

# ENCRYPTION NEEDS IN IOWA



## Table of Contents

<b>I. Introduction</b> .....	2
<b>II. Geography of Iowa</b> .....	2
<b>III. Demographics of User Agencies and Home Jurisdictions</b> .....	3
<b>IV. Current Technological State for Users</b> .....	4
<b>V. State Desire for Interoperable Encryption</b> .....	4
<b>VI. Technological Recommendation to the ISICSB</b> .....	4
<b>VII. Technological, Logistical and Fiscal Barriers</b> .....	5
<b>VIII. Discussion</b> .....	6
<b>IX. Proposed Solutions</b> .....	6
<b>X. Conclusion</b> .....	7
<b>Appendix A. Acknowledgements</b> .....	8
<b>Appendix B. ISICSB TR-2018-002: Technical Recommendation for Multi-Key Equipped Subscriber Units</b> .....	9

## I. Introduction

In December of 2016, the State of Iowa committed to build a statewide APCO Project 25 (P25) interoperable land mobile radio (LMR) network. The Iowa Statewide Interoperable Communications System (ISICS) is codified as the interoperable communications platform in Iowa<sup>1</sup> and is governed by the Iowa Statewide Interoperable Communications System Board (ISICSB).<sup>2</sup> The ISICS LMR network is specified to deliver at least 95% mobile radio coverage with delivered audio quality (DAQ) of 3.4 or better with 99.999% reliability. A map of the sites as of February 2018 is shown in Figure 1.

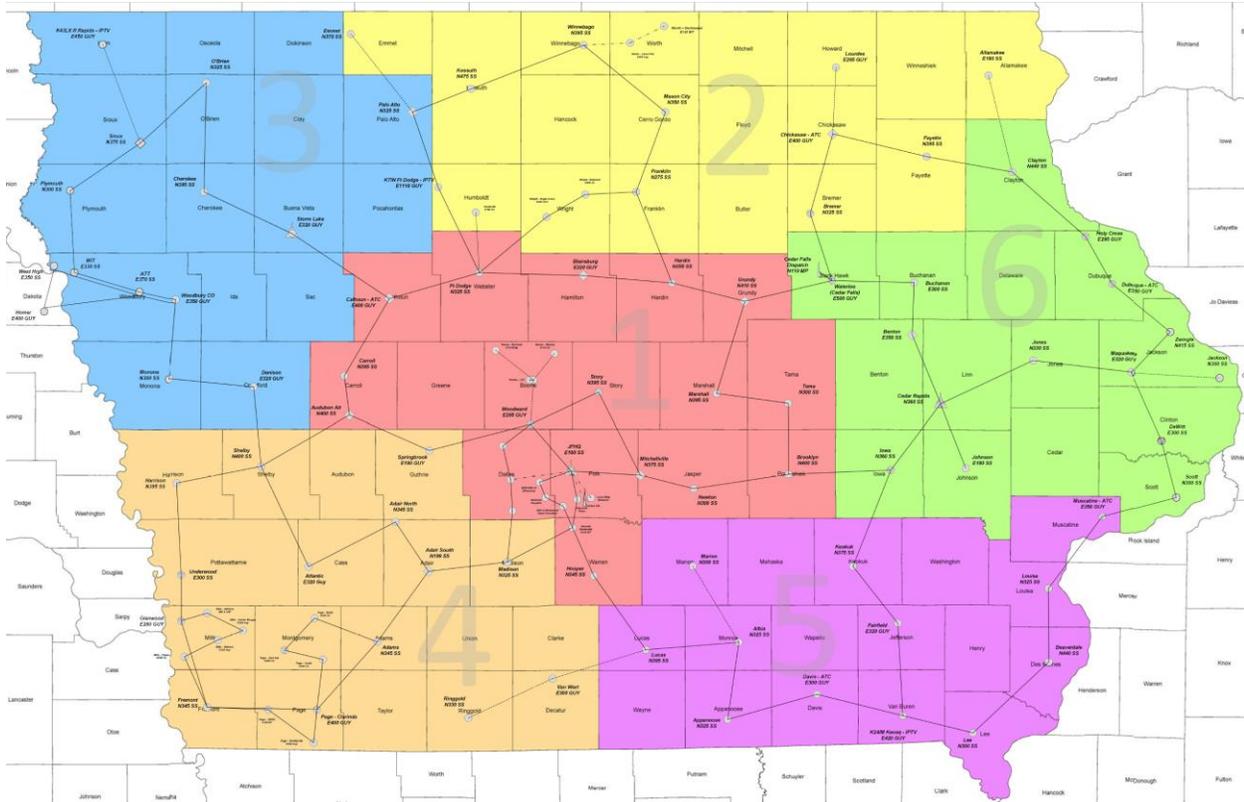


Figure 1. Layout of the ISICS Network with various Homeland Security Regions shaded.

The desired use of the network is primarily for interoperable communications on varying scales including day-to-day interoperability. Local, state and federal agencies in the public safety and public service disciplines are eligible to join the network for interoperable and, if desired, operable use. Local users are able to add additional infrastructure to the network to enhance portable in-building coverage.

## II. Geography of Iowa

Figure 1 also conveys that Iowa is a relatively geographically large state that spans 56,273 square miles. The terrain in Iowa varies greatly from flat lands to rolling hills and bluffs along river beds especially in

<sup>1</sup> Iowa Code [29C.23](#).

<sup>2</sup> Iowa Code [80.28](#) and [80.29](#).

Eastern Iowa. Expansive agricultural land is intertwined with robust timber area, rural communities and larger metropolitan areas.

### III. Demographics of User Agencies and Home Jurisdictions

There are nearly 400 law enforcement agencies with approximately 5,800 sworn officers<sup>3</sup> that are tasked with enforcing laws in Iowa. In addition to law enforcement, 732 fire departments serve Iowa's 3,145,711 residents<sup>4</sup>. Of the fire departments, approximately 90% of the personnel are volunteer<sup>5</sup>.

Iowa's population distribution has undergone an evolution over the past decade (Figure 2)<sup>6</sup>. It is estimated that only ten of 99 counties have populations exceeding 65,000. The vast majority of counties have populations that range between 5,000 and 19,999 residents. Only 27 counties have estimated population growth from April 1, 2010 to July 1, 2017.

### Iowa County Population and Percent Change

(from April 1, 2010 population estimates base to July 1, 2017)

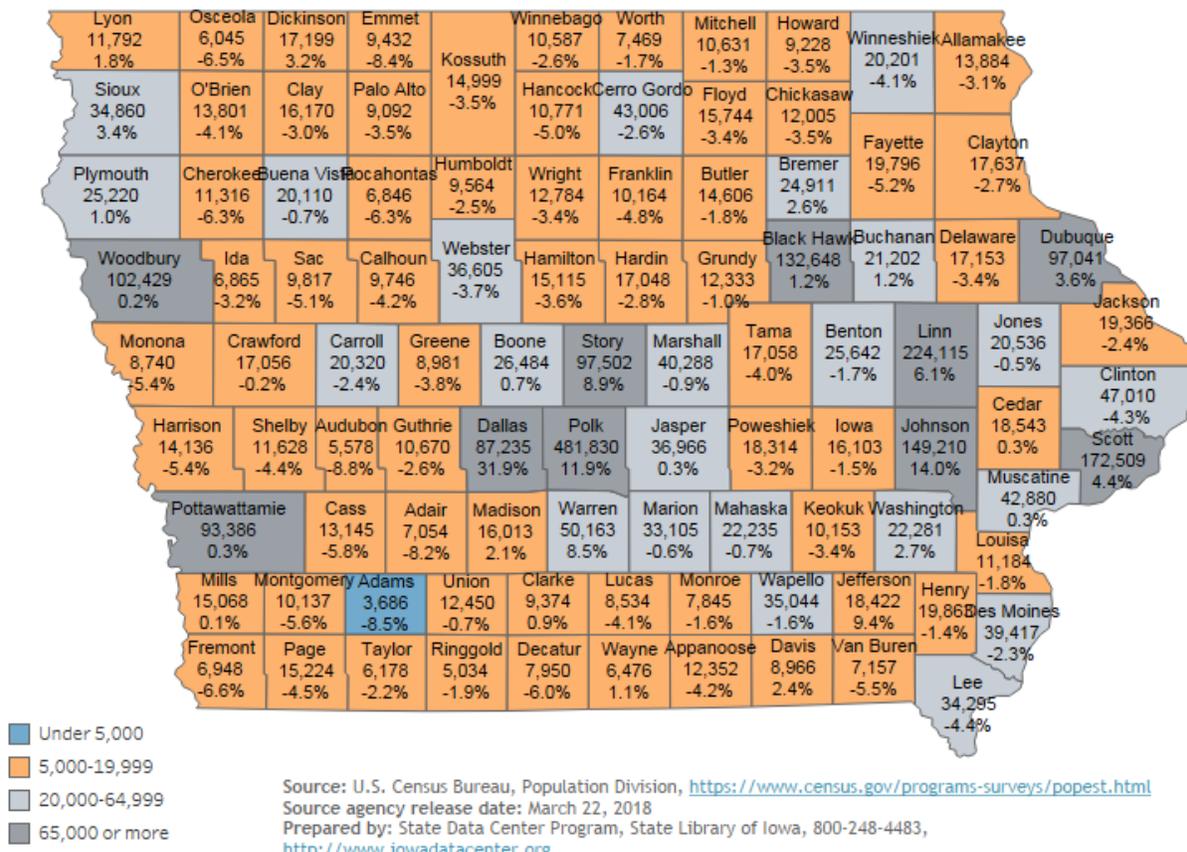


Figure 2. Iowa population and estimated population change map from April 1, 2010 to July 1, 2017.

<sup>3</sup> US Bureau of Justice Statistics' 2008 *Census of State and Local Law Enforcement Agencies*

<sup>4</sup> <https://www.census.gov/quickfacts/fact/table/ia,US/PST045217>

<sup>5</sup> <https://apps.usfa.fema.gov/registry/summary#stateTotalsTable>

<sup>6</sup> <http://www.iowadatatcenter.org/data/estimates>

The general taxable based in Iowa has also changed. Recent statistics show that only 43 of 99 counties have taxable values (excluding utilities) that exceed \$1 billion. Of the remaining counties, 13 have taxable values (excluding utilities) below \$500 million<sup>7</sup>.

Crime statistics in Iowa are put into two categories—violent and property. Property crime includes things like robbery, burglary, larceny, arson and motor vehicle theft. Violent crime includes murder, rape and aggravated assault.

From 2010<sup>8</sup> through 2016<sup>9</sup>, the overall trend of property crime has been decreasing at a county level with 63 of 99 counties reporting decreases in property crime (average crime rate per 100,000 people). That same time period has seen an overall increase in violent crime at the county level. Of the counties in Iowa, 66 of 99 counties reported an increase in violent crime. Of the counties reporting increases in crime, only three counties with increases in property crimes saw their populations increase. For violent crime, only 17 of the 66 counties that reported increases saw an increase in population. From these statistics, it is possible to infer that crime statistics do not correlate directly with population changes.

#### **IV. Current Technological State for Users**

Iowa's 2017 *State Communication Interoperability Plan*<sup>10</sup> outlined several items related to land mobile radio (LMR) communications in Iowa. Roughly 70% of Iowa agencies still rely on VHF. There are a few regional LMR networks that are not uniform in their frequency band, numerous disparate county-level networks and the Iowa Statewide Interoperable Communications System (ISICS).

Within these networks, there is a mixture of encryption algorithms that are currently employed. They include DES and DES variants, ADP, ARC4 and AES-256. Each network with deployed encryption uses different methodologies to manage key updates such as a key fill device (KFD) or over-the-air rekeying (OTAR).

#### **V. State Desire for Interoperable Encryption**

The ISICSB created the Encryption Subcommittee under the supervision of the Technology Committee in August 2017 to investigate the need for, deployment and management of encrypted interoperable talkgroups on the ISICS LMR Platform. Various scenarios were discussed based on severity of impact to life and property of citizens and public safety personnel.

These scenarios ranged from coordinated high-risk operations that span multiple agencies or a large geographical area, sensitive operations involving dignitaries, aviation incidents and others. After reviewing the scenarios, the Encryption Subcommittee concluded that there is a developing and evolving operational need for encrypted interoperability in Iowa.

#### **VI. Technological Recommendation to the ISICSB**

---

<sup>7</sup> <https://dom.iowa.gov/document/county-taxable-tif-valuations-class-ay2016fy2018>

<sup>8</sup> [http://www.dps.state.ia.us/commis/ucr/2010/iacrime\\_2010.shtml](http://www.dps.state.ia.us/commis/ucr/2010/iacrime_2010.shtml)

<sup>9</sup> [http://www.dps.state.ia.us/commis/ucr/2016/iacrime\\_2016.shtml](http://www.dps.state.ia.us/commis/ucr/2016/iacrime_2016.shtml)

<sup>10</sup> [https://isicbsb.iowa.gov/sites/default/files/documents/2017/10/iowa\\_scip\\_10-11-17\\_draftv4\\_clean.pdf](https://isicbsb.iowa.gov/sites/default/files/documents/2017/10/iowa_scip_10-11-17_draftv4_clean.pdf)

The Encryption Subcommittee continued to meet regularly for the next several months. Topics of discussion ranged from technological obstacles to logistical concerns that included the deployment and management of key material. A meeting was held with members of TR-8.3 to assist with various technical aspects of encryption on an interoperable LMR system. From that meeting a technical recommendation<sup>11</sup> ([Appendix B](#)) was drafted and adopted by the ISICSB that stated:

*...encrypted interoperable talk groups specified in the Detailed Design Review (DDR) be left in the programming code plug for user groups. However, encrypted interoperable talk groups should remain inactive until encryption is deployed and tested on the ISICS Platform. This includes dissemination of traffic encryption keys (TEK) and dissemination and enactment of policies and procedures that affect encrypted interoperable communication along with associated costs.*

*...  
Given this acquired information and set of conclusions, the Encryption Subcommittee submits a technical recommendation to ISICSB that users of the ISICS Platform who have a desire to utilize secure, encrypted interoperable talk groups available in the ISICS Regional Interoperable and Statewide Talk Groups Fleet Map purchase multi key subscriber units.*

## VII. Technological, Logistical and Fiscal Barriers

The Encryption Subcommittee met several more times to discuss the technological and logistical barriers that may present themselves with the deployment and management of encrypted interoperable talkgroups. Research was conducted to discover what Iowa counties and other states are using for their statewide LMR networks with respect to encryption algorithms and if a defined key update cycle existed. From that research, some commonalities were discovered:

1. Some counties use vendor proprietary encryption algorithms and update their key material with yearly maintenance cycles;
2. Some agencies use encryption but have not updated their keys due to concerns with orphaned radios, a lack of understanding of OTAR and backward compatibility with TEKs;
3. Some local agencies will contract with a vendor to manage their encryption programs. They may or may not employ OTAR as a strategy for updating key material.
4. States that use OTAR have everyone on the same KMF, but agencies outside of the state are not considered;

Iowa is a geographically sizeable state with 56,273 square miles with a very diverse array of users. With respect to the logistics of key update cycles, a very short update cycle may prove burdensome.

While some of the concerns raised in the previous set of bullet points may be addressed with training and planning, the Encryption Subcommittee identified several technological barriers that may prevent effective deployment and management of key material used for the encrypted interoperable talkgroups on ISICS. Given the array of deployed systems and networks in Iowa, it has to be assumed that each network is possibly utilizing a unique key management facility (KMF). While a standard exists for inter-KMF communication, not every manufacturer has chosen to adopt it into products.

A technological barrier was identified as well with subscriber units. At the time of this writing, each subscriber unit is only capable of utilizing one unique key encryption key (UKEK). This precludes subscriber radios from communicating with multiple KMFs even though they may be able to register and

---

<sup>11</sup> [ISICSB TR-2018-002](#)

affiliate with multiple P25 LMR networks. In this case, a subscriber unit may not be able to utilize the ISICS KMF because it will only be able to accept key material from its home system's KMF.

In addition, shortcomings were identified with updating KFDs and consoles. They are not universally updatable via internet protocol or via the LMR network. Without over-the-ethernet keying (OTEK), over-the-internet keying (OTIK) or OTAR, each of these devices would have to be updated manually by the System Administrator or his/her designee. This is laborious and time-consuming and may require too many full-time employees (FTE) for agency budgets.

## VIII. Discussion

A greater demand is being placed on public safety to appropriately address various concerns related to public safety while addressing the possibility of shrinking budgets. These demands include decreasing population but rising violent crime, an increased focus on preventing terror and a higher priority on security details that may involve several agencies. The potential desire and need for secure interoperable communications is increasing. An abundance of disparate systems with varying capabilities will preclude a single solution for several reasons:

1. Agencies may have their own KMF, and those agencies' subscriber units would be unable to connect to a different KMF for an interoperable LMR system;
2. Agencies may use encryption but not have OTAR;
3. Some devices are incapable of OTAR, or it is not practical and requires a new protocol that would need to be standardized using IP capabilities of wired local area networks and in some instances Internet access;
4. KMFs cannot universally communicate with each other as not all manufacturers have adopted the inter-KMF communication standard.

However a multifaceted approach to improving pathways for key material management will allow agencies who require encrypted communications more flexibility in deploying and managing key material with a lower overall cost. These pathways may include updates and expansion of TIA-102 standards and relatively uniform adoption of those standards.

## IX. Proposed Solutions

The Encryption Subcommittee has concluded that several steps by standards-setting entities and manufacturers could alleviate many of the technological and logistical barriers that pertain to statewide LMR networks and effective management of encrypted interoperable talkgroups.

First, a standardization and uniform adoption of an OTEK/OTIK would allow for seamless updates of key material for devices. This includes but is not limited to devices that would have the ability to access local area networks and the Internet via secure tunnels (VPN, SSH, etc) for remote access to a KMF such as consoles, recorders, KFDs and other products that have or will have limited or no RF access to an LMR network but may need to incorporate, access and/or distribute various encryption key material. Any updates should be accomplished with little or no user intervention.

The ability of OTEK/OTIK should include the ability to:

- Load and change TEKs and KEKs
- Setting initial and modifying existing management periods

- Flexibility in interfacing with multiple key management devices
- Ability for a Master KMF (defined below) to create and modify partitions on the crypto module

Secondly, a standard and uniform adoption of inter-KMF communications would allow for agencies that utilize their own KMFs to share key material among themselves. This would facilitate faster key updates for agencies that need to interoperate with each other on a common platform, but operate on disparate systems.

The Encryption Subcommittee recognizes that a request for manufacturers to incorporate an existing standard into a product goes beyond the scope of any standards-setting bodies. However, the Encryption Subcommittee also sees the need for stating that this standard should be incorporated into products to ensure that standard capabilities exist among SUs utilized by users that need an increasing level of security and operational flexibility.

Thirdly, a standardization and uniform adoption of multiple KMF communications for subscriber units would allow field personnel to register and affiliate with various LMR systems and update their key material via OTAR. This would allow for field operatives that rarely visit a radio shop but still need to utilize multiple LMR systems for operations to ensure that they have the most current key material installed in their devices.

This could be accomplished by establishing the home system KMF as the Master KMF for the subscriber unit. The Master KMF would be set to recognize the UKEKs, KEKs and TEKs from foreign systems and their quantity, partition and location the crypto module appropriately. Once that programming is complete, any other KMF that a SU would affiliate with is considered a Secondary KMF and only has access to its partition of the crypto module. The Master KMF would be able to add/remove foreign system partitions to a SU.

The partitioning of the crypto module should allow floating or aliased SLN assignment to add flexibility to programming and partitioning.

Then any foreign conventional or trunked radio system programmed into the SU with its own KMF would have the ability to modify its partition on the crypto module.

The theoretical maximum of possible Secondary KMFs should be directly tied to the number of available programming slots in a SU. This would allow SUs that may be tied to dozens of systems to utilize OTAR capabilities to update the key material pertinent to that particular foreign system.

Upon programming of a SU, the appropriate KMF address would be included into any trunked or conventional P25 system parameters. If an incorrect address is entered, the SU should notify the user upon completed registration and affiliation that the pertinent KMF is unreachable so that corrective action can be taken.

## **X. Conclusion**

The Encryption Subcommittee acknowledges that modern secure interoperable communications are possible under some but not all circumstances. There are various steps that standards-setting bodies and manufacturers can take that would enhance the abilities of agencies to deploy and manage encryption key material on various scales. As a result, the ISICSB fully supports the development and

implementation of standards and features that enhance the interoperable communications in an encrypted environment.

## Appendix A. Acknowledgements

The members of the Encryption Subcommittee have put in numerous hours discussing problems that affect aspects of effectively deploying and managing AES-256 encryption on statewide interoperable talkgroups. The members of the Committee are as follows:

- Special Agent in Charge CJ Noelck, Iowa Department of Criminal Investigation
- Captain David Ness, Des Moines Police Department
- Rob Dehnert, Westcom
- Eric Nevins, Des Moines Police Department
- District Chief Curtis Walser, Cedar Rapids Fire Department
- John Simons, Air Marshalls Service
- Trooper Nathan Rippey, Iowa State Patrol
- Scott Richardson, Iowa Department of Public Safety
- Assistant Chief Paul Feddersen, Iowa Department of Criminal Investigation
- Sergeant Heath Hove, Iowa State Patrol
- Dave Brittain, Iowa Department of Public Safety
- Rhonda McKibben, Iowa Department of Public Safety
- Lieutenant Mike Kasper, Linn County Sheriff's Office
- Sheriff Rob Rotter, Iowa County Sheriff's Office
- Lieutenant Josh Hale, Iowa State University Police Department
- Glen Sedivy, Woodbury County Communications Center Director
- Chief Greg Chia, Indianola Fire Department
- Andy Buffington, Winnebago/Hancock County Emergency Management
- Robert Carothers, Des Moines Police Department
- Patrick Updike, Iowa Department of Corrections

Several members of the Federal Partnership for Interoperable Communications, TR-8.3 and the P25 Steering Committee assisted the Encryption Subcommittee with their mission. The ISICSB and Encryption Subcommittee would like to thank:

- Andy Davis, TIA/TR-8.3, Motorola
- Jim Downs, DHS/FPIC
- Josh Johnson, TIA/TR-8.3, EF Johnson
- Alan Massie, FBI
- Paul McCarty, Harris
- Roger Strope, Missouri
- Derek Wells, TIA/TR-8.3, Harris

## **Appendix B. ISICSB TR-2018-002: Technical Recommendation for Multi-Key Equipped Subscriber Units**

## Technical Recommendation for Multi-Key Equipped Subscriber Units

### ISICSB TR-2018-002

John R. Benson  
HSEMD

Andy Buffington  
Communications Center

Linda Frederiksen  
EMS

Larry Smith  
Emergency Management

Kelly Groskurth  
Member At-Large

Ellen Hagen  
Fire Department (Volunteer)

Rob Rotter  
Sheriff's Office

Michael Kasper  
Sheriff's Office

Deb Krebill  
Fire Department

Tom Lampe  
Iowa DPS

Jason Leonard  
Municipal Police Department

Carole Lund-Smith  
ILEA

David Ness  
Municipal Police Department

Denise Pavlik  
Communications Center

Marty Smith  
Iowa DPH

Jeff Sundholm  
Iowa DOT

Jeffery Swearngin  
Iowa DNR

Patrick Updike  
Iowa DOC

Bob von Wolffradt  
Office of the CIO

Legislative Members  
Senator Jim Lykam  
Senator Randy Feenstra  
Representative Bob Kressig  
Representative Steven Holt

#### Executive Summary and Technical Recommendation:

The Encryption Subcommittee has convened regularly since August of 2017. In this time, the Subcommittee has assessed the need for encrypted interoperable talk groups and explored the technical issues with an encrypted interoperable environment. Given this acquired information and set of conclusions, the Encryption Subcommittee submits a technical recommendation to ISICSB that users of the ISICS Platform who have a desire to utilize secure, encrypted interoperable talk groups available in the ISICS Regional Interoperable and Statewide Talk Groups Fleet Map purchase multi key subscriber units.

The Encryption Subcommittee recommends that the encrypted interoperable talk groups specified in the Detailed Design Review (DDR) be left in the programming code plug for user groups. However, encrypted interoperable talk groups should remain inactive until encryption is deployed and tested on the ISICS Platform. This includes dissemination of traffic encryption keys (TEK) and dissemination and enactment of policies and procedures that affect encrypted interoperable communication along with associated costs.

The Encryption Subcommittee also recommends designations be made for suggested use of some interoperable talk groups.

These recommendations apply to the specified encrypted interoperable talk groups on the ISICS fleet map. This does not apply to local geopolitical operable talk groups.

These recommendations do not apply to a local agency or entity that may want to utilize vendor-specific encryption algorithms and schemes or Data Encryption Standard (DES) variants for local operability.

#### Summary of Proceedings:

The current land mobile radio (LMR) landscape in Iowa consists of several district networks that are often oriented around geopolitical boundaries or subdivisions. The vast majority of these networks operate in the conventional VHF spectrum. Primary interoperable communications pathways in the past have been done without encryption (in the clear).

The buildout of the P25 Phase II trunked Iowa Statewide Interoperable Communications System (ISICS) Platform presents several new opportunities for interoperable communications that did not previously exist in Iowa. In addition to statewide coverage and more user capacity, one of these new features is encryption on interoperable talk groups.

John R. Benson  
HSEMD

Andy Buffington  
Communications Center

Linda Frederiksen  
EMS

Larry Smith  
Emergency Management

Kelly Groskurth  
Member At-Large

Ellen Hagen  
Fire Department (Volunteer)

Rob Rotter  
Sheriff's Office

Michael Kasper  
Sheriff's Office

Deb Krebill  
Fire Department

Tom Lampe  
Iowa DPS

Jason Leonard  
Municipal Police Department

Carole Lund-Smith  
ILEA

David Ness  
Municipal Police Department

Denise Pavlik  
Communications Center

Marty Smith  
Iowa DPH

Jeff Sundholm  
Iowa DOT

Jeffery Sweargin  
Iowa DNR

Patrick Updike  
Iowa DOC

Bob von Wolffradt  
Office of the CIO

Legislative Members  
Senator Jim Lykam  
Senator Randy Feenstra  
Representative Bob Kressig  
Representative Steven Holt

Up to three encrypted interoperable talk groups were allocated for each region and statewide for a total of 21 encrypted interoperable talk groups during the detailed design review (DDR) in 2015. The preferred method of encryption was to be AES256.

The Encryption Subcommittee convened for the first time in August 2017 to explore encrypted interoperable talk groups on the ISICS Platform and develop recommendations and policies for encrypted interoperable talk groups on ISICS. The Subcommittee is comprised of representatives from a local municipal dispatch center, State of Iowa Radio Dispatch, State of Iowa technicians, local sheriff's office representatives, federal law enforcement, local municipal police and fire, state university police, emergency management, Iowa State Patrol, Iowa Department of Criminal Investigation and statewide interoperability coordinator.

In the first meeting, a desire for secure communication was conveyed among the various user group representatives. Several scenarios were identified in which encrypted interoperable channels would benefit multi-agency and/or multijurisdictional communications during planned and unplanned events.

In addition, it was recognized that federal agencies are obligated to be compliant with Federal Information Security Management Act of 2002 (FISMA) in their own communications and when operating on other networks. This includes adherence to National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) when and where they apply. This means federal agencies must utilize AES256 encryption in their operable and interoperable communications when LMR traffic is sensitive but unclassified. This includes communication with state and/or local agencies. Utilizing AES256 encryption would allow for various federal agencies to securely communicate with state and/or local agencies.

In subsequent meetings, the Encryption Subcommittee has recognized there are limitations with how subscriber radios can communicate under an encrypted environment. Technical difficulties exist regarding key management as well. These limitations stem from several sources, but work is on-going within TIA/TR-8.3 (standards-setting committee) to enhance pathways for encrypted interoperable communications and key management. Manufacturers have worked to mitigate technical challenges that affect the ability to securely communicate between single key and multi key subscriber units.

The Encryption Subcommittee met on November 28, 2017 met with representatives from TR-8.3 to discuss the current status of several standards, on-going development of those standards and items that are for future study. The TR-8.3 members represented Harris, Motorola, EF Johnson, Federal Bureau of Investigation (FBI), Department of Homeland Security Office of

John R. Benson  
HSEMD

Andy Buffington  
Communications Center

Linda Frederiksen  
EMS

Larry Smith  
Emergency Management

Kelly Groskurth  
Member At-Large

Ellen Hagen  
Fire Department (Volunteer)

Rob Rotter  
Sheriff's Office

Michael Kasper  
Sheriff's Office

Deb Krebill  
Fire Department

Tom Lampe  
Iowa DPS

Jason Leonard  
Municipal Police Department

Carole Lund-Smith  
ILEA

David Ness  
Municipal Police Department

Denise Pavlik  
Communications Center

Marty Smith  
Iowa DPH

Jeff Sundholm  
Iowa DOT

Jeffery Swearngin  
Iowa DNR

Patrick Updike  
Iowa DOC

Bob von Wolffradt  
Office of the CIO

Legislative Members  
Senator Jim Lykam  
Senator Randy Feenstra  
Representative Bob Kressig  
Representative Steven Holt

Emergency Communication (OEC) and Federal Partnership for Interoperable Communications (FPIC).

During the meetings, the following conclusions were reached:

- Interest in encrypted LMR capability is increasing and expanding;
- There are advantages and disadvantages inherent to single key and multi key subscriber units;
- EF Johnson, Harris and Motorola subscriber units' software has been updated to allow for a complete range of key IDs (KIDs) to be assigned to a traffic encryption key (TEK);
- Multi key subscriber units offer the most flexibility for a diverse array of users, allow for separate TEKs for operability but present management challenges;
- Single key subscriber units represent the most basic goal of encryption by eliminating scanner eavesdropping but may limit interoperability;
- An agency that desires to flash update subscriber units to multi key encryption (if possible) may have to allocate significantly more funds to for those updates when compared to purchasing a multi key radio at the time of initial procurement;
- An agency or geopolitical subdivision that purchases a single key radio may need to use the statewide key in order to interoperate with other agencies in addition to local operability;
- FPIC has a standing recommendation that agencies utilize the capability and flexibility offered by multi key AES256 equipped radios;
- Efforts should be made at a state level to keep the number of TEKs utilized on the ISICS Platform to a minimum to maintain consistency with the DDR;
- There may be agencies in Iowa that possess subscriber units that do not currently offer encryption or may have purchased single key radios;
- Coordination with other agencies and entities will need to occur to ensure interoperability exists;
- Encrypted interoperable talk groups need to be optional on the ISICS platform, and not every user will need access to them;
- The current set of encrypted interoperable talk groups may need to remain inactive until set policies and procedures for usage are defined;

Given this acquired information and set of conclusions, the Encryption Subcommittee submits a technical recommendation to ISICSB that users of the ISICS Platform who have a desire to utilize secure, encrypted interoperable talk groups available in the ISICS Regional Interoperable and Statewide Talk Groups Fleet Map purchase multi key subscriber units.

The Encryption Subcommittee recommends that the encrypted interoperable talk groups specified in the DDR be left in the programming code plug for user groups. However, encrypted interoperable talk groups should remain inactive until encryption is deployed and tested on the ISICS Platform. This includes dissemination of TEKs and dissemination and enactment of policies and

John R. Benson  
HSEMD

procedures that affect encrypted interoperable communication along with associated costs.

Andy Buffington  
Communications Center

The Encryption Subcommittee also recommends designations be made for suggested use of some interoperable talk groups.

Linda Frederiksen  
EMS

These recommendations apply to the specified encrypted interoperable talk groups on the ISICS fleet map. This does not apply to local geopolitical operable talk groups.

Larry Smith  
Emergency Management

Kelly Groskurth  
Member At-Large

These recommendations do not apply to a local agency or entity that may want to utilize vendor-specific encryption algorithms and schemes or DES variants for local operability.

Ellen Hagen  
Fire Department (Volunteer)

Rob Rotter  
Sheriff's Office

Michael Kasper  
Sheriff's Office

Deb Krebill  
Fire Department

Tom Lampe  
Iowa DPS

Jason Leonard  
Municipal Police Department

Carole Lund-Smith  
ILEA

David Ness  
Municipal Police Department

Denise Pavlik  
Communications Center

Marty Smith  
Iowa DPH

Jeff Sundholm  
Iowa DOT

Jeffery Sweargin  
Iowa DNR

Patrick Updike  
Iowa DOC

Bob von Wolffradt  
Office of the CIO

Legislative Members  
Senator Jim Lykam  
Senator Randy Feenstra  
Representative Bob Kressig  
Representative Steven Holt