Date:       Wednesday, September 18, 2019  
Time:      1:00 p.m.  
Location:  Board Room

Agenda

1) Call to Order and Introductions

2) Approval of June 26, 2019 meeting summary

3) 2020 Regional 911 Budget  
   a) Seculore

4) 911 Legislation Update  
   - Federal  
   - State  
   - Local

5) Missouri 911 Service Board Report

6) Kansas 911 Coordinating Council

7) RAMBIS  
   - Radio use  
   - Continued maintenance requirements

8) Cost Share Requests:  
   - Independence

9) PSAP Updates:  
   - Douglas County Implementation  
   - Atchison County Membership

10) Public Safety Program Updates:  
    - Training  
    - Technical Services  
    1) Router Project Update  
    - Database / Mapping
11) SirenGPS

12) Other Business

13) Adjournment

**Future Meeting Dates:**

PS User Committee @ 1:00 pm in MARC Boardroom

- November 20, 2019
- March 4, 2020
- June 24, 2020
- September 2, 2020
- December 2, 2020
2020 BUDGET

Regional 911 System and Public Safety Communications

Mid-America Regional Council
MEMORANDUM

TO: Public Safety Communications Board
FROM: Eric Winebrenner, Public Safety Program Director
RE: 2020 Budget Highlights

It is my pleasure to present to you the proposed 2020 budget for the Regional 911 system. This budget has been developed to continue to meet the Public Safety Communication Board’s goals for the Regional 911 system, which include maintaining a state-of-the-art regional interoperable communications system for metropolitan Kansas City.

The proposed budget for 2020 totals $8,876,317, which represents an 18.7% increase over the approved budget for 2019. The following issues are presented for the Board to review when considering adoption of this budget:

- **Training Component** — In 2019, the training component was contracted to MARC’s Government Training Institute (GTI) for administration. After reviewing this arrangement over the past year, we have determined that moving administration of the 911 training program back to Public Safety will be more efficient, so it has been returned to the 2020 Regional 911 budget. The 911 Training Coordinator will continue to collaborate and coordinate with GTI on regional training initiatives.

- **Online Training** — MARC’s Public Safety program will offer interactive 911 training online for the first time in 2020. Costs for the first year are estimated at $35,672.

- **Consortium Membership Fees** — A study of consortium membership fees was conducted to ensure revenues were enough to cover the cost of operating the training programs. After review, it is recommended that consortium memberships for MARC 911 member agencies be eliminated in 2020, and that training costs be included in the monthly allocation billing. This change will allow all MARC 911 member agencies to send personnel to 911 and selected GTI training. The cost to accomplish this, including the interactive online training, is $130,000.

  For reference, MARC collected $90,000 in consortium member fees from member agencies and supported GTI training with an additional $13,500 in 2019. Agencies outside the MARC region paid a total of $12,090 in consortium member fees. Under the new arrangement, non-MARC members will still be allowed to purchase consortium memberships at a cost of $200 per individual seat.

- **Maintenance** — 911 network maintenance and RAMBIS network maintenance will be contracted through Commenco in 2020. The 911 network maintenance costs will increase by 18%, to $1,044,604, and RAMBIS network maintenance will increase by 5% to $86,649.

- **MARC Coordination** — Expenses for MARC coordination will increase by less than 1% compared to the 2018 budget (the most recent year that included training coordinator costs).
• **Capital Projects/Equipment Replacement** — Costs for capital projects and equipment replacement will increase by 86% in 2020, or $2,871,520, for the following reasons:
  
  o After purchasing new selective routers, the fund balance will be approximately $458,000.
  
  o 2020 is the first year of planned PSAP equipment upgrades, with 60 workstations in line for replacement. Commenco currently estimates the cost for these upgrades at $1,298,250 but anticipates these costs may increase over the course of the calendar year.
  
  o Cybersecurity measures require a test environment where software can be tested prior to installation on the live network. The estimated cost is $266,130.
  
  o Under the planned phased approach to PSAP equipment upgrades, VESTA Software support for older workstations will need to be renewed to maintain each workstation to its replacement year. The estimated cost is $567,056.
  
  o Various Microwave Networks and PTP Links need repair, replacement or implementation. The estimated cost is $214,000.
  
  o Miscellaneous costs, including electrical installation, cabling costs, fiber installation connection costs, tower structural analysis, etc., are budgeted at $228,980.
  
  o Several items that were previously included in Cost Share are now included in Capital Projects/Equipment Replacement. These include equipment or software for the operation of the network that are repeated yearly or are improvements to sustained equipment:
    
    • Datamaster: $89,000
    • AlertSense: $4,500
    • WhatsUpGold: $7,500
    • ALI server upgrade: $25,000
    • Network computer replacement: $10,000

• **Cybersecurity** — Cybersecurity will be an ongoing issue after the 911 network is connected to the internet for Next Generation 911 functionality. After the Department of Homeland Security audit was presented to the Board in July, staff researched options for the most comprehensive cybersecurity for the 911 system. MARC staff recommends contracting for cybersecurity services with a company that specializes in cybersecurity for 911 systems. The proposed budget for this in 2020 is $151,380.

These are some of the issues that are causing an increase in the proposed budget for 2020. As the Regional 911 system grows from a 1960s-era analog system to a 21st century digital system with Next Generation 911 capabilities, the costs associated with adding functionality and maintaining the system in a state-of-the-art condition will necessarily increase. MARC staff are working diligently to determine the most cost-effective means to accomplish the Board’s goals for the Regional 911 system. In 2020, equipment replacement will be the main cost driver to the increase in the proposed 911 budget.

The following pages provide more detail about the proposed 2020 budget, by county and by program activity. If you have any questions, please feel free to contact me.
MARC 911 staff would like to express their appreciation to members of the Public Safety Communication Board for their ongoing contributions and support as we work together to provide the highest possible quality of 911 communications to residents across the Kansas City metro area.

Sincerely,

Eric Winebrenner
Public Safety Program Director
Mid-America Regional Council

September 2019
Public Safety Communications Board Members

Chief Elected County Officials (8)
- Presiding Commissioner Jerry Nolte, Clay County, Missouri
- County Executive Frank White, Jackson County, Missouri
- Commission Chair Ed Eilert, Johnson County, Kansas
- Commission Chair Doug Smith, Leavenworth County, Kansas
- Presiding Commissioner Rob Roberts, Miami County, Kansas
- Presiding Commissioner Ron Schieber, Platte County, Missouri
- Presiding Commissioner Bob King, Ray County, Missouri
- Mayor/CEO David Alvey, Unified Government of Wyandotte County/Kansas City, Kansas

MARC Board Representatives (2)
- Legislator Scott Burnett, Jackson County, Missouri
- Vacant

Cass County Emergency Services Board (1)
- Executive Director Robin Tieman

Police Chiefs (4)
- Chief Rick Smith, Kansas City, Missouri, Police Department
- Interim Chief Michael York, Kansas City, Kansas, Police Department
- Chief Frank Donchez Jr., Overland Park, Kansas Police Department
- Chief Brad Halsey, Independence, Missouri, Police Department

County Sheriffs (2)
- Sheriff Mark Owen, Platte County, Missouri
- Sheriff Calvin Hayden, Johnson County, Kansas

Fire Chiefs (2)
- Chief Richard Carrizzo, South Platte Fire Protection District
- Chief Dave Williams, Leawood Fire Department, representing Metro Fire Chiefs

EMS Chiefs (2)
- Chief Paul Davis, Johnson County Med-Act
- Chief Gary Reese, Kansas City, Missouri

911 Users (2)
- Major Scott Boden, Johnson County Sheriff’s Office
- Steve Hoskins, Kansas City, Missouri, Police Department

PSAP Supervisors (4)
- Wendy Dedeke, Leavenworth County, Kansas
- Don Ward, Overland Park, Kansas
- Jamie Taylor, Lee’s Summit, Missouri
- Linda Alvarez, North Kansas City, Missouri

At-Large Elected Officials (2)
- Mayor Kris Turnbow, Raymore, Missouri
- Councilman Andy Huckaba, Lenexa, Kansas
Regional 911 System Service Area

The 911 Interlocal Cooperation Agreement covers 45 public safety answering points in 11 counties: Atchison, Douglas, Johnson, Leavenworth, Miami, and Wyandotte counties in Kansas and Cass, Clay, Jackson, Platte and Ray in Missouri.

Regional coordination ensures that all 911 callers in the region – no matter where they are located – have access to the same responsive, high-quality 911 service. Standardization of equipment allows local communities to share a common support system and stay abreast of new ideas and technology to build a cohesive 911 system for the future.

<table>
<thead>
<tr>
<th>CALL VOLUMES</th>
<th>Emergency 911 calls</th>
<th>Non-emergency calls</th>
<th>Total calls</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>1,548,534</td>
<td>3,072,322</td>
<td>4,620,856</td>
</tr>
<tr>
<td>2019 YTD</td>
<td>897,074</td>
<td>1,842,191</td>
<td>2,739,265</td>
</tr>
</tbody>
</table>
Goals and Responsibilities

Goals of the Regional 911 System

- Provide a single number (911) for reaching emergency assistance.
- Provide the same capability for service throughout the metropolitan Kansas City area and ensure that all equipment provides a minimum level of operating features (i.e., ANI, ALI, TDD, cellular phones, VoIP, language interpretation).
- Maintain regional integrity of the 911 system (quality and reliability of service).
- Ensure that the cost of the network is shared equitably throughout the metropolitan area.
- Provide flexibility at the local level to enhance the service at local expense.
- Foster ability to provide state-of-the-art equipment to the answer points.

Goals of the Regional Public Safety Communications System

- Maintain a state-of-the-art regional interoperable communications system for metropolitan Kansas City.
- Ensure that the cost of the network and system infrastructure is shared equitably throughout the metropolitan Kansas City area.
- Ensure compatibility, to the extent possible, with existing public safety systems in metropolitan area.
- Seek alternative funding methods to reduce costs to participating agencies.

Roles and Responsibilities of the Public Safety Communications Board

- Monitor provision of 911 services as outlined in the statement of mutual goals and responsibilities.
- Monitor and revise 911 and communications system operating policies as outlined in the 911 Interlocal Cooperative Agreement.
- Monitor and audit charges for 911 and communications services.
- Monitor 911 surcharge fund balances and tax rates and work with area counties to resolve issues related to the adequate funding for the regional 911 system.
- Review and approve an annual budget for 911 and communications system services provided by the Mid-America Regional Council.
- Review and approve an annual plan of action prepared by the Public Safety Communications Users Committee to maintain and enhance, as appropriate, the regional 911 system and the regional public safety communications system.
- Monitor state and federal legislation, tariffs, and regulations, and new technology and practices that may impact the metropolitan Kansas City 911 system and/or regional communications system and recommend actions or positions by MARC or area counties to respond to issues.
- Oversee and coordinate public education and promotion efforts by area local governments and public safety agencies, including the review and monitoring of telephone directories.
- Address impacts of emerging technology on 911 operations and the regional communications system.
- Monitor technical operation of the regional communications system and 911 system to include the network design and performance, selective routing and database management.
- Authorize service agreements relating to 911 and public safety communications for agencies outside of the MARC region that desire to participate in regional activities.
- Approve expenditures from the 911 surcharge collected by area counties for changes or improvements to the operating system.
- Oversee the acquisition, use and maintenance of communications equipment owned by MARC.
- Coordinate communications projects and activities with other committees to include Regional Homeland Security Coordinating Committee and the Metropolitan Area Regional Radio System Management Council.
- Address ongoing policy issues, as appropriate and necessary.

**Financial Summary**

The cost to operate Kansas City’s regional 911 system is shared by the 11 member counties and the city of Excelsior Springs (which has its own funding mechanism, separate from the county) on a per capita basis. Counties pay their share of expenses by collecting sales taxes specifically for 911 or collecting monthly 911 surcharges from residential and commercial phone customers. If these revenues run short, counties may need to use general funds to meet their financial obligations to the regional system.

Kansas counties all use the same fee structure — a 90-cent surcharge each month on the bill for any device capable of calling 911. In Missouri, counties currently rely on either sales tax revenues or surcharges on landline phones. The state of Missouri passed legislation in 2018 that allows counties more funding options, including surcharges on wireless devices, subject to voter approval.

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Funding Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atchison County, Kan.</td>
<td>90¢ monthly surcharge, all devices</td>
</tr>
<tr>
<td>Cass County, Mo.</td>
<td>Dedicated 1/8% sales tax</td>
</tr>
<tr>
<td>Clay County, Mo.</td>
<td>2% monthly surcharge, landlines</td>
</tr>
<tr>
<td>Douglas County, Kan.</td>
<td>90¢ monthly surcharge, all devices</td>
</tr>
<tr>
<td>Jackson County, Mo.</td>
<td>6% monthly surcharge, landlines</td>
</tr>
<tr>
<td>Johnson County, Kan.</td>
<td>90¢ monthly surcharge, all devices</td>
</tr>
<tr>
<td>Leavenworth County, Kan.</td>
<td>90¢ monthly surcharge, all devices</td>
</tr>
<tr>
<td>Miami County, Kan.</td>
<td>90¢ monthly surcharge, all devices</td>
</tr>
<tr>
<td>Platte County, Mo.</td>
<td>1.5% monthly surcharge, landlines</td>
</tr>
<tr>
<td>Ray County, Mo.</td>
<td>Dedicated 1% sales tax</td>
</tr>
<tr>
<td>Wyandotte County, Kan.</td>
<td>90¢ monthly surcharge, all devices</td>
</tr>
<tr>
<td>City of Excelsior Springs, Mo.</td>
<td>15% monthly surcharge, landlines</td>
</tr>
</tbody>
</table>

Each jurisdiction’s share of the cost of the regional 911 system ($8,876,317) is calculated by determining its share of the regional population (2,040,957).
Financial priorities for the regional 911 system include activities associated with the delivery and processing of 911 calls. Historically, the Public Safety Communications Board has interpreted this provision to apply to the following cost categories:

- **911 Network**: Costs associated with the dedicated network over which 911 calls are delivered and selective routing of 911 calls, which includes the RAMBIS microwave network.
- **GIS Maintenance**: Costs associated with provision of the ALI database, either by a telephone company, by MARC or by a third-party database provider. Costs associated with geographic addressing and mapping to support the regional 911 system, including initial project and ongoing maintenance costs.
- **911 Training**: Providing ongoing training for telecommunicators and supervisors.
- **Language Line**: Over-the-phone translation services available to each Public Safety Answering Point (PSAP).
- **911 Equipment Maintenance**: The maintenance contract to maintain the 911 equipment in each PSAP, including equipment that a 911 telecommunicator uses to process the call, selected ancillary equipment like headsets, and the integration of other lines that support the functioning of a 911 center.
- **RAMBIS Maintenance**: The maintenance contract, insurance, utilities and other costs related to maintaining the RAMBIS network.
- **911 SS7**: Costs associated with Signaling System 7, an international telecommunications standard that defines how network elements in a public switched telephone network exchange information over a digital signaling network.
• **MARC Coordination Services**: Expenditures associated with overall system administration, outreach, planning and policy development. (See details on page 15.)

• **Capital Projects/Equipment Replacement**: Funds needed to keep the network operational and up to current state-of-the-art standards. (See pages 13-14.)

• **Capital Projects/Equipment Replacement Contingency**: In 2019, a contingency fund was started with the goal of having 10% of the annual budget as a reserve. This will be accomplished by putting 2% of the Capital Projects/Equipment Replacement funds into the contingency fund.

• **Cost Share/Miscellaneous Expenses**: This category has grown over the years to be a catch all for numerous expenses. For 2020, we have attempted to better categorize these expenses and reduce this category to include only unexpected costs or experimental short-term project costs. (See details on page 16.)

• **Cybersecurity**: This category was established in the 2020 budget to protect the 911 system from cybersecurity threats, using a third-party vendor to evaluate and monitor the 911 network.

**Proposed Expenditures by Category, 2020**
## Expenditures by Category, 2018-2020

<table>
<thead>
<tr>
<th>Category</th>
<th>ACTUAL 2018</th>
<th>BUDGETED 2019</th>
<th>PROPOSED 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Projects/Equipment Replacement</td>
<td>$1,445,544</td>
<td>$1,577,677</td>
<td>$2,571,520</td>
</tr>
<tr>
<td>911 Network</td>
<td>1,859,294</td>
<td>2,050,000</td>
<td>2,110,000</td>
</tr>
<tr>
<td>MARC Coordination</td>
<td>1,635,818</td>
<td>1,609,299</td>
<td>1,849,910</td>
</tr>
<tr>
<td>911 Equipment Maintenance</td>
<td>643,263</td>
<td>886,320</td>
<td>1,044,604</td>
</tr>
<tr>
<td>GIS Maintenance</td>
<td>291,901</td>
<td>286,057</td>
<td>259,455</td>
</tr>
<tr>
<td>RAMBIS Equipment Maintenance</td>
<td>166,258</td>
<td>125,724</td>
<td>193,454</td>
</tr>
<tr>
<td>Cybersecurity (1)</td>
<td>-</td>
<td>-</td>
<td>151,380</td>
</tr>
<tr>
<td>911 Training (2)</td>
<td>-</td>
<td>286,057</td>
<td>130,000</td>
</tr>
<tr>
<td>Cost Share/New Project</td>
<td>26,949</td>
<td>269,967</td>
<td>115,500</td>
</tr>
<tr>
<td>Contingency Fund (3)</td>
<td>-</td>
<td>30,935</td>
<td>57,430</td>
</tr>
<tr>
<td>Language Line</td>
<td>46,765</td>
<td>55,000</td>
<td>55,000</td>
</tr>
<tr>
<td>911 SS7</td>
<td>38,101</td>
<td>38,064</td>
<td>38,064</td>
</tr>
<tr>
<td><strong>TOTAL EXPENDITURES</strong></td>
<td><strong>$6,153,894</strong></td>
<td><strong>$7,215,100</strong></td>
<td><strong>$8,876,317</strong></td>
</tr>
</tbody>
</table>

**Notes:**
1. The cybersecurity project was added in 2020.
2. 911 Training was paid for through Consortium Dues in 2018, which is not reflected in this budget.
3. The contingency fund was added in 2019.

## Proposed 2020 Expenditures by Jurisdiction

### Table 1: Atchison, Cass and Clay Counties

<table>
<thead>
<tr>
<th>Category</th>
<th>ATCHISON COUNTY</th>
<th>CASS COUNTY</th>
<th>CLAY COUNTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Projects/Equip. Replacement</td>
<td>$23,811</td>
<td>$139,960</td>
<td>$296,884</td>
</tr>
<tr>
<td>911 Network</td>
<td>17,497</td>
<td>102,843</td>
<td>218,151</td>
</tr>
<tr>
<td>MARC Coordination</td>
<td>15,340</td>
<td>90,166</td>
<td>191,261</td>
</tr>
<tr>
<td>911 Equipment Maintenance</td>
<td>8,662</td>
<td>50,915</td>
<td>108,001</td>
</tr>
<tr>
<td>GIS Maintenance</td>
<td>2,151</td>
<td>12,646</td>
<td>26,825</td>
</tr>
<tr>
<td>RAMBIS Equipment Maintenance</td>
<td>1,604</td>
<td>9,429</td>
<td>20,001</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>1,255</td>
<td>7,378</td>
<td>15,651</td>
</tr>
<tr>
<td>911 Training</td>
<td>1,078</td>
<td>6,336</td>
<td>13,441</td>
</tr>
<tr>
<td>Cost Share/New Project</td>
<td>958</td>
<td>5,630</td>
<td>11,941</td>
</tr>
<tr>
<td>Contingency Fund</td>
<td>476</td>
<td>2,799</td>
<td>5,938</td>
</tr>
<tr>
<td>Language Line</td>
<td>456</td>
<td>2,681</td>
<td>5,686</td>
</tr>
<tr>
<td>911 SS7</td>
<td>316</td>
<td>1,855</td>
<td>3,935</td>
</tr>
<tr>
<td><strong>TOTAL ANNUAL COST</strong></td>
<td><strong>$73,604</strong></td>
<td><strong>$432,639</strong></td>
<td><strong>$917,716</strong></td>
</tr>
<tr>
<td><strong>COST PER MONTH</strong></td>
<td><strong>$6,134</strong></td>
<td><strong>$36,053</strong></td>
<td><strong>$76,476</strong></td>
</tr>
</tbody>
</table>
Table 2: Douglas, Jackson and Johnson Counties

<table>
<thead>
<tr>
<th></th>
<th>DOUGLAS COUNTY</th>
<th>JACKSON COUNTY</th>
<th>JOHNSON COUNTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Projects/Equip. Replacement</td>
<td>$155,926</td>
<td>$948,505</td>
<td>$765,631</td>
</tr>
<tr>
<td>911 Network</td>
<td>114,575</td>
<td>696,964</td>
<td>562,588</td>
</tr>
<tr>
<td>MARC Coordination</td>
<td>100,452</td>
<td>611,053</td>
<td>493,240</td>
</tr>
<tr>
<td>911 Equipment Maintenance</td>
<td>56,723</td>
<td>345,048</td>
<td>278,522</td>
</tr>
<tr>
<td>GIS Maintenance</td>
<td>14,089</td>
<td>85,702</td>
<td>69,178</td>
</tr>
<tr>
<td>RAMBIS Equipment Maintenance</td>
<td>10,505</td>
<td>63,901</td>
<td>51,580</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>8,220</td>
<td>50,003</td>
<td>40,362</td>
</tr>
<tr>
<td>911 Training</td>
<td>7,059</td>
<td>42,941</td>
<td>34,662</td>
</tr>
<tr>
<td>Cost Share/New Project</td>
<td>6,272</td>
<td>38,151</td>
<td>30,796</td>
</tr>
<tr>
<td>Contingency Fund</td>
<td>3,119</td>
<td>18,970</td>
<td>15,313</td>
</tr>
<tr>
<td>Language Line</td>
<td>2,987</td>
<td>18,167</td>
<td>14,665</td>
</tr>
<tr>
<td>911 SS7</td>
<td>2,067</td>
<td>12,573</td>
<td>10,149</td>
</tr>
<tr>
<td><strong>TOTAL ANNUAL COST</strong></td>
<td><strong>$481,993</strong></td>
<td><strong>$2,931,977</strong></td>
<td><strong>$2,366,686</strong></td>
</tr>
<tr>
<td><strong>COST PER MONTH</strong></td>
<td><strong>$40,166</strong></td>
<td><strong>$244,331</strong></td>
<td><strong>$197,224</strong></td>
</tr>
</tbody>
</table>

Table 3: Leavenworth, Miami and Platte Counties

<table>
<thead>
<tr>
<th></th>
<th>LEAVENWORTH COUNTY</th>
<th>MIAMI COUNTY</th>
<th>PLATTE COUNTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Projects/Equip. Replacement</td>
<td>$98,972</td>
<td>$46,130</td>
<td>$125,671</td>
</tr>
<tr>
<td>911 Network</td>
<td>72,725</td>
<td>33,896</td>
<td>92,344</td>
</tr>
<tr>
<td>MARC Coordination</td>
<td>63,760</td>
<td>29,718</td>
<td>80,961</td>
</tr>
<tr>
<td>911 Equipment Maintenance</td>
<td>36,004</td>
<td>16,781</td>
<td>45,717</td>
</tr>
<tr>
<td>GIS Maintenance</td>
<td>8,943</td>
<td>4,168</td>
<td>11,355</td>
</tr>
<tr>
<td>RAMBIS Equipment Maintenance</td>
<td>6,668</td>
<td>3,108</td>
<td>8,466</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>5,218</td>
<td>2,432</td>
<td>6,625</td>
</tr>
<tr>
<td>911 Training</td>
<td>4,481</td>
<td>2,088</td>
<td>5,689</td>
</tr>
<tr>
<td>Cost Share/New Project</td>
<td>3,981</td>
<td>1,855</td>
<td>5,055</td>
</tr>
<tr>
<td>Contingency Fund</td>
<td>1,979</td>
<td>923</td>
<td>2,513</td>
</tr>
<tr>
<td>Language Line</td>
<td>1,896</td>
<td>884</td>
<td>2,407</td>
</tr>
<tr>
<td>911 SS7</td>
<td>1,312</td>
<td>611</td>
<td>1,666</td>
</tr>
<tr>
<td><strong>TOTAL ANNUAL COST</strong></td>
<td><strong>$305,937</strong></td>
<td><strong>$142,594</strong></td>
<td><strong>$388,470</strong></td>
</tr>
<tr>
<td><strong>COST PER MONTH</strong></td>
<td><strong>$25,495</strong></td>
<td><strong>$11,883</strong></td>
<td><strong>$32,372</strong></td>
</tr>
</tbody>
</table>
Table 4: Ray and Wyandotte Counties, City of Excelsior Springs

<table>
<thead>
<tr>
<th></th>
<th>RAY COUNTY</th>
<th>WYANDOTTE COUNTY</th>
<th>EXCELSIOR SPRINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Projects/Equip. Replacement</td>
<td>$32,833</td>
<td>$221,601</td>
<td>$15,595</td>
</tr>
<tr>
<td>911 Network</td>
<td>24,125</td>
<td>162,833</td>
<td>11,459</td>
</tr>
<tr>
<td>MARC Coordination</td>
<td>21,152</td>
<td>142,762</td>
<td>10,046</td>
</tr>
<tr>
<td>911 Equipment Maintenance</td>
<td>11,944</td>
<td>80,614</td>
<td>5,673</td>
</tr>
<tr>
<td>GIS Maintenance</td>
<td>2,967</td>
<td>20,023</td>
<td>1,409</td>
</tr>
<tr>
<td>RAMBIS Equipment Maintenance</td>
<td>2,212</td>
<td>14,929</td>
<td>1,051</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>1,731</td>
<td>11,682</td>
<td>822</td>
</tr>
<tr>
<td>911 Training</td>
<td>1,486</td>
<td>10,032</td>
<td>706</td>
</tr>
<tr>
<td>Cost Share/New Project</td>
<td>1,321</td>
<td>8,913</td>
<td>627</td>
</tr>
<tr>
<td>Contingency Fund</td>
<td>657</td>
<td>4,432</td>
<td>312</td>
</tr>
<tr>
<td>Language Line</td>
<td>629</td>
<td>4,244</td>
<td>299</td>
</tr>
<tr>
<td>911 SS7</td>
<td>435</td>
<td>2,937</td>
<td>207</td>
</tr>
<tr>
<td><strong>TOTAL ANNUAL COST</strong></td>
<td><strong>$101,490</strong></td>
<td><strong>$685,004</strong></td>
<td><strong>$48,205</strong></td>
</tr>
<tr>
<td><strong>COST PER MONTH</strong></td>
<td><strong>$8,458</strong></td>
<td><strong>$57,084</strong></td>
<td><strong>$4,017</strong></td>
</tr>
</tbody>
</table>

**911 Capital Fund**

MARC administers the Regional 911 System under the guidance and leadership of the Public Safety Communications Board. The Board sets annual priorities for expenditures to ensure that the system is well-maintained and kept up-to-date with new technologies. Funds to support the system are paid by member counties.

Because funds are accrued over time to cover large-cost projects, a 911 Capital Fund was established to plan and track expenditures. MARC’s agency-wide 2019 budget (adopted in late 2018) included an overview of planned expenditures from the 911 Capital Fund for the next five years.

<table>
<thead>
<tr>
<th>911 CAPITAL FUND</th>
<th>PLANNED EXPENDITURES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2019</td>
</tr>
<tr>
<td>Geospatial Routing</td>
<td>$ —</td>
</tr>
<tr>
<td>Microwave Networks &amp; Point-to-Point Links</td>
<td>307,709</td>
</tr>
<tr>
<td>Microwave Overlay</td>
<td>—</td>
</tr>
<tr>
<td>Miscellaneous &amp; Contingency</td>
<td>214,000</td>
</tr>
<tr>
<td>PSAP Upgrades</td>
<td>87,188</td>
</tr>
<tr>
<td>Selective Router Replacement</td>
<td>1,583,476</td>
</tr>
<tr>
<td>Software Support Renewals</td>
<td>23,700</td>
</tr>
<tr>
<td>VESTA® Host Server Upgrade</td>
<td>—</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>$2,216,073</strong></td>
</tr>
</tbody>
</table>
The 2019 budget for the 911 Capital Fund included purchase and installation of a selective router, along with improvements to the microwave networks and point-to-point links used to transmit 911 calls, ongoing PSAP upgrades and software support renewals.

An updated list of proposed capital projects for 2020 is shown below:

<table>
<thead>
<tr>
<th>PROJECT</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datamaster (1)</td>
<td>$89,000</td>
</tr>
<tr>
<td>AlertSense Notification Software annual cost (1)</td>
<td>4,500</td>
</tr>
<tr>
<td>WhatsUpGold/Flow yearly monitor cost (1)</td>
<td>7,500</td>
</tr>
<tr>
<td>ALI server upgrade project (1)</td>
<td>25,000</td>
</tr>
<tr>
<td>Network computer replacement (1)</td>
<td>10,000</td>
</tr>
<tr>
<td>Workstation replacement project (2)</td>
<td>1,098,250</td>
</tr>
<tr>
<td>Eight extra workstations to get to the new average of 60 per year (2)</td>
<td>200,000</td>
</tr>
<tr>
<td>VESTA Software support renewals (3)</td>
<td>567,000</td>
</tr>
<tr>
<td>Microwave Network/PTP Links (4)</td>
<td>214,000</td>
</tr>
<tr>
<td>911 Test Servers and Workstations (5)</td>
<td>266,131</td>
</tr>
<tr>
<td>Replacing three servers per year for three years, (one host per year)</td>
<td>140,639</td>
</tr>
<tr>
<td>Windows 10 upgrade cost</td>
<td>20,500</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>229,000</td>
</tr>
</tbody>
</table>

**TOTAL CAPITAL PROJECTS** $2,871,520

**Notes:**

(1) Several items that had been in the cost-share section of the budget were moved to capital projects for 2020: Datamaster, AlertSense, WhatsUpGold, the ALI server upgrade, and network computer replacements.

(2) The four-year workstation replacement program will start in 2020. We will replace approximately 60 workstations per year every year to keep the Regional 911 system’s 240 workstations up to date. This rotation will also help keep our system current with Windows updates.

(3) VESTA Software support renewals are required to keep technical support for our aging VESTA software. The workstation replacement program will also assist in this process, as workstations running VESTA will be upgraded every four years on a rotating basis.

(4) Microwave Network/PTP links will be maintained, repaired and placed to improve the 911 Network and its reliability.

(5) 911 Test Servers and Workstations will be installed at MARC to allow new software to be tested in a controlled environment before it is placed on the Regional 911 System.
MARC Coordination Budget

MARC receives revenues to support coordination activities from member jurisdictions, as well as from training and other income sources. Budgeted revenues and expenses are shown below. Each year, any funds remaining in the MARC Coordination Budget are transferred to the 911 Capital Fund.

<table>
<thead>
<tr>
<th></th>
<th>2018 BUDGET</th>
<th>2019 BUDGET</th>
<th>2020 BUDGET</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PUBLIC SAFETY REVENUES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordination Fees</td>
<td>$1,778,837</td>
<td>$1,609,288</td>
<td>$1,849,910</td>
</tr>
<tr>
<td>Public Education/Promotions</td>
<td>9,000</td>
<td>9,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Training Registration Fees/Other</td>
<td>16,000</td>
<td>7,500</td>
<td>9,400</td>
</tr>
<tr>
<td>Training Memberships</td>
<td>60,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL REVENUES</strong></td>
<td>$1,863,837</td>
<td>$1,625,788</td>
<td>$1,864,310</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>2018 BUDGET</th>
<th>2019 BUDGET</th>
<th>2020 BUDGET</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PUBLIC SAFETY EXPENSES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salaries and Wages</td>
<td>$787,401</td>
<td>$687,837</td>
<td>$758,213</td>
</tr>
<tr>
<td>Employee Benefits</td>
<td>385,037</td>
<td>342,541</td>
<td>382,140</td>
</tr>
<tr>
<td>Indirect Costs</td>
<td>354,078</td>
<td>313,234</td>
<td>360,351</td>
</tr>
<tr>
<td>Contractual Services</td>
<td>59,160</td>
<td>24,200</td>
<td>51,400</td>
</tr>
<tr>
<td>Legal Fees</td>
<td>5,000</td>
<td>3,000</td>
<td>5,000</td>
</tr>
<tr>
<td>In-Region Travel</td>
<td>4,700</td>
<td>3,000</td>
<td>3,800</td>
</tr>
<tr>
<td>Out-of-Region Travel</td>
<td>50,250</td>
<td>35,440</td>
<td>47,706</td>
</tr>
<tr>
<td>Rent</td>
<td>69,821</td>
<td>63,199</td>
<td>66,079</td>
</tr>
<tr>
<td>Insurance</td>
<td>13,260</td>
<td>13,542</td>
<td>15,948</td>
</tr>
<tr>
<td>Postage</td>
<td>1,400</td>
<td>750</td>
<td>850</td>
</tr>
<tr>
<td>Supplies and General Expense</td>
<td>22,150</td>
<td>22,030</td>
<td>24,524</td>
</tr>
<tr>
<td>Equipment Rental</td>
<td>1,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Maintenance and Expenses</td>
<td>16,818</td>
<td>24,224</td>
<td>25,000</td>
</tr>
<tr>
<td>Equipment</td>
<td>4,080</td>
<td>9,400</td>
<td>14,500</td>
</tr>
<tr>
<td>Meeting</td>
<td>36,750</td>
<td>34,450</td>
<td>41,350</td>
</tr>
<tr>
<td>Registration Fees</td>
<td>7,750</td>
<td>7,300</td>
<td>6,920</td>
</tr>
<tr>
<td>Professional Memberships</td>
<td>2,602</td>
<td>2,618</td>
<td>2,618</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>6,080</td>
<td>6,500</td>
<td>7,460</td>
</tr>
<tr>
<td>Training</td>
<td>10,200</td>
<td>6,370</td>
<td>21,300</td>
</tr>
<tr>
<td>Printing</td>
<td>9,300</td>
<td>3,000</td>
<td>6,000</td>
</tr>
<tr>
<td>Vehicle Depreciation</td>
<td>17,000</td>
<td>23,153</td>
<td>23,153</td>
</tr>
<tr>
<td><strong>TOTAL EXPENSES</strong></td>
<td>$1,863,837</td>
<td>$1,625,788</td>
<td>$1,864,310</td>
</tr>
</tbody>
</table>
COST-SHARE BUDGET

Each year, some funds are budgeted for anticipated expenses that do not fit into the other budget categories, such as new projects or miscellaneous expenses. The cost of these expenses is allocated to members using the same per capita formulas as other budget categories. For 2020, cost share expenses are budgeted at $115,500. Expenses are itemized below.

<table>
<thead>
<tr>
<th>COST-SHARE ITEM</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headsets</td>
<td>$24,000</td>
</tr>
<tr>
<td>Tower and Antenna Inspections</td>
<td>14,500</td>
</tr>
<tr>
<td>Scout Fiber Enhancement</td>
<td>52,000</td>
</tr>
<tr>
<td>SMART Controller replacement</td>
<td>5,000</td>
</tr>
<tr>
<td>Site Alarming Upgrades</td>
<td>5,000</td>
</tr>
<tr>
<td>Shelter Equipment Upgrades</td>
<td>5,000</td>
</tr>
<tr>
<td>HVAC Upgrade</td>
<td>5,000</td>
</tr>
<tr>
<td>CAMA Trunks moved to host</td>
<td>5,000</td>
</tr>
<tr>
<td>Vesta Server Backup system</td>
<td>24,000</td>
</tr>
<tr>
<td><strong>TOTAL COST SHARE</strong></td>
<td><strong>$115,000</strong></td>
</tr>
</tbody>
</table>

Submitted for Approval, September 2019

CONTACTS:
Eric Winebrenner  
MARC Public Safety Program Director  
 ewinebrenner@marc.org  
 816-701-8211

Mike Daniels  
Public Safety Communications Planning & Administrative Manager  
mdaniels@marc.org  
 816-701-8221
A COMPREHENSIVE CYBERSECURITY VULNERABILITY ASSESSMENT:

The SecuLore CyberBenchmark is the only cybersecurity risk assessment built specifically for public safety and based upon FCC, APCO, DHS, and NIST best practices. Developed by experts in 9-1-1 technology and cybersecurity, this in-depth report identifies threats and provides prioritized, actionable recommendations to remediate vulnerabilities and enhance your cybersecurity.

ELEVATE YOUR CYBER AWARENESS

DETECTION BEFORE EXPLOITATION

➤ Utilizing SecuLore’s patent pending technology, the CyberBenchmark identifies vulnerabilities before hackers use them against you. Our team of cyber analysts are armed with unique expertise in public-safety-targeted cyber attacks and use this experience to identify activity that may be an indication of hackers’ presence in your network.

RECOMMENDED ANNUALLY

➤ The FCC recommends that all PSAPs complete an annual cybersecurity risk assessment to guard against cyber attacks that could take down 9-1-1 systems.

CREATED BY AN INDUSTRY EXPERT

➤ Founder & CEO Timothy Lorello, a 9-1-1 technology expert with over 17 years of experience, served on the team that wrote the supplemental Task Force on Optimal PSAP Architecture (TFOPA) Report—an industry standard from the FCC.
WHAT SHOULD YOU EXPECT FROM A CYBERBENCHMARK?

➢ An Assessment Tailored to You
   An initial consultation gives us a baseline of your network architecture and cybersecurity goals, so we can customize the CyberBenchmark to fit your needs.

➢ Passive Data Capture
   Paladin™, our patent-pending network appliance, captures 1-2 weeks of data for network segments outlined in the initial consultation.

➢ In-Depth Data Analysis
   Our 19-step analytical process follows industry best practices and continually evolves to include the latest threat detection techniques.

➢ Minimal Time Requirement
   The CyberBenchmark takes 3-5 weeks to complete. However, we only take 4-8 hours of your time, which includes the initial consultation and final presentation.

Final Presentation & Deliverables Include:

- CyberBenchmark Report
  A complete review of the project’s findings

- Vulnerability Reports
  Actionable vulnerability remediation recommendations for each segment captured

- NIST Risk Analysis Checklist
  A prioritized list of all vulnerabilities discovered based on risk

- Key Cybersecurity Policies
  Customized cybersecurity policies specific to your environment

- Cyber Incident Response Plans
  A recommended action plan to guide your team when a cyber incident occurs

- Master IP List
  A record of all IP addresses detected with all supporting analysis

WHY SECULORE SOLUTIONS?

An innovator in public-safety-focused cybersecurity, SecuLore Solutions is passionate about protecting critical services from cyber criminals. Led by experts in both 9-1-1 technology and cyber warfare, our team partners with public safety, local governments, and IT teams to provide training, tools, and support needed to defend our public infrastructure from increasingly sophisticated cyber attacks.

WANT TO LEARN MORE?

VISIT OUR WEBSITE
www.SecuLore.com

SEND US AN EMAIL
info@SecuLore.com

GIVE US A CALL
410-305-0234
Toll Free: 844-732-8567
MANAGED CYBERSECURITY MONITORING DESIGNED WITH PUBLIC SAFETY IN MIND:

SecuLore’s Paladin Overwatch service simplifies cybersecurity for public safety agencies and local governments, empowering IT teams with the resources and allies needed to protect our mission-critical infrastructure. Cyber attacks against public safety agencies have been publicly reported in all 50 states. It’s not a matter of “if” you will be targeted but “when” it will impact you. With Paladin Overwatch, you gain a defense-in-depth cybersecurity strategy with cutting edge technology and a team of experts that understand your mission.

A NEW LAYER OF CYBERSECURITY

BEHAVIOR-BASED CYBERSECURITY

SecuLore offers the next level of monitoring by implementing behavioral-based cybersecurity that is customized specifically for public safety and is designed to identify threats that are often missed by other layers of security. Utilizing our experience with the cyberattacks we find in public safety agencies and local governments across the country, we continually evolve our methods to stay a step ahead of cyber criminals.

PATENT-PENDING TECHNOLOGY

SecuLore Solutions is headquartered in Odenton, Maryland. All of our services utilize layer 2 cybersecurity technology that we design and manufacture in the USA.

PARTNERSHIP-FOCUSED CYBER TEAM

Paladin Overwatch provides you with a team of cyber experts who learn the baseline of your network and work with your IT team to evolve your cybersecurity over time.

We CYBER-PROTECT Our Nation’s Most Important Number: 9-1-1
**WHY SECULORE SOLUTIONS?**

An innovator in public-safety-focused cybersecurity, SecuLore Solutions is passionate about protecting critical services from cyber criminals. Led by experts in both 9-1-1 technology and cyber warfare, our team partners with public safety, local governments, and IT teams to provide training, tools, and support needed to defend our public infrastructure from increasingly sophisticated cyber attacks.

---

**WHAT DOES OVERWATCH INCLUDE?**

- **A Dedicated Cyber Analyst**
  A SecuLore cybersecurity analyst learns your network and is your dedicated partner in identifying & resolving vulnerabilities.

- **Daily Network Checks**
  SecuLore checks your network daily for suspicious changes in traffic behavior.

- **Weekly Cybersecurity Reports**
  SecuLore sends you an in-depth vulnerability report with remediation recommendations every week.

- **Automated Cybersecurity Alerts**
  SecuLore contacts you for urgent vulnerabilities found in your network based on your custom sensitivity levels.

- **No Maintenance or Replacement Fees**
  Paladin Overwatch is provided as a service and all upkeep and updates are on us.

---

**WHAT CAN YOU DO WITH PALADIN?**

- **Visualize Network Traffic 24/7**
  Paladin shows your network traffic with important details in real time, all the time.

- **Verify Firewall Configuration**
  Filter network traffic to systematically verify and fix your firewall rules for in-depth analysis of your network architecture.

- **Protect Critical Networks**
  Critical networks should be closed to the outside world. Validate that closed networks are truly closed.

- **Capture & Save Suspicious Data**
  Notice something suspicious? Save data for in-depth forensic analysis with one click.

---

**WANT TO LEARN MORE?**

VISIT OUR WEBSITE
www.SecuLore.com

SEND US AN EMAIL
info@SecuLore.com

GIVE US A CALL
410-305-0234
Toll Free: 844-732-8567

---

We CYBER-PROTECT Our Nation’s Most Important Number: 9-1-1
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.
SecuLore Solutions  
2288 Blue Water Blvd Suite #329  
Odenton, MD 21113  

<table>
<thead>
<tr>
<th>Name/Address</th>
</tr>
</thead>
</table>
| Mid-America Regional Council  
| Eric Winebrenner  
| 600 Broadway, Suite 200  
| Kansas City, MO 64105 |

<table>
<thead>
<tr>
<th>Date</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/23/19</td>
<td>8/22/19</td>
</tr>
</tbody>
</table>

| Quote # | QT-DM-072319-MARC-CBM51-HGAC |

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Ordered</th>
<th>U/M</th>
<th>Rate</th>
<th>Amount</th>
</tr>
</thead>
</table>
| CYBM-HG | Cybersecurity Benchmark based upon NIST, FCC, DHS and APCO guidelines  
Includes:  
Data Architecture review  
Network segmentation recommendations  
Traffic Analysis  
Initial vulnerability assessment | 1 | e/a | $8,500.00 | $8,500.00 |
| CYBBM-ADD | CyberBenchmark - Additional Segment  
Data capture and analysis from additional network segment beyond scope of base CyberBenchmark process | 47 | e/a | $2,000.00 | $94,000.00 |
| HGACBuy | contract number EC07-18 |
| | Subtotal | $102,500.00 |
| HGAC-CYBM | H-GAC CyberBenchmark Discount | 1 | e/a | ($1,020.00) | ($1,020.00) |
| SPDSC | Special Multi-Segment Discount | 47 | e/a | ($200.00) | ($9,400.00) |
| | David McSpadden  
| | SecuLore Solutions  
| | 512-868-5951  
| | david.mcspadden@seculore.com |

v6.14.19  
Good for 30 days from date of sales estimate  
Total $92,080.00
911 Real-Time Analytics

SirenGPS invites public safety agencies to deploy real-time, data-driven, artificial intelligence for 911.

Capitalizing on 911 Real-Time Analytics

Responding to a mass casualty incident requires public safety agencies to recognize the scale of a developing emergency. SirenGPS' 911 Real-Time Analytics monitors emergency calls to automatically detect terrorist attacks, active shooters, and other mass casualty incidents in real time.

Saving Time Means Saving Lives

Mass casualty incidents create a sudden need for more ambulances, police, and other services than we have available in a given community. These necessary resources from nearby mutual aid partners can arrive sooner when emergencies are quickly identified and information is shared automatically between all parties.

SirenGPS’ patented 911 Real-Time Analytics software analyzes the frequency, proximity, and location of 911 calls to identify mass casualty incidents. When the analytics indicate that a collaborative response is required, public safety and their mutual aid partners are automatically notified. This means ambulances, police, and emergency services arriving on the scene faster, when saving time means saving lives.

Time lost recognizing the need for mutual aid:

During the Aurora, Colorado movie theatre attack it took almost 11 minutes to recognize the need for mutual aid.

Seconds matter:
Sandy Hook
December 2012
26 lives lost in 6 min

Las Vegas
October 2017
58 lives lost in 10 min
How it Works

911 Real-Time Analytics plugs into your existing 911 computer-aided dispatch (CAD) API for a seamless integration. The analytics engine monitors emergency calls and applies a set of algorithms. These algorithms take into consideration the frequency, proximity and location of 911 calls, 911 call history for the location, historical 911 call activity for locations of the same type, as well as other factors to calculate a probability score.

Getting Started
No hardware or software installation and no training of personnel is needed for 911 Real-Time Analytics. Setup is limited to defining a list of contacts who will receive notifications of mass casualty events based on the analytics.
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.
Hardware and Network Setup

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><strong>PWR</strong></td>
<td>Power adapter input.</td>
</tr>
<tr>
<td><strong>USB</strong></td>
<td>Reserved. Do not connect peripherals to these ports.</td>
</tr>
<tr>
<td><strong>HDMI</strong></td>
<td>Reserved. Do not connect peripherals to this port.</td>
</tr>
<tr>
<td><strong>LAN</strong></td>
<td>Ethernet LAN port. Connect this port to the PSAP local area network.</td>
</tr>
<tr>
<td><strong>MGMT</strong></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).

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><strong>Global Public Safety</strong></td>
<td>TAC.10 CAD</td>
</tr>
<tr>
<td></td>
<td><a href="http://globalsoftwarecorp.com/">http://globalsoftwarecorp.com/</a></td>
</tr>
<tr>
<td><strong>CentralSquare Technologies</strong></td>
<td>CentralSquare CAD</td>
</tr>
<tr>
<td></td>
<td><a href="https://www.centralsquare.com/public-safety/cad">https://www.centralsquare.com/public-safety/cad</a></td>
</tr>
<tr>
<td><strong>Motorola Solutions</strong></td>
<td>PremierOne CAD</td>
</tr>
</tbody>
</table>
**Table 3. Supported CR Systems**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hexagon Safety &amp; Infrastructure</strong></td>
<td>Intergraph I/CAD <a href="https://www.hexagonsafetyinfrastructure.com/products/command-control-and-communications/intergraph-computer-aided-dispatch">https://www.hexagonsafetyinfrastructure.com/products/command-control-and-communications/intergraph-computer-aided-dispatch</a></td>
</tr>
<tr>
<td><strong>Harris Computer</strong></td>
<td>Global CAD <a href="https://globalsoftwarecorp.com/">https://globalsoftwarecorp.com/</a></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></td>
</tr>
<tr>
<td>LAN IP</td>
<td>Supplied by DHCP</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Supplied by DHCP</td>
</tr>
<tr>
<td>MGMT Network</td>
<td></td>
</tr>
<tr>
<td>MGMT IP</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>Subnet mask</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></td>
</tr>
<tr>
<td>Width</td>
<td>5.82&quot; (148mm)</td>
</tr>
<tr>
<td>Height</td>
<td>1.72&quot; (44mm)</td>
</tr>
<tr>
<td>Depth</td>
<td>4.64&quot; (118mm)</td>
</tr>
<tr>
<td>Package</td>
<td>5.5&quot; (H) x 9.5&quot; (W) x 8&quot; (D)</td>
</tr>
<tr>
<td>Weight</td>
<td></td>
</tr>
<tr>
<td>Gross Weight</td>
<td>3.52 lbs (1.6 kg)</td>
</tr>
<tr>
<td>Net Weight</td>
<td>2.2 lbs (1 kg)</td>
</tr>
<tr>
<td>Environmental</td>
<td></td>
</tr>
<tr>
<td>Operating</td>
<td>-20°C to 50°C (-4°F to 122°F)</td>
</tr>
<tr>
<td>Non-operating</td>
<td>-40°C to 70°C (-40°F to 158°F)</td>
</tr>
<tr>
<td>Operating</td>
<td>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
New technology or services often raise questions for public safety agencies. Does deploying this new service create the risk of a lawsuit? Could a lawsuit result if we make this available to some citizens and not others? What if the new service is not available all of the time? Happily, the law is clear in both Missouri and Kansas that public safety agencies have broad latitude to make decisions about how to achieve the mission. Public safety agency legal protections rooted in duty, discretion and sovereign immunity, are not the easiest concepts to understand. However, the reason for the protection is obvious: public safety agencies require legal protection to strive toward the goal of making communities safe.

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 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.
Duty, Discretion and Public Safety Technology Prerogative

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 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, Discretion and Public Safety Technology Prerogative

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.
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 are available for download at https://sirengps.com/misc/contract-documents
sirengps_911rta_service_agreement_terms_and_conditions_-_09.06.19.pdf

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

---

Page 2 of 3
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 is essentially theoretical, 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/about/resources.
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:
- Community event materials:
- 911 Day at the K attended by

Additional information to share:

- Telecommunicators Appreciation Celebration (TAC) planning in progress will be held in April 2020 at the Intercontinental Hotel on the Plaza.
- We would like to encourage participation in the Cell Phone Sally school program. We need each PSAP to identify 2 or 3 telecommunicators to participate in this program for your jurisdictions. Please let Sally know if you plan on participating in 2020.