**FY 2018-2019 Virginia Beach Budget**
**Response to Council Questions**

**Question Number**: FY 19 16

**Question:** What is the business case for police encryptions software and the potential of using public domain software encryption?

**Date Requested**: 3/20/2018

**Requested By**: Councilman Moss

**Department**: Police Department/Information Technology

**Response:**

Please see the attached document, “Police Radio Encryption: Business Case Document,” which was prepared for this project by the Police Department and IT.

# Police Radio Encryption

Business Case Document

*October 2, 2017*


Prepared by:

*Grady L. Bird*
*Public Safety IT Business Relationship Manager*

*George W. Simpson, IV*
*Public Safety IT Business Analyst*

*Lt. William C. Zelms*
*Support Division, Virginia Beach Police Department*

# Table of Contents

# 1 Executive Summary

The proposed Police Radio Encryption CIP is intended to fund the equipment and infrastructure improvements needed to allow all police-issued radios to operate on encrypted channels. This enhancement would greatly increase officer safety and decrease the likelihood for loss of life or injury to citizens who may be impacted by a criminal suspect listening to police communications.

With the prevalence of police scanner apps, as well as dedicated social media groups, officers are unable to securely discuss tactical information while in the midst of conducting an operation. This has allowed suspects to evade capture and has placed officers and citizens in greater danger.

Social media groups actively post real-time updates to police cases, as well as dispatch/police radio transmissions received via computer and/or phone-based apps. Social media group facilitators have even provided instructions to their members to provide assistance to officers who are on a call for service or traffic stop. While well-intentioned, this places both the officer and citizen in unnecessary danger.

Encrypting radio communications will:

- Improve operational safety of police officers
- Protect sensitive information
- Keep citizens out of harm's way

This request is to fund the implementation of AES Multi-key encryption on the City's public safety radio network. The proposed solution includes 2400 subscribers (radios) to cover all of VBPD, ECCS Dispatch, and priority liaisons across other departments and agencies.

# 2 Background

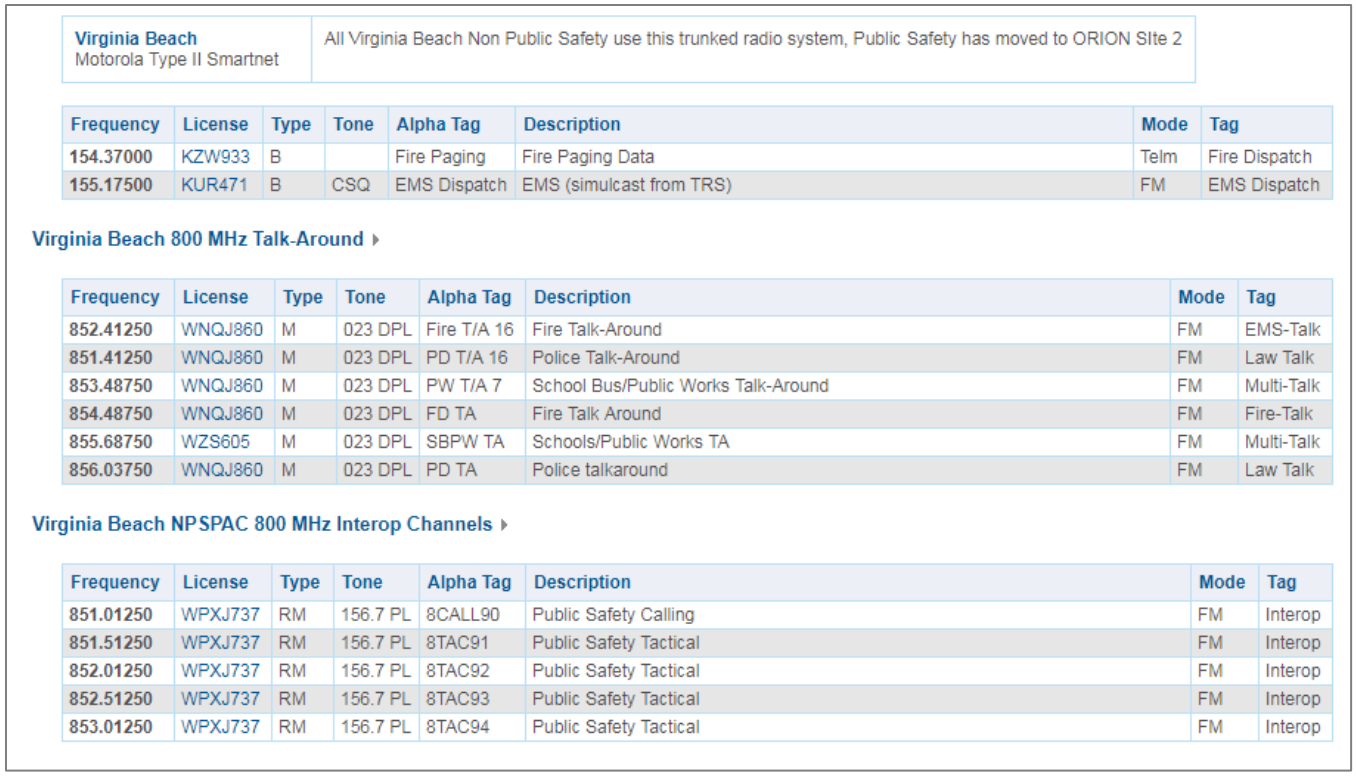
With the prevalence of police scanner apps, as well as dedicated social media groups, officers are unable to securely discuss tactical information while in the midst of conducting an operation. This has allowed suspects to evade capture and has placed officers and citizens in greater danger. The following examples highlight the critical and immediate need for encrypted police communications:

1. In 2011, Special Investigation Detectives were attempting to apprehend a suspect who was wanted for several counts of Burglary. Social media posts indicated he was hiding at a girlfriend's residence. Community Policing Squad officers surrounded the house and attempted to take the suspect into custody. All communications leading up to this point were done over the police-issued radios. When officers entered the residence, they were unable to locate the suspect. When he was apprehended at a later date, he informed detectives that he used a police scanner app on his phone to listen to the officers as they were approaching the house. He fled prior to a perimeter being set up.
2. In May 2016, Special Investigation Detectives debriefed a confidential informant to learn their drug-running habits. The informant told detectives that he and his associates used police scanners to scout if they are being followed.
3. In 2017, a confidential informant again told detectives that he and his associates regularly used police scanner apps to conduct surveillance on police activity prior to moving their narcotics.
4. On June 30, 2017, officers were involved in a vehicle pursuit of a male who was suspected of committing a sexual assault at Tidewater Community College. During the pursuit, the suspect was actively listening to police communications via app on his cell phone. The suspect crashed his vehicle after Stinger spikes were deployed, and was taken into custody without incident.
5. In July 2017, Special Investigations and SWAT were conducting a search warrant near Lynnhaven Mall. A supervisor was approached by a citizen who showed him a Facebook group who was posting every action they were taking. The group was monitoring communications and updating information on social media in real-time as the officers were preparing to make entry.

Another risk of using unencrypted communications is that it provides open access to sensitive information. A simple web search can reveal a listing of public safety radio frequencies. Scanners and apps make it easy for these channels to be monitored by anyone. During an emergency or event, the communication taking place could include personal or confidential information such as:

- Personally Identifiable Information (e.g. address, name, Social Security Number)
- Protected Health Information
- Criminal History
- Victim Identities

The subsequent release of this information can be done without verification. If the information is incorrect or misheard, the consequences can be disastrous. If authorities are looking for a suspect but have not had a chance to verify a description, the public will be looking for the wrong person – perhaps flooding emergency response with irrelevant phone calls and tips. Even worse, imagine the torment of hearing of a loved one's death via social media only to later find out the information was incorrect.



**Virginia Beach**
Motorola Type II Smartnet

All Virginia Beach Non Public Safety use this trunked radio system, Public Safety has moved to ORION SIte 2

| Frequency | License | Type | Tone | Alpha Tag | Description | Mode | Tag |
|---|---|---|---|---|---|---|---|
| 154.37000 | KZW933 | B | | Fire Paging | Fire Paging Data | Telm | Fire Dispatch |
| 155.17500 | KUR471 | B | CSQ | EMS Dispatch | EMS (simulcast from TRS) | FM | EMS Dispatch |

**Virginia Beach 800 MHz Talk-Around**

| Frequency | License | Type | Tone | Alpha Tag | Description | Mode | Tag |
|---|---|---|---|---|---|---|---|
| 852.41250 | WNQJ860 | M | 023 DPL | Fire T/A 16 | Fire Talk-Around | FM | EMS-Talk |
| 851.41250 | WNQJ860 | M | 023 DPL | PD T/A 16 | Police Talk-Around | FM | Law Talk |
| 853.48750 | WNQJ860 | M | 023 DPL | PW T/A 7 | School Bus/Public Works Talk-Around | FM | Multi-Talk |
| 854.48750 | WNQJ860 | M | 023 DPL | FD TA | Fire Talk Around | FM | Fire-Talk |
| 855.68750 | WZS605 | M | 023 DPL | SBPW TA | Schools/Public Works TA | FM | Multi-Talk |
| 856.03750 | WNQJ860 | M | 023 DPL | PD TA | Police talkaround | FM | Law Talk |

**Virginia Beach NPSPAC 800 MHz Interop Channels**

| Frequency | License | Type | Tone | Alpha Tag | Description | Mode | Tag |
|---|---|---|---|---|---|---|---|
| 851.01250 | WPXJ737 | RM | 156.7 PL | 8CALL90 | Public Safety Calling | FM | Interop |
| 851.51250 | WPXJ737 | RM | 156.7 PL | 8TAC91 | Public Safety Tactical | FM | Interop |
| 852.01250 | WPXJ737 | RM | 156.7 PL | 8TAC92 | Public Safety Tactical | FM | Interop |
| 852.51250 | WPXJ737 | RM | 156.7 PL | 8TAC93 | Public Safety Tactical | FM | Interop |
| 853.01250 | WPXJ737 | RM | 156.7 PL | 8TAC94 | Public Safety Tactical | FM | Interop |

**Figure 1 - Listing of Virginia Beach Radio Frequencies**[1]

Social media groups actively post real-time updates to police cases, as well as dispatch/police radio transmissions received via computer and/or phone-based apps. Group facilitators have even provided instructions to their members to provide assistance to officers who are on a call for service or traffic stop. While well-intentioned, this places both the officer and citizen in unnecessary danger.

[1] https://www.radioreference.com/apps/db/?ctid=2954


**Figure 2 – Posting of VBPD radio communications on social media**

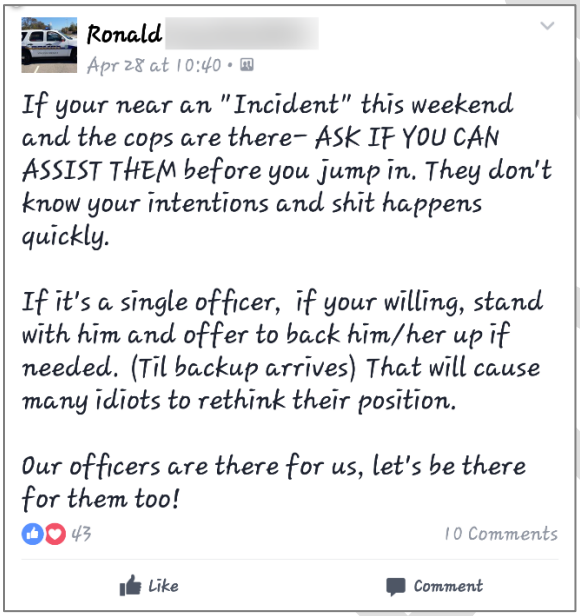



**Figure 3 - Social media groups being encouraged to step in and assist police officers**

Given the examples listed above and society's ever-increasing reliance and use of technology to receive and spread information, police radio encryption is of the utmost urgency.

# 3 Business Opportunity

## 3.1 Overview

The City's radio communications infrastructure is capable of integrating the components needed for encryption. Enabling this capability requires increasing channel capacity to handle the additional encryption key data that would be sent with each transmission. Additional servers and software would be deployed to handle the security and management of the encryption keys. Implementing a Key Management Facility (KMF) and Over-the-Air-Rekeying (OTAR) would allow for the encryption keys and devices to be centrally controlled, secured, and managed.

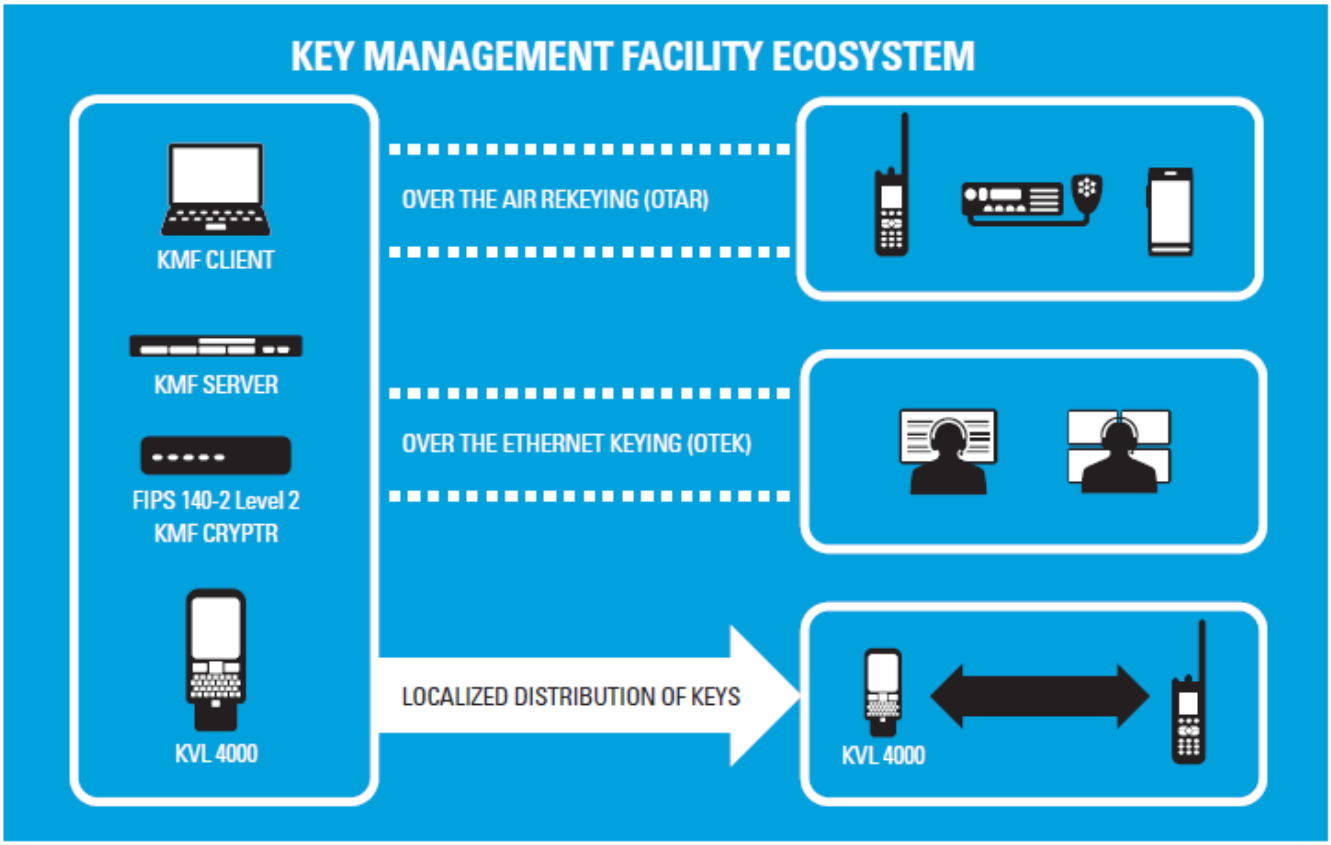



**Figure 4 - High-level view of encryption key management and dissemination**[2]

## 3.2 Goals

- Improve operational safety of police officers
- Protect sensitive information
- Keep citizens out of harm's way

[2] https://www.motorolasolutions.com/content/dam/msi/docs/business/products/two-way_radio_networks/key_management_facilities/key_management_facility/_documents/static_files/kmf_specsheet.pdf

## 3.3 Objectives

- Allow secure two-way voice communication between officers, dispatch, and other public safety officials
- Maintain security and privacy of criminal history, personally identifiable information (PII), and personal health information (PHI)
- Be available for use by schools, fire department, sheriff's office, local military liaisons, and other agencies providing mutual aid
- Encrypt communication among approximately 2400 radio units
- Increase channel capacity for transmission of encryption keys and data
- Management and administration of encryption keys
- Maintain capability to communicate on open channels in cases of mutual aid

## 3.4 Strategic Alignment

### 3.4.1 City Council Goals

- **Goal 5 - Be a Competitive First Class Resort for Residents, Businesses, and Tourists**
  - 5.1 - Safer and more inviting environment for families: 24 hours a day
- **Goal 6 - Be the Safest City in Virginia**
  - 6.1 - Maintain lowest crime rate in Virginia with the highest clearance rate.
  - 6.3 - Be prepared for, respond to, and recover from catastrophic events.
  - 6.4 - Have a well-trained, well equipped public safety staff.
- **Goal 9 - Data and Technology Is Used To Enhance Community Livability, Prosperity, and Sustainability**
  - 9.6 - The City is recognized as a leader in technology.

### 3.4.2 Communities of Interest

- **Public Safety**

### 3.4.3 Master Technology Plan Alignment

- **Improve Infrastructure and Operations**
  - I 7- Develop a sustainable funding source for essential technology infrastructure
  - I8 - Develop, fund and execute a City-wide radio system strategy

### 3.4.4 Mandates, Regulations, Policies:

- **Yes**

Criminal Justice Information System (CJIS) and the Virginia Criminal Information Network (VCIN) mandate the protection of sensitive information such as Criminal History and PII/PHI.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) legislates security and privacy of Personal Health Information.

## 3.5 Solution Scope

This solution includes business analysis, requirements gathering, technical design, encryption servers, software licenses, programming of radios, and management of encryption keys and services. This is primarily limited to

Virginia Beach Police Department and ECCS (dispatch). Additional budget has been included to cover implementation on priority devices within other departments/agencies, for a total of 2400 subscriber units.

This solution is for the encryption of voice communications only and does not cover all radio communications within the City.

## 3.6 Stakeholder List

| Name | Title | Department | Role |
|---|---|---|---|
| James A. Cervera | Chief | Virginia Beach Police Department | Sponsor |
| Billy Zelms | Lt, Support Division | Virginia Beach Police Department | Key Stakeholder |
| Stephen Williams | Director | Emergency Communications and Citizen Services | Key Stakeholder |
| Mutual Aid Agencies | | VBFD,VBEMS, FEMA, etc | Key Stakeholder |
| Marc St. Clair | Unified Communications | Information Technology | Key Stakeholder |

## 3.7 Dependencies or Constraints

- Open channels must be planned for and maintained.
- A phased approach to implementation may cause interruptions to all public safety communications.
- Only radios with this capability enabled will be able to communicate via encrypted channels.
- Cannot impede emergency dispatch operations.

## 3.8 Assumptions

No assumptions at this time.

## 3.9 Risks

- Impacts to other departments and agencies must be mitigated.
- Loss of functionality, even temporarily, can result from improper planning or implementation.
- Limiting the ability of citizens to listen to direct communications could be perceived as removing transparency from government.

## 3.10 Business Continuity Issues

This solution will become the primary means of communication for the Police Department. As a result, infrastructure and services must remain operational and provide at least basic radio communication at all times.

## 3.11 Consequences of Inaction

As demonstrated above, use of the current system increases the danger to officers and citizens.

# 4 Recommendation

The recommended approach is to complete a business analysis including technical and functional requirements, architectural designs, and implementation plan. Following the analysis, the solution will be finalized and implemented accordingly.

## 4.1 Justification/Rationale

Radio communications are a critical path for information during public safety events and operations. Implementing new technologies or processes involves a multitude of agencies, departments, and units. These entities cooperate across jurisdictional boundaries and transcend all levels of government. Avoiding disruption on such a large scale requires careful planning and execution. The analysis phase included in this approach serves to identify possible negative impacts and develop strategies for mitigating those impacts.

## 4.2 Implementation Factors

Total estimated implementation duration is *9-12* months.

### 4.2.1 Resource Needs and Capabilities

| Analysis | # Months | Hours | % Allocation | Total Hours | FTC Rate | Total FTC |
|---|---|---|---|---|---|---|
| **Project Manager** | 3 | 504 | 10.00% | 50.4 | 104 | **$5,242** |
| **System Analyst** | 3 | 504 | 10.00% | 50.4 | 97 | **$4,889** |
| **Business Analyst** | 3 | 504 | 25.00% | 126 | 100 | **$12,600** |
| **Network Engineer** | 3 | 504 | 10.00% | 50.4 | 111 | **$5,594** |
| **Radio Engineer** | 3 | 504 | 10.00% | 50.4 | 122 | **$6,149** |
| **Total** | | | | | | **$34,474** |

| Implementation | # Months | Hours | % Allocation | Total Hours | Rate | Total |
|---|---|---|---|---|---|---|
| **Project Manager** | 9 | 1512 | 15.00% | 226.8 | 104 | **$23,587** |
| **Systems Analyst** | 9 | 1512 | 5.00% | 75.6 | 97 | **$7,333** |
| **Business Analyst** | 9 | 1512 | 5.00% | 75.6 | 100 | **$7,560** |
| **Software Engineer** | 9 | 1512 | 20.00% | 302.4 | 105 | **$31,752** |
| **Systems Engineer** | 9 | 1512 | 40.00% | 604.8 | 105 | **$63,504** |
| **Network Engineer** | 9 | 1512 | 25.00% | 378 | 111 | **$41,958** |
| **Radio Engineer** | 9 | 1512 | 75.00% | 1134 | 122 | **$138,348** |
| **Total** | | | | | | **$314,042** |

| **Grand Total Implementation and Analysis** | **$348,516** |
|---|---|

### 4.2.2 Scheduling and Resources

Resources are assumed to be available at the time funding is approved.

### 4.2.3 Sustainment and Support

Management of encryption keys and services is expected to require full-time support. Due to the critical nature of these services, it is preferable to rely on contract staff from the vendor in order to maintain necessary service levels.

- The estimated cost for this support is $250k annually.

## 4.3 Financial Measures

### 4.3.1 Implementation Costs

| **Implementation Costs** | **Amount** |
|---|---|
| IT Professional Services | $348,516 |
| Licensing Fees | $48,000 |
| Software | $2,800,000 |
| Hardware | $40,000 |
| Vendor Professional Services (for configuration and upgrade) | $1,100,000 |
| Implementation Reserve (15%) | $650,477 |
| **Total** | **$4,986,993** |

### 4.3.2 Total Cost of Ownership

| **One Time Costs** | | | | | | | |
|---|---|---|---|---|---|---|---|
| Analysis and Implementation | **$4,986,993** | | | | | | |
| **On-going Costs** | | | | | | | |
| | **Year 1** | **Year 2** | **Year 3** | **Year 4** | **Year 5** | **Year 6** | **Total** |
| IT Support | | | | | | | |
| Vendor Support | | $250,000 | $250,000 | $250,000 | $250,000 | $250,000 | **$1,250,000** |
| Other On-going costs | | | | | | | |
| **Total** | **$4,986,993** | **$250,000** | **$250,000** | **$250,000** | **$250,000** | **$250,000** | **$6,236,993** |

# 5 Acceptance and Approval

## 5.1 Peer Review

The name(s) and signature(s) below indicate that the Business Case has been peer reviewed and accepted. All requested modifications to this document have been incorporated as requested, and the Business Case is ready for EMT and/or sponsor review.

| Name | Role | Date | Signature |
|---|---|---|---|
| Grady L. Bird | Public Safety CBRM | 10/25/17 | |
| | | | |
| | | | |

## 5.2 Sponsor

Signature below indicates agreement that the Business Opportunity is accurately represented and that the recommended approach is reasonably expected to achieve the desired outcomes.

James A. Cervera — Date

Police Chief

## 5.3 IT

Signature below indicates approval of the recommendation(s) presented herein, and authorizes the use of IT resources as indicated (pending availability and prioritization).

Pedro “Peter” Wallace — Date

Chief Information Officer

Ed Feeney — Date

Darrell Riddick — Date

# Attachment A – Community of Interest Business Imperative

## Community of Interest: Public Safety

### Scoring

Each FY 19 CIP Funding Request was scored using the IRB Scoring Worksheet with the following results.

| CIP | Score |
|---|---|
| 3.701 First Responders Traffic Signal Preemption | 59 |
| 3.710 911 Call Taker/Dispatch Stations | 59 |
| 3.702 Emergency Management System | 57 |
| CIT-04 Police Radio Encryption | 54 |
| CIT-01 Fire & EMS Station Collaboration Solution | 47 |
| 3.609 Smart 911 and Rave Panic Button | 47 |

### Steering Committee Ranking

The Public Safety Steering Committee met in closed session on Thursday, October 12th and reviewed the IRB Scoring recommendations for the six Public Safety FY 19 CIP Funding Requests. The Committee recommended the following priority as a business imperative ranking:

1. Police Radio Encryption
2. 911 Call Taker/Dispatch Stations
3. Emergency Management System
4. Fire & EMS Station Collaboration Tool
5. First Responders Traffic Signal Preemption
6. Smart 911 and Rave Panic Button

### Advisory Board Ranking

The Public Safety Advisory Board met on Wednesday, October 18th and reviewed the IRB Scoring recommendations for the six Public Safety FY 19 CIP Funding Requests. The Advisory Board recommended the following priority as a business imperative ranking:

1. Police Radio Encryption
2. 911 Call Taker/Dispatch Stations
3. Emergency Management System
4. Fire & EMS Station Collaboration Tool
5. First Responders Traffic Signal Preemption

Stephen Williams, the Director of ECCS, withdrew Smart 911 and Rave Panic Button.