examining the call patterns from past events as they become available.

Anecdotal evidence suggests potentially significant differences between the pattern, practice and experience from one community to the next. Development and testing will validate the use of learning models to adapt the application of 911 RTA algorithmic pattern analysis to reliably identify emergent incidents in a manner that accounts for environmental factors.

**Initial Implementation and Live Testing**

While preliminary research on past active shooter incidents indicates that 911 RTA can reliably identify an emergent incident in the first moments of an attack, additional work is required to refine the process to differentiate outcomes and calculate probability. Development and testing will confirm the reliability of pattern analysis. As outcomes have been validated and perform reliably, these services will be operationally deployed with first responder agencies, by implementing situational awareness alerts in alignment with local communication protocols. This is accomplished by associating each participating agency with a geofence that defines the area of that agency’s responsibility for alert delivery and providing those agencies with a web page that allows administrators from each agency to manage alert delivery methods and distribution.


12. Lombardo, Joseph, Sheriff. (2018) *Report from the Las Vegas Metropolitan Police Department’s Force Investigation Team on the shooting that occurred on October 1, 2017, at 3901 S. Las Vegas Boulevard at the Route 91 Harvest music festival.* Las Vegas Metropolitan Police Department. Las Vegas, NV.


SIRENGPS SERVICE AGREEMENT

This Service Agreement (This Agreement) is entered into by and between The City (City) – an entity authorized under the statutes of the State of Missouri. (“Service Recipient”, “Client” or “Community”) and SirenGPS, Inc. a company registered in the State of Delaware, with its principal place of business at 9272 Olive Boulevard, St. Louis, MO 63132 (“SirenGPS”), collectively the “Parties”.

The Effective Date for Services under This Agreement is: December 1, 2019

Services Included Under This Agreement:
911 Real-Time Analytics (911 RTA) integrates with 911 telecommunications hardware and/or software to monitor emergency communication, identify significant incidents, and provide notifications of those incidents. Service to be configured onsite and via web-based services.

License Fee and Service Details:
SirenGPS will provide the following services for a License Fee(s) as follows:
SirenGPS will provide 911 RTA services at no charge for the first twelve (12) months. Services will continue at the same rate for as long as SirenGPS is authorized to accept subscriptions for the 911 RTA service from private entities approved by the City.

Geofences: Six (6)
Seats: twelve (12)
SirenGPS account manager will review incident code, geofence and contact information with a representative from the client to confirm alignment with current operations, personnel and permissions.

One Time or Other Fees(s): None
Third Party Communication Fees: No Charge
SMS, email, voice charges and integration via API with one external system is Included.

Additional Terms and Conditions:
The Parties understand and agree that this Agreement incorporates the SIRENGPS 911RTA SERVICE AGREEMENT TERMS AND CONDITIONS (TOS) and the SIRENGPS SERVICE LEVEL AGREEMENT (SLA) available for review at https://sirengps.com/misc/contract-documents.

X_____________________________ X_________________________
SirenGPS, Inc. City
SIRENGPS SUPPORT AND MAINTENANCE AGREEMENT (SLA)

1. OVERVIEW

Subject to compliance in all material aspects with the Service Agreement between SirenGPS and the Service Recipient (Client), SirenGPS will maintain and support its service(s) and application(s) in a consistent and clear manner, pursuant to this Service Level Agreement (SLA). For purposes of this SLA, “services and applications” shall mean SirenGPS web-based Service availability and Service operation and, except as otherwise expressly detailed below, it is not intended to include any minimum standards for third party response times, message deliveries, third party map interface quality, Internet or communication provider performance or a guaranty of any other third party’s performance associated with any SirenGPS Service(s). Additionally, while SirenGPS Services are intended to assist in providing proper communication during a crisis, SirenGPS cannot take and does not assume any responsibility for the effectiveness of Services when and if triggered during such a crisis or at any other time. SirenGPS shall maintain its web-based Service Offerings to function as designed, intended and represented and will maintain the product to a Sigma 6 standard for availability. Where Client’s inability to access the Service is the result of failure or lack of availability or performance of systems, processes or other instrumentality not under SirenGPS direct control this shall not be deemed a Service outage or result in recognized down-time. Input or suggestions provided by SirenGPS during Service set-up and/or configuration shall not be construed as advice, guidance or a guaranty of success. Client remains ultimately responsible for its use of the Service, for the setup and configuration of the Service. This SLA is only intended to set forth the support and maintenance obligations of SirenGPS vis-à-vis its back-end infrastructure that is intended to enable proper communication when and if necessary.

SirenGPS will make any changes to its applications accurately, under a controlled procedure and in a confined development and testing environment specifically maintained for this purpose. SirenGPS will take the necessary steps and procedures to assure that deployment of new changes will not change the level of service. SirenGPS monitors both the frequency and the nature of service problems and takes action to implement changes to reduce or eliminate recurring problems.

Except with respect to end-user software customer service, SirenGPS is to work only with Client designated administrators and technical contacts.

2. PROCEDURES & SERVICE LEVELS

2.1 Problem Reporting Procedure

Service Recipient may report problems to the SirenGPS Technical Support group by email and phone.

<table>
<thead>
<tr>
<th>Standard support</th>
<th>Email</th>
<th>Support hours</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="mailto:support@sirengps.com">support@sirengps.com</a></td>
<td>(800) 570.3807 ext 1 9:00 am and 6:00 pm Central Time during normal business, non-holiday days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emergency support</th>
<th>Email</th>
<th>Support hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Excludes application related support]</td>
<td>PLEASE CALL, DO NOT EMAIL</td>
<td>(800) 570.3807 ext 1 24/7 basis for those matters determined to be urgent, as noted in the table below.</td>
</tr>
</tbody>
</table>

Please leave a clear message with your contact details, and a support representative will contact you within 30 minutes.

All requests for service should include the Client name, a description of the problem, email address, name and telephone number of the Service Recipient contact person.
Please provide as much information about the problem as possible. A Technical Support Specialist will contact Client by either a return e-mail or a return phone call – or as otherwise requested – and will confirm that SirenGPS has received and logged the problem and the Client representative contact information.

The SirenGPS Technical Support Specialist will work with the Client contact to resolve the problem, to the extent that it is determined in good faith that the problem is beyond the remedial capabilities of Client. If the problem cannot be resolved in a short period of time by phone or email, the Technical Support Specialist will keep Service Recipient informed as to the progress.

When the problem has been resolved, the Client will be notified by email and the service request will be closed on SirenGPS's records.

### 2.2 Call Priority Commitments

The following are the SirenGPS response commitments for answering calls and evaluating priority:

<table>
<thead>
<tr>
<th>SirenGPS Priority</th>
<th>SirenGPS Definition</th>
<th>Guideline</th>
<th>Response Time</th>
<th>Resolution Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical</td>
<td>Major server or applications failure with system unavailable.</td>
<td>Within 2 hours</td>
<td>within 4 hours</td>
</tr>
<tr>
<td>2</td>
<td>Major</td>
<td>Medium function or service affected with restricted availability and some User impact.</td>
<td>Within 2 – 4 hours</td>
<td>within 2 working days</td>
</tr>
<tr>
<td>3</td>
<td>Minor</td>
<td>Minor function or service affected with minor impact and system still available/functional.</td>
<td>Within 1 working day.</td>
<td>within 7 working days</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Low priority background task. System and functionality are available.</td>
<td>Within 1 working day</td>
<td>By agreement</td>
</tr>
</tbody>
</table>

**Note:** "Response Time" is defined as the initial investigation of the problem and the gathering of any necessary data. It is the initiation of the resolution and not necessarily the time it takes to fix the problem.

### 2.3 Scheduled maintenance:

**Regular:** In the event that SirenGPS must perform scheduled maintenance that will impact service, SirenGPS will notify Client through the contact identified for that purpose. Scheduled maintenance is infrequent and typically does not affect the availability of the web-based infrastructure. Scheduled maintenance will be no greater than an average of 4 hours per month to a maximum of 48 hours per year, and will not exceed 7 hours in any calendar month.

**Urgent Maintenance:** SirenGPS may perform urgent maintenance at its detection center. SirenGPS will endeavor to notify Client 24 hours prior to urgent maintenance at the email address set forth above. Urgent maintenance will not exceed 4 hours per calendar month and will be calculated as part of the scheduled maintenance.
2.4 Problem Escalation Procedure

Problem escalation defines the procedure in place to identify high priority issues and make senior people aware so that additional resources, if necessary, can be used to help resolve an urgent problem. This is for use on those occasions where a problem is significantly affecting Client’s access to the service(s) and the current action being taken does not appear to be producing a resolution quickly enough.

The table below identifies those people who will be contacted if a call has not been resolved by the elapsed time shown (elapsed time being time beyond that committed to by SirenGPS in the table above):

<table>
<thead>
<tr>
<th>SirenGPS Priority</th>
<th>SirenGPS Definition</th>
<th>Guideline</th>
<th>Escalation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical</td>
<td>Major server or applications failure with system unavailable.</td>
<td>1 hr: SirenGPS Tech Support Mgr and IT Team 2 hrs: VP/CTO</td>
</tr>
<tr>
<td>2</td>
<td>Major</td>
<td>Medium function or service affected with restricted availability and some User impact.</td>
<td>2 hrs: SirenGPS Tech Support Mgr and IT Team 4 hrs: VP/CTO</td>
</tr>
<tr>
<td>3</td>
<td>Minor</td>
<td>Minor function or service affected with minor impact and system still available.</td>
<td>2 days: SirenGPS Tech Support Mgr and IT Team 5 days: VP/CTO</td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Low priority background task.</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

If there is a dispute as to whether a matter is “urgent” or “very urgent”, then the parties shall escalate the matter to the respective CEOs/Presidents of each company.

3. Uptime Guarantee of 99.95% or Greater

SirenGPS shall make every effort to provide its cloud-based service available via the internet through a browser-based portal on a 24/7/365 basis. In the event that the Client is unable to access the service due to the service being “down” for a period of time that represents a portion of the Service Period that exceeds this uptime guarantee, SirenGPS shall apply a discount to the next periodic Subscription Charge as follows:

<table>
<thead>
<tr>
<th>Uptime</th>
<th>Discount</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;99.95%</td>
<td>5%</td>
</tr>
<tr>
<td>&lt;99%</td>
<td>20%</td>
</tr>
<tr>
<td>&lt;95%</td>
<td>100%</td>
</tr>
<tr>
<td>Year</td>
<td>Console</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>2017</td>
<td>Console 01</td>
</tr>
<tr>
<td></td>
<td>Console 02</td>
</tr>
<tr>
<td></td>
<td>Console 03</td>
</tr>
<tr>
<td></td>
<td>Console 04</td>
</tr>
<tr>
<td></td>
<td>Console 05</td>
</tr>
<tr>
<td>2018</td>
<td>Console 01</td>
</tr>
<tr>
<td></td>
<td>Console 02</td>
</tr>
<tr>
<td></td>
<td>Console 03</td>
</tr>
<tr>
<td></td>
<td>Console 04</td>
</tr>
<tr>
<td></td>
<td>Console 05</td>
</tr>
<tr>
<td>2019</td>
<td>Console 01</td>
</tr>
<tr>
<td></td>
<td>Console 02</td>
</tr>
<tr>
<td></td>
<td>Console 03</td>
</tr>
<tr>
<td></td>
<td>Console 04</td>
</tr>
<tr>
<td></td>
<td>Console 05</td>
</tr>
</tbody>
</table>

### Leavenworth Police Department

<table>
<thead>
<tr>
<th>Year</th>
<th>Console</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Console 01</td>
<td>294</td>
<td>277</td>
<td>342</td>
<td>277</td>
<td>376</td>
<td>342</td>
<td>259</td>
<td>223</td>
<td>288</td>
<td>243</td>
<td>228</td>
<td>287</td>
<td>3,436</td>
</tr>
<tr>
<td></td>
<td>Console 02</td>
<td>198</td>
<td>227</td>
<td>302</td>
<td>229</td>
<td>268</td>
<td>303</td>
<td>241</td>
<td>246</td>
<td>291</td>
<td>216</td>
<td>155</td>
<td>283</td>
<td>2,959</td>
</tr>
<tr>
<td></td>
<td>Console 03</td>
<td>413</td>
<td>435</td>
<td>477</td>
<td>483</td>
<td>563</td>
<td>526</td>
<td>681</td>
<td>539</td>
<td>583</td>
<td>522</td>
<td>563</td>
<td>473</td>
<td>6,258</td>
</tr>
<tr>
<td></td>
<td>Console 04</td>
<td>557</td>
<td>426</td>
<td>439</td>
<td>562</td>
<td>526</td>
<td>616</td>
<td>646</td>
<td>567</td>
<td>559</td>
<td>527</td>
<td>459</td>
<td>405</td>
<td>6,289</td>
</tr>
<tr>
<td></td>
<td>Console 05</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2018</td>
<td>Console 01</td>
<td>218</td>
<td>158</td>
<td>176</td>
<td>166</td>
<td>268</td>
<td>129</td>
<td>118</td>
<td>295</td>
<td>151</td>
<td>54</td>
<td>31</td>
<td>90</td>
<td>1,854</td>
</tr>
<tr>
<td></td>
<td>Console 02</td>
<td>151</td>
<td>150</td>
<td>143</td>
<td>118</td>
<td>143</td>
<td>125</td>
<td>127</td>
<td>216</td>
<td>140</td>
<td>56</td>
<td>16</td>
<td>4</td>
<td>1,389</td>
</tr>
<tr>
<td></td>
<td>Console 03</td>
<td>577</td>
<td>570</td>
<td>639</td>
<td>673</td>
<td>726</td>
<td>753</td>
<td>872</td>
<td>800</td>
<td>695</td>
<td>726</td>
<td>666</td>
<td>573</td>
<td>8,270</td>
</tr>
<tr>
<td></td>
<td>Console 04</td>
<td>537</td>
<td>471</td>
<td>501</td>
<td>639</td>
<td>670</td>
<td>724</td>
<td>831</td>
<td>810</td>
<td>728</td>
<td>720</td>
<td>766</td>
<td>696</td>
<td>8,093</td>
</tr>
<tr>
<td></td>
<td>Console 05</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>2019</td>
<td>Console 01</td>
<td>230</td>
<td>308</td>
<td>202</td>
<td>262</td>
<td>300</td>
<td>239</td>
<td>651</td>
<td>732</td>
<td>701</td>
<td>2,499</td>
<td>6,124</td>
<td>6,124</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Console 02</td>
<td>146</td>
<td>158</td>
<td>163</td>
<td>171</td>
<td>191</td>
<td>184</td>
<td>178</td>
<td>93</td>
<td>184</td>
<td>158</td>
<td>1,626</td>
<td>1,626</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Console 03</td>
<td>516</td>
<td>450</td>
<td>542</td>
<td>525</td>
<td>601</td>
<td>658</td>
<td>157</td>
<td>114</td>
<td>123</td>
<td>114</td>
<td>3,800</td>
<td>3,800</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Console 04</td>
<td>430</td>
<td>417</td>
<td>585</td>
<td>267</td>
<td>685</td>
<td>596</td>
<td>657</td>
<td>750</td>
<td>693</td>
<td>589</td>
<td>5,669</td>
<td>5,669</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Console 05</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
### Mid-America Regional Council

#### Call Count By Console | 2018

<table>
<thead>
<tr>
<th>County</th>
<th>Position Name</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leavenworth</td>
<td>Fort Leavenworth Provost Marshal</td>
<td>163</td>
<td>89</td>
<td>100</td>
<td>91</td>
<td>108</td>
<td>94</td>
<td>89</td>
<td>99</td>
<td>105</td>
<td>71</td>
<td>69</td>
<td>81</td>
<td>1,159</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Leavenworth</td>
<td>76</td>
<td>78</td>
<td>116</td>
<td>106</td>
<td>155</td>
<td>115</td>
<td>107</td>
<td>107</td>
<td>145</td>
<td>96</td>
<td>128</td>
<td>90</td>
<td>1,313</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Johnson</td>
<td>1,936</td>
<td>1,125</td>
<td>1,057</td>
<td>1,023</td>
<td>1,225</td>
<td>1,367</td>
<td>1,403</td>
<td>1,507</td>
<td>1,264</td>
<td>1,262</td>
<td>607</td>
<td>1,063</td>
<td>14,839</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Wyandotte</td>
<td>2,922</td>
<td>1,785</td>
<td>1,508</td>
<td>1,435</td>
<td>1,646</td>
<td>1,698</td>
<td>1,829</td>
<td>1,769</td>
<td>1,739</td>
<td>1,807</td>
<td>1,601</td>
<td>1,550</td>
<td>21,289</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Clay</td>
<td>150</td>
<td>658</td>
<td>1,263</td>
<td>1,217</td>
<td>1,355</td>
<td>862</td>
<td>1,549</td>
<td>1,668</td>
<td>1,786</td>
<td>1,618</td>
<td>1,931</td>
<td>1,334</td>
<td>15,411</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Cass</td>
<td>131</td>
<td>970</td>
<td>1,725</td>
<td>1,629</td>
<td>2,046</td>
<td>1,855</td>
<td>1,960</td>
<td>2,206</td>
<td>1,906</td>
<td>2,035</td>
<td>2,269</td>
<td>1,657</td>
<td>20,389</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Leavenworth</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Platte</td>
<td>893</td>
<td>633</td>
<td>872</td>
<td>776</td>
<td>1,045</td>
<td>624</td>
<td>666</td>
<td>1,427</td>
<td>758</td>
<td>371</td>
<td>161</td>
<td>433</td>
<td>8,659</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Ray</td>
<td>639</td>
<td>527</td>
<td>630</td>
<td>461</td>
<td>510</td>
<td>565</td>
<td>560</td>
<td>1,009</td>
<td>702</td>
<td>293</td>
<td>126</td>
<td>69</td>
<td>6,091</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Miami</td>
<td>2,009</td>
<td>1,925</td>
<td>2,214</td>
<td>2,248</td>
<td>2,353</td>
<td>2,308</td>
<td>3,179</td>
<td>2,882</td>
<td>2,834</td>
<td>3,255</td>
<td>3,125</td>
<td>2,407</td>
<td>30,739</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Leavenworth</td>
<td>1,745</td>
<td>1,723</td>
<td>1,795</td>
<td>2,047</td>
<td>2,116</td>
<td>2,261</td>
<td>2,931</td>
<td>2,856</td>
<td>2,786</td>
<td>3,088</td>
<td>3,001</td>
<td>3,013</td>
<td>29,362</td>
</tr>
<tr>
<td>County Sheriff's Office</td>
<td>Leavenworth</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>37</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>10,664</td>
<td>9,514</td>
<td>11,281</td>
<td>11,035</td>
<td>12,561</td>
<td>11,749</td>
<td>14,321</td>
<td>15,579</td>
<td>13,981</td>
<td>13,930</td>
<td>12,981</td>
<td>11,731</td>
<td>149,327</td>
<td></td>
</tr>
</tbody>
</table>
### Mid-America Regional Council

**Call Count By Console | 2019**

#### State
- KS: 91,457 (3.81%)
- MO: 0%

#### County
- Jackson: 1,259,124
- Johnson: 450,028
- Clay: 176,724
- Cass: 150,993
- Wyandotte: 143,119
- Leavenworth: 91,457
- Platte: 78,198
- Ray: 39,179
- Miami: 9,383

#### Call Volume
- Total: 91,457

#### State Call Volume
- KS: 91,457 (3.81%)
- MO: 0%

#### County Call Volume
- Jackson: 1,259,124
- Johnson: 450,028
- Clay: 176,724
- Cass: 150,993
- Wyandotte: 143,119
- Leavenworth: 91,457
- Platte: 78,198
- Ray: 39,179
- Miami: 9,383

#### Call Count By Console

<table>
<thead>
<tr>
<th>PSAP</th>
<th>Position Name</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fort Leavenworth Provost Marshal</td>
<td>Position 01</td>
<td>80</td>
<td>82</td>
<td>85</td>
<td>102</td>
<td>99</td>
<td>85</td>
<td>108</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>641</td>
</tr>
<tr>
<td>Fort Leavenworth Provost Marshal</td>
<td>Position 02</td>
<td>87</td>
<td>83</td>
<td>105</td>
<td>108</td>
<td>113</td>
<td>104</td>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>700</td>
</tr>
<tr>
<td>Leavenworth County Sheriff's Office</td>
<td>Position 01</td>
<td>1,180</td>
<td>1,161</td>
<td>1,039</td>
<td>1,258</td>
<td>1,475</td>
<td>1,453</td>
<td>1,445</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9,011</td>
</tr>
<tr>
<td>Leavenworth County Sheriff's Office</td>
<td>Position 02</td>
<td>1,517</td>
<td>1,397</td>
<td>1,764</td>
<td>1,651</td>
<td>1,879</td>
<td>1,667</td>
<td>1,668</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11,543</td>
</tr>
<tr>
<td>Leavenworth County Sheriff's Office</td>
<td>Position 03</td>
<td>1,533</td>
<td>1,354</td>
<td>1,491</td>
<td>1,567</td>
<td>1,804</td>
<td>1,525</td>
<td>1,506</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10,780</td>
</tr>
<tr>
<td>Leavenworth County Sheriff's Office</td>
<td>Position 04</td>
<td>1,871</td>
<td>1,774</td>
<td>2,087</td>
<td>2,043</td>
<td>2,262</td>
<td>2,318</td>
<td>2,076</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14,431</td>
</tr>
<tr>
<td>Leavenworth County Sheriff's Office</td>
<td>Position 05</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Leavenworth Police Department</td>
<td>Position 01</td>
<td>1,169</td>
<td>1,402</td>
<td>1,313</td>
<td>399</td>
<td>1,495</td>
<td>1,240</td>
<td>2,585</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9,603</td>
</tr>
<tr>
<td>Leavenworth Police Department</td>
<td>Position 02</td>
<td>816</td>
<td>867</td>
<td>870</td>
<td>905</td>
<td>998</td>
<td>1,007</td>
<td>933</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6,396</td>
</tr>
<tr>
<td>Leavenworth Police Department</td>
<td>Position 03</td>
<td>1,898</td>
<td>1,713</td>
<td>2,053</td>
<td>1,982</td>
<td>2,280</td>
<td>2,602</td>
<td>832</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>13,360</td>
</tr>
<tr>
<td>Leavenworth Police Department</td>
<td>Position 04</td>
<td>1,913</td>
<td>1,688</td>
<td>2,233</td>
<td>1,885</td>
<td>2,471</td>
<td>2,313</td>
<td>2,478</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14,981</td>
</tr>
<tr>
<td>Leavenworth Police Department</td>
<td>Position 05</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>12,065</td>
<td>11,521</td>
<td>13,040</td>
<td>11,900</td>
<td>14,877</td>
<td>14,315</td>
<td>13,739</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>91,457</td>
</tr>
</tbody>
</table>
The Public Safety Board voted to eliminate the consortium membership fees for the 11 counties within the MARC region. Training will be paid by each county’s membership fees for all 667 dispatchers. This will include the newly revamped in-person classroom curriculum that has four new training tracks (FIRE/EMS, POLICE, GENERAL, WELLNESS) that will launch January 1, 2020. The new curriculum will be taught by superstar instructors from within our region who serve as subject matter experts at conferences all over the United States. We are still looking for more, so if you know of one, please send his or her contact information to Pam Opoka: popoka@marc.org. MARC membership also includes the new online training platform from Power Phone that will feature 18 (45-60 minute) modules per year. These modules are officially accepted by International Academy Emergency Dispatch for Emergency Medical Dispatch Continuing Education Units. Additionally, membership includes select GTI classes.

For partner members (other than PSAPs) inside or outside the MARC region, training memberships include MARC’s in-person classroom with four new training tracks and select GTI classes. It will not include the online training platform from Power Phone. This is a premium value for only $200 per position! This fee is paid annually based on the PSAP’s fully staffed position number.

Registration:

The website will have different language to include three registration options:

- **MARC 911 System Member** (select County in drop-down menu)

  Please select this option if you are in a PSAP within the MARC region and have PSAP equipment serviced by MARC 911 Technicians.

- **Partner Member**

  Please select this option if you are in a PSAP within the MARC region, but DO NOT have PSAP equipment serviced by MARC 911 Technicians.

- **Other Registrant**

  Please select this option if you are outside the MARC region.

Class Fees:

- 3-4 hours $50
- 8 hours $100
- APCO CTO 3-days $107
- APCO Basic 40-hour Telecommunicator (PST1) 5-days $107
Public Safety Communications Board,

When I prepared the budget, I made a mistake in personnel costs. In 2019 we adjusted personnel cost to support the actual work being done under the GTI contract by the Training Coordinator and two support staff. We were charging 80% of one salary and 20% of a second to the GTI contract. When I calculated the 2020 budget, I added the Training Coordinator to our personnel cost, but failed to adjust the support staff positions back to 100%.

The total approved budget for 2020 is $8,876,317 including a Coordination cost of $1,849,910. When calculating the personnel cost correctly the 2020 total budget should be $8,974,739 including a Coordination of cost $1,948,332.

The amount of the error is $98,422.

We are requesting an adjustment to the personnel section of the 911 Coordination budget in the amount of $98,422.

I have included a new Jurisdiction Cost document in the agenda packet.

Michael Daniels
Public Safety Communications Planning and Administrative Manager
### Approved 2020 MARC 911 Budget

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Population</th>
<th>Percent of Regional Population</th>
<th>2020 Allocation (% of population x $8,876,317)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atchison County, Kan.</td>
<td>16,924</td>
<td>0.83%</td>
<td>73,604</td>
</tr>
<tr>
<td>Cass County, Mo.</td>
<td>99,478</td>
<td>4.87%</td>
<td>432,639</td>
</tr>
<tr>
<td>Clay County, Mo.</td>
<td>211,013</td>
<td>10.34%</td>
<td>917,716</td>
</tr>
<tr>
<td>Douglas County, Kan.</td>
<td>110,826</td>
<td>5.43%</td>
<td>481,993</td>
</tr>
<tr>
<td>Jackson County, Mo.</td>
<td>674,158</td>
<td>33.03%</td>
<td>2,931,977</td>
</tr>
<tr>
<td>Johnson County, Kan.</td>
<td>544,179</td>
<td>26.66%</td>
<td>2,366,686</td>
</tr>
<tr>
<td>Leavenworth County, Kan.</td>
<td>70,345</td>
<td>3.45%</td>
<td>305,937</td>
</tr>
<tr>
<td>Miami County, Kan.</td>
<td>32,787</td>
<td>1.61%</td>
<td>142,594</td>
</tr>
<tr>
<td>Platte County, Mo.</td>
<td>89,322</td>
<td>4.38%</td>
<td>388,470</td>
</tr>
<tr>
<td>Ray County, Mo.</td>
<td>23,336</td>
<td>1.14%</td>
<td>101,490</td>
</tr>
<tr>
<td>Wyandotte County, Kan.</td>
<td>157,505</td>
<td>7.72%</td>
<td>685,004</td>
</tr>
<tr>
<td>City of Excelsior Springs, Mo.</td>
<td>11,084</td>
<td>0.54%</td>
<td>48,205</td>
</tr>
</tbody>
</table>

**REGIONAL TOTALS** 2,040,957 100% $8,876,317

### Amended 2020 MARC 911 Budget

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Population</th>
<th>Percent of Regional Population</th>
<th>2020 Allocation (% of population x $8,876,317)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atchison County, Kan.</td>
<td>16,924</td>
<td>0.83%</td>
<td>74,420</td>
</tr>
<tr>
<td>Cass County, Mo.</td>
<td>99,478</td>
<td>4.87%</td>
<td>437,437</td>
</tr>
<tr>
<td>Clay County, Mo.</td>
<td>211,013</td>
<td>10.34%</td>
<td>927,892</td>
</tr>
<tr>
<td>Douglas County, Kan.</td>
<td>110,826</td>
<td>5.43%</td>
<td>487,337</td>
</tr>
<tr>
<td>Jackson County, Mo.</td>
<td>674,158</td>
<td>33.03%</td>
<td>2,964,488</td>
</tr>
<tr>
<td>Johnson County, Kan.</td>
<td>544,179</td>
<td>26.66%</td>
<td>2,392,929</td>
</tr>
<tr>
<td>Leavenworth County, Kan.</td>
<td>70,345</td>
<td>3.45%</td>
<td>309,329</td>
</tr>
<tr>
<td>Miami County, Kan.</td>
<td>32,787</td>
<td>1.61%</td>
<td>144,175</td>
</tr>
<tr>
<td>Platte County, Mo.</td>
<td>89,322</td>
<td>4.38%</td>
<td>392,777</td>
</tr>
<tr>
<td>Ray County, Mo.</td>
<td>23,336</td>
<td>1.14%</td>
<td>102,616</td>
</tr>
<tr>
<td>Wyandotte County, Kan.</td>
<td>157,505</td>
<td>7.72%</td>
<td>692,600</td>
</tr>
<tr>
<td>City of Excelsior Springs, Mo.</td>
<td>11,084</td>
<td>0.54%</td>
<td>48,205</td>
</tr>
</tbody>
</table>

**REGIONAL TOTALS** 2,040,957 100% $8,974,739
**Financial Update**

Third Quarter Budget:

- May: $567,509.47
- June: $569,370.42
- July: $561,894.94
- August: $550,528.52
- **Total**: $2,249,303.35

Third Quarter Expenses:

- Telephone: $718,375.13
- Language Line: $19,411.14
- 9-1-1 SS7: $12,687.76
- Metro GIS: $83,984.76
- 9-1-1 GTI: $57,351.32
- 9-1-1 Coordination: $536,429.32
- Equipment/Capital Projects: $515,577.36
- Contingency Fund/Cap. Proj.: $10,311.68
- RAMBIS Maintenance: $39,965.70
- 9-1-1 Equipment Maintenance: $239,180.92
- Cost Share Expenses: $12,338.48

**Equipment Replacement Fund Balance**

- $458,341.34

**Outreach Update**

- School programs coordinated:
  - The Cell Phone Sally school program has been provided to 5,000 students at 40 schools in the region. Lee’s Summit Fire Department has presented the program to all 18 elementary schools in the district.
  - Thank you to Kansas City Mo. Police Department, Johnson County ECC, Douglas County, Cass County, Platte County, Miami County and Sugar Creek Police Department for making the time to provide presentations
- Call for nominations for Outstanding Performance Awards (OPAs) has begun. The deadline for submitting nominations is January 31. Saralyn is the contact person for OPAs.

**Additional information to share:**

- Save the Date for the 23rd Annual Telecommunicators Appreciation Celebration on April 17, 2020 at the InterContinental Hotel on the Country Club Plaza. Registration will open February 1.
- Don’t forget to nominate your 911 Hero’s