ISICSB
Iowa Statewide Interoperable Communications System Board

Report to the Iowa Legislature on the Status of the Iowa Statewide Interoperable Communications System Board (ISICSB) Calendar Year 2018

IOWA STATEWIDE INTEROPERABLE COMMUNICATIONS SYSTEM
ISICS

FirstNet™

Table of Contents

I. Overview

During the first session of the 82nd General Assembly, the Iowa Legislature established the Iowa Statewide Interoperability Communications System Board (ISICSB)[1]. 2007 Iowa Acts, House File 353, created Iowa Code Section 80.28, which addresses the membership of the Board, with Section 80.29 identifying its duties, as follows:

> "A statewide interoperable communications system board is established, under the joint purview of the department and the state department of transportation. The board shall develop, implement, and oversee policy, operations, and fiscal components of communications interoperability efforts at the state and local level, and coordinate with similar efforts at the federal level, with the ultimate objective of developing and overseeing the operation of a statewide integrated public safety communications interoperability system. For the purposes of this section and section 80.29, *"interoperability"* means the ability of public safety and public services personnel to communicate and to share data on an immediate basis, on demand, when needed, and when authorized."

The ISICSB has been in existence for eleven years, progressively improving policy and procedures for Iowa interoperability and advancing stakeholder involvement in decision making.

2017 -2019 Chair and Vice-Chair are as follows:

Chair: Bureau Chief Thomas Lampe, Department of Public Safety
(515) 725-6113, lampe@dps.state.ia.us

Vice-Chair: Captain Jason Leonard, Waverly Police Department
(319) 352-5400, jasonl@ci.waverly.ia.us

[1] ISICSB web site: https://isicsb.iowa.gov/

II. Key Figures for 2018

52 Standards and policies adopted to enhance interoperability

2 Technical Recommendations to assist public safety and public service personnel with equipment decisions and radio programming

240+ Registered for ISICSB training opportunities

17 Classes offered by ISICSB in coordination with other agencies to enhance interoperability.

51 Applications accepted for ISICS use in 2018

60+ Total Agencies/Groups[2] using ISICS

16 Major events using ISICS for interoperability in 2018[3]

113 PSAPs that will have access by the end of 2019

1 Whitepaper on Encryption that was presented at a national meeting

[2] Many of these groups include multiple agencies.

[3] Iowa State Football, University of Iowa Football and Iowa State Fair

III. Key Definitions and Acronyms

Definitions

Interoperability: two or more agencies—independent of discipline—that must work with and communicate with each other during a collaborative response. An example would a local police department working with a local fire department during an emergency.

Operability: single agency handling day-to-day communications and associated activities such as emergency response without assistance from another agency or entity.

Acronyms

CIO	State of Iowa Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COML	Communications Leader
COMT	Communications Technician
DHS	Department of Homeland Security
DPS	Department of Public Safety
DNR	Department of Natural Resources
DOC	Department of Corrections
DOT	Department of Transportation
DSWIC	Deputy Statewide Interoperability Coordinator
ECD	Emergency Communications Division
FCC	Federal Communications Commission
FFY	Federal Fiscal Year
FPIC	Federal Partnership for Interoperable Communications
ICN	Iowa Communications Network
INTD	Incident Tactical Dispatch
ISICS	Iowa Statewide Interoperable Communications System
ISICSB	Iowa Statewide Interoperable Communications System Board
ISP	Iowa State Patrol
ISSI	Inter-Sub System Interface
LMR	Land Mobile Radio
NCSWIC	National Council of Statewide Interoperability Coordinators
NECP	National Emergency Communications Plan
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NPSBN	National Public Safety Broadband Network
OEC	Office of Emergency Communications
P25	Project 25

PSAP	Public Safety Answering Point
RFP	Request for Proposal
RIC	Regional Interoperability Committee
SCIP	Statewide Communications Interoperability Plan
SFY	State Fiscal Year
SLIGP	State and Local Implementation Grant Program
SME	Subject Matter Expert
SPOC	State Point of Contact
SWG	Standards Working Group
SWIC	Statewide Interoperability Coordinator
TA	Technical Assistance
TIA	Telecommunications Industry Association
TR-8	Project 25 Steering Group
UGC	User Group Committee
VHF	Very High Frequency
WISE	Wi-Fi Internet for School Emergencies

IV. Membership

December 2018 ISICSB Members

Local Representatives

Name	Position	City/Locale
David Ness	Municipal Police Department	Des Moines P.D.
Jason Leonard	Municipal Police Department	Waverly P.D.
Ellen Hagen	Fire Department (Volunteer)	Jewell F.D.
Michele Bischof	Fire Department (Career)	Des Moines F.D.
Vacant	Communication Center Manager	
Andy Buffington	Communication Center Manager	Winnebago Co.
Robert Rotter	County Sheriff	Iowa County
Michael Kasper	County Sheriff	Linn County
Angela Clouser	Member-at-Large	Panorama Community Schools
Larry Smith	Emergency Management	Keokuk County
Vacant	Emergency Medical Services	

State Agency Representatives

John Benson	Department of Homeland Security and Emergency Management
Marty Smith	Department of Public Health
Thomas Lampe	Department of Public Safety
Carole Lund-Smith	Iowa Law Enforcement Academy
Jeffrey Swearngin	Department of Natural Resources
Patrick Updike	Department of Corrections
Robert von Wolffradt	Chief Information Officer
Sandra Black	Department of Transportation

Legislative Ex-Officio Members

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

V. Communications Interoperability Efforts

The ISICSB holds monthly public meetings, on the second Thursday of the month. The meetings are streamed live for public viewing in addition to a conference line being available for remote attendance. The ISICSB posts information such as meeting agendas, minutes, polices, standards and a calendar of events on a web site at www.isicsb.iowa.gov.

Since its inception, ISICSB has addressed legislative mandates, as contained in Iowa Code 80.29. The following sections outline the accomplishments of the ISICSB in operating under Iowa Code 80.29.

1. **Implement and maintain organizational and operational elements of the board, including staffing and program activity.**

   A. ISICSB Members, Staff, Funding and Activities

   From its inception in 2007 through 2018, ISICSB has relied on Federal Interoperability Grants and State appropriations to support Board activities. In State Fiscal Year (SFY) 2018 and 2019, $115,661 in state funding was appropriated to ISICSB.

   Each Board and committee member has a full-time professional position and performs Board duties on volunteer and part-time basis. Mileage is a reimbursable expense.

   As part of a national interoperability initiative, from 2008 each state was to establish a Statewide Interoperability Coordinator (SWIC) position. This position is also consistent with this Iowa Code mandated element. This SWIC position has been critical to improving interoperability in Iowa, addressing these legislative mandates, and the resulting accomplishments of the Board. Chris Maiers serves as the Iowa SWIC.

   Until 2014, SWIC salary was paid for by Federal Interoperability grants. Starting in Federal Fiscal Year (FFY) 2015 and continuing through FFY 2017, State and Local Implementation Grant Program (SLIGP) pays half the SWIC's salary and expenses. This grant program creates a national public safety broadband network (NPSBN). In 2018 SLIGP 2.0 was implemented and covers approximately half of the SWIC's salary. It is essential that legislative funding continue to be appropriated to pay half of the SWIC's salary to continue to meet Iowa's various non-broadband radio interoperability needs.

   In 2014 the Board hired an administrative assistant. This position is funded by State and Local Implementation Grant Program (SLIGP) grant funds. The position is limited to duties to support FirstNet Broadband.

   During 2016 through a partnership with Iowa Communication Network (ICN), Helen Troyanovich, an electrical engineer, became Deputy SWIC. DSWIC Troyanovich was fully funded through SLIGP grant and focuses on broadband outreach, engineering,

interoperability, and regional interoperability committee (RIC) participation within ISICSB. Deputy SWIC Troyanovich returned to her ICN position in July 2017.

In 2012, Congress passed the Middle Class Relief Act which included NPSBN creating FirstNet Authority. A state and local broadband planning grant program known as SLIGP was included.

In 2013, SLIGP grant became available. Iowa applied for this grant in that year and in August was awarded funds for a three year period with the restriction that this grant can only be used for broadband planning activities, and not the SWIC's overall interoperability duties. NPSBN funds are used specifically to educate Iowa's public safety community about this new national broadband network, and solicit feedback from our public safety community about their broadband communications needs.

While these efforts parallel many efforts related to improving interoperability, they are limited to broadband. NPSBNs like FirstNet are intended to supplement interoperable capabilities offered by public safety LMR networks like ISICS by providing information that may not be simple to communicate via voice communications.

In 2017, SLIGP 2.0 was announced as a means to continue to fund public safety broadband initiatives across the nation. Iowa applied for and was awarded this grant. The funds continue to support ISICSB efforts to expand broadband interoperability in Iowa in addition to funding the SWIC's activities.

SLIGP 2.0 has allowed the ISICSB and SWIC to devote time to engage with stakeholders and provide input to the State Point of Contact (SPOC), Thomas Lampe, and to identify potential public safety, public service and other extended users of NPSBN and prepare for data sharing. The SPOC served as the primary information source for FirstNet related matters during the decision making process of opting-in or opting-out of the FirstNet buildout. Work continues on the development of policies and agreements to increase data sharing among agencies.

As a part of those efforts, planning is on-going to help agencies transition to incorporating more data into operations for daily activities and special events. This has been accomplished with individual stakeholder meetings and outreach events.

The ISICSB expanded their FirstNet Broadband Sub-Committee to address planning, technology and public private partnership issues of NPSBN in Iowa. This FirstNet Broadband Sub Committee was co-chaired by Ric Lumbard, Executive Director of the ICN, and State of Iowa Chief Information Officer (CIO) Bob von Wolffradt. SWICs Allen and Maiers, DSWIC Troyanovich, along with two ISICSB Board members, and other state and local subject matter experts rounded out this committee. The Sub Committee met monthly to become more informed about broadband technology, Iowa public safety needs, NPSBN public safety grade requirements, and identify potential private companies willing to engage in a public safety wireless broadband network.

NSPBN directed each state to identify a state point of contact (SPOC) for NPSBN interactions. Then Governor Branstad appointed ISICSB Chair Thomas Lampe as the SPOC for NPSBN planning and implementation in Iowa. During 2017 SPOC Lampe and other ISICSB members attended national and regional meetings advancing FirstNet's understanding of Iowa public safety needs for a NPSBN.

On November 18, 2014, Iowa became the 8th state to hold an Initial Consultation with seven senior representatives of FirstNet. Over 50 Iowa state and local representatives met with FirstNet to begin the multiphase process of determining if Iowa wishes to opt-in, building NPSBN in conjunction with FirstNet, or opt-out, requiring Iowa to shoulder the total expense to build out their portion of a NPSBN.

FirstNet met with Governor Branstad on December 3, 2015, to explain legal interpretations of enabling legislation regarding states options in selecting whether to opt in or opt out of partnering with FirstNet to build out Iowa's portion of the National Public Safety Broadband Network. SPOC Lampe and SWIC Allen also attended.

On July 18, 2017, Governor Reynolds made the decision for Iowa to become the fifth state to opt-in with FirstNet. Following the "Opt-In" decision, Governor Reynolds reappointed Thomas Lampe as SPOC for Iowa On November 17, 2017.

B. Committees

The primary committees under the ISICSB all have goals, metrics, objectives and action plans that are outlined in the *2017 Statewide Communications Interoperability Plan (SCIP)*. Since the adoption of this plan each committee has made progress towards achieving the goals laid out in the SCIP. SWIC Maiers is planning to request assistance from the Emergency Communications Division (ECD) of the Cybersecurity and Infrastructure Security Agency (CISA) to help refresh the SCIP in 2019.

The Governance Committee, in conjunction with other Board committees, continues to steer activities with local public safety community partners in a collaborative way to establish regional governance presence throughout Iowa.

The Governance Committee anticipates it will continue leveraging local public safety community partners for knowledge and advice in 2019 and beyond as the Board continues the task of completing the deployment of a new statewide interoperable Project 25 (P25), Phase 2, 700 MHz land mobile radio (LMR) platform in Iowa. This platform is known as the Iowa Statewide Interoperable Communications System (ISICS).

The Governance Committee continues to work with local public safety community partners to establish effective and appropriate governance practices and relationships creating a foundation for successful operation of both ISICS and Iowa's portion of a NPSBN.

The Finance Committee continues to meet routinely to evaluate the financials of the ISICSB and approve expenditures. Any grant funding that is leveraged by the ISICSB to support programs is thoroughly vetted in compliance with all requirements.

If more funding becomes available for the ISICSB to support local programs with interoperable solutions via ISICS, processes will be developed accordingly.

The Operations Committee has worked throughout 2018 to find effective ways to leverage ISICS for interoperable communications via coordination with the Standards Working Group and other committees as necessary.

The Operations Committee has also worked to ensure that all PSAPs in Iowa will have access to ISICS for interoperability by the end of calendar year 2019. This is ahead of the goal outlined in the SCIP of 95% of all PSAPs having access by the end of calendar year 2020.

The Outreach Committee has worked to send out a regular newsletter to interoperability stakeholders in Iowa. Regional outreach events were also scheduled for ISICS and FirstNet. At these outreach events, presentations were given on ISICS and FirstNet. Attendees had an opportunity to witness demonstrations of the networks and ask questions to program managers.

The Technology Committee has continued its work in evaluating technological opportunities for the ISICSB to enhance interoperability via ISICS and NPSBN. Work in 2018 included developing a program guide for agencies joining ISICS (*ISICSB TR-2018-001 – Programming Guide Technical Recommendation*), collaborating with the Encryption Subcommittee to publish a technical recommendation pertaining to multi-key subscriber radios (*ISICSB TR-2018-002 – Multi-Key Equipped Subscriber Units*) and a white paper (*Encryption Needs in Iowa*) that was presented at a recent national meeting of the P25 User Needs Subcommittee, and collaborating with the Standards Working Group (SWG) on standards that require more technical expertise.

Technology Committee work in 2019 is expected to include further development of technological solutions for interoperability stakeholders in Iowa and licensing of three 800 MHz Scene of Action channels.

The Training and Exercise Committee developed and deployed several training sessions for interoperability training in 2018 that are outlined later in this report. These activities also align with SCIP goals. Work in 2019 will include publishing guidance and training modules for the various ISICS standards and continuing work to expand the cadre of credentialed Communications Unit personnel.

The User Group Committee (UGC) continues to develop and enhance processes to get agencies connected to ISICS. New forms were developed in 2018 that greatly streamlined the process as well. Feedback from the UGC was also built into the ISICSB web site that applicants can use to join the system. Work in 2019 is expected to include further

development on the ISICS application process and to strengthen the Regional Interoperability Committees (RICs).

The FirstNet Broadband Subcommittee will reconvene in January 2019 to begin the process of exploring and developing policies and standards on NPSBN.

2. Review and monitor communications interoperability performance and service levels on behalf of Agencies.

The ISICSB and 911 Communications Council have coordinated their activities and scheduled meetings on the same dates and at the same locations for several years. This has helped promote information sharing between the ISICSB and the Council in public forums.

During 2018 SWIC Maiers and 911 Program Manager Blake DeRouchey continued to meet weekly to ensure alignment of objectives and coordination of efforts between ISICSB and the Council. Those meetings will continue to be held routinely in 2019 and beyond.

Since 2014, ISICSB has released a series of Policy Statements consistent with the National Emergency Communications Plan (NECP) and made efforts to provide clarity to the naming or re-naming of all public safety interoperability radio channels within all radio bands. SWIC Maiers and 911 Program Manager Blake DeRouchey were active participants in the 2019 revision to the NECP.

ISICSB management has monitored public safety interoperability responses in Iowa. There were incidents in Iowa where the response involved a number of agencies responding and interoperability issues identified. ISICS management contacted those involved in the response, examined interoperability issues, and offered solutions that could solve interoperability communication issues that evolved from the incident. Some of the findings were:

- Lack of training field personnel on how interoperability channels work.
- Improperly labeled radio channels.
- Other available options to achieve interoperability with the equipment they use on a day-to-day basis.
- Local or county policies in some instances were prohibiting responders from using interoperability channels because of their lack of updating the policy to reflect newer technology and the availability of more channels.
- In some cases, communication centers were only broadcasting on certain channels that other agencies could not monitor.
- In other cases, there was significant interference created by other states in interoperability channels.

ISICSB Technology Committee continues to work collaboratively with several local communities to identify solutions and implement resolution to the communication problems.

Those challenges continue to prevent Iowa from having coordinated communications much of the time in the incidents examined.

Iowa's statewide communication platform called the Iowa Statewide Interoperable Communications System (ISICS) was awarded for construction in 2015 and scheduled to be fully operational in 2019, will go a long way in solving Iowa's public safety interoperability challenges. It is one of the fastest deployments of any statewide LMR system.

Absent a completed statewide interoperable system like ISICS, it is very difficult to solve communication issues that counties and cities have in Iowa. The ISICSB will continue to explore viable options and additional initiatives to improve interoperability in the coming year.

During 2018, ISICSB conducted a series of regional training workshops designed to improve interoperability, including a focus on delivery of the U.S. Department of Homeland Security's (DHS) Communications Leader (COML) and Communications Technician (COMT) courses.

- ISICS Regional Training (12 classes) in six cities across Iowa.
- ICS 300 in Cedar Rapids and Mason City
- Incident Tactical Dispatch (INTD) in Monticello
- Audio Gateway Training in Council Bluffs and Des Moines

The ISICSB also sent Cedar Rapids Fire District Chief Curtis Walser, a credentialed COML and COMT, to a COML Bootcamp in Tennesssee. COML Boot Camps are used to test and re-credential COMLs. Iowa currently does not have a re-credentialing process. By sending Chief Walser, the ISICSB was able to gain an insight on what may be best practices used by other states to keep their COMLs and COMTs up-to-date on training and credentialing. Further work on this is expected in 2019.

The ISICSB continues to use technology to advance information sharing with the public through use of conference lines, which are open for all board meetings with the intent of gaining more one-on-one local input from a broader range of local users on interoperability issues. Virtual meeting rooms were utilized in 2018 to allow for public viewing of documents that are up for review and for notetaking.

ISICSB continued its role as a voting member of the Telecommunications Industry Association (TIA) and Project 25 (P25) Steering Group known as TR-8 industry-wide standards setting group. SWIC Maiers has voted on several P25 standards that facilitate and expand interoperability on radio networks such as ISICS. ISICSB Chair Thomas Lampe and SWIC Maiers are also a members of the P25 Steering Committee.

3. Establish, monitor, and maintain appropriate policies and protocols to ensure that interoperable communications systems function properly.

The ISICSB is promoting the national policy of using plain language in radio communications throughout Iowa. A standard for plain language use on ISICS was adopted in 2018.

The ISICSB approved a policy in 2014 adopting the use of a minimum number of national interoperable channels in each radio as a statewide standard on January 1, 2014, and adopted the use of the national standard channel nomenclature. During 2016 this policy was revised to reflect contemporary changes occurring with new technologies and operational plans across Iowa. In 2018 an all-encompassing minimum program requirements standard was adopted for all ISICS users that includes the statewide and regional interoperability talkgroups and national interoperability channels. This helps ensure that regardless of where public safety personnel travel, they will have a means and method for interoperable communications.

The ISICSB developed and published 'quick' one page templates and instructions for ease of use and programming channels into radio equipment. This is posted publicly on the ISICSB web site as an official ICS-217A form[4].

Because ISICSB lacks enforcement authority of any policy, this limits achievement of interoperability as some county and local governments continue past practices using legacy channel naming conventions like "Mutual Aid" which is inconsistent with new federal guidance. This non-compliance with ISICSB Policy and other federal directives, contributes to creating user confusion within Iowa regarding communications assets and hindering radio interoperability best practices. SWIC Maiers continues to meet with local agency stakeholders to stress the importance of standardization of channel nomenclature.

With Iowa's local control focus and county patchwork of "silo" radio systems operating in different radio frequencies, statewide interoperability policies and protocols are challenging to establish. With disparate systems, what works for one county may not work for another. However a statewide platform like ISICS reduces this confusion since all users can be on a platform with a statewide system.

As local agencies connect to ISICS for interoperability, it is expected that some of the hurdles relating to interoperable communications will be mitigated. Other challenges relating to training and equipment procurement may persist for years.

ISICSB passed a number of policy statements beginning in July 2014. After working closely with Attorney General Staff on a process for developing, prominently posting for on ISICSB website to incentivize public comment, Board discussion and, if appropriate, voting by the Board to determine if a policy statement represented a best practice for Iowa public safety stakeholders. Lastly all policy statements are posted on ISICSB web site in order of chronological order. All policy statements, standards, technical recommendations and documents are listed below for reference.

- ***Policy statements passed in 2014:***

[4] ISICSB ICS-217A: https://isicsb.iowa.gov/sites/default/files/copy_of_2012-05_aka_isicsmc12-b_revised1_ics_217a_v2017_01_1.pdf

- **2014-1** *Support of Project 25 Standard.*
- **2014-2** *Endorsement of Strategic Technology Reserve (STR) Trailers*.
- **2014-3** *Support of No Encryption on Interoperability Channels*.
- **2014-4** *Endorsement of Credentialing Process of COML/COMT*.

- ***Policy statements passed in 2015:***
  - **2015-01** *Endorsement for support for procurement and state funding of P-25 700 MHz LMR platform* (which also created a standing committee User Group Committee (UGC) charged with managing collaboration on platform usage).
  - **2015-02** *Supporting government control of interoperability frequencies and channels.*
  - **2015-03** *Defining Public Safety Grade*.
  - **2015-04** *Iowa Statewide Interoperability Channels.*
  - **2015-05** *AES 256 Encryption SLN TEK KID*
- ***Policy statements passed in 2016:***
  - **2016-01** *Supporting Funding of Local Procurement of Public Safety Grade Land Mobile Radio (LMR) Equipment Used on Statewide Interoperable Networks, and Platforms*
- ***Policy statements passed in 2017:***
  - **2012-05** *Policy (aka ISICSMC12-B) Revised - Minimum Interoperable Radio Channels & Nomenclature*
  - **2017-07** *Policy Statement supporting the National Emergency Number Association (NENA) i3 Standard for Next Generation 9-1-1 (NG9-1-1)*
- **ISICS Platform Requires a complex set of standards, processes and procedures to this end ISICSB established a subcommittee to focus exclusively on policy and procedures for ISICS users as guidance for all users. The following standards were adopted by ISICSB in 2017:**
  - **1.1.0** - *Subscriber Security*
  - **2.1.0** - *Variance and Waivers*
  - **2.2.0** - *Maintenance of Alias List*
  - **2.3.0** - *System Login Naming Maintenance*
- ***Documents published in 2017:***
  - **ICS Form 217A** - *Communications Resource Availability Worksheet*
  - **Staff Study** - *ISSI Committee Recommendation for Iowa Statewide Interoperable Communication System (ISICS) use of ISSI connection*
- **ISICSB's established a subcommittee focusing exclusively on policy and procedures for ISICS users as guidance for all users successfully drafted the following standards that were adopted by ISICSB in 2018:**
  - **1.2.0 -** *Talkgroup and Multigroup Ownership*
  - **1.3.0 -** *Statewide Interoperable Plain Language Policy*
  - **1.4.0 -** *Statewide Pursuit Communications*
  - **1.5.0 -** *ISICS Regional & Statewide Interoperability Talkgroups*
  - **1.5.1 -** *Transport Interoperability*

- **1.5.2 -** *Use of Statewide and-or Reg Interop Talkgroups-Air*
- **1.6.0 -** *Talkgroup and Multigroup Ownership*
- **1.7.0 -** *Minimum Programing Requirements*
- **1.8.0 -** *Event and Exercise Communications Planning*
- **1.10.0 -** *Cross Spectrum Interoperabity*
- **1.11.0 -** *Use of 700-800 MHz Scene of Action (SOA) Channel*
- **2.4.0 -** *Operational Management*
- **2.5.0 -** *Network Management*
- **2.6.0 -** *Database Management*
- **2.7.0 -** *Training Radio Telecommunicators*
- **2.8.0 -** *Requesting Access and Participation Plan Revisions*
- **2.9.0 -** *Requesting Participation by Non-Public Safety/Non-Public Service Organizations*
- **2.10.0 -** *Training Technical Staff*
- **2.11.0 -** *Training ISICS End Users*
- **2.12.1 -** *System Security Groups*
- **2.12.2 -** *Security System Keys*
- **2.12.3 -** *Encryption Key Security*
- **2.13.0 -** *Subscriber Radio Standards*
- **2.13.1 -** *Subscriber Surplus Radio Disposal*
- **3.1.0 -** *Radio Aliases*
- **3.2.0 -** *Talkgroup and Multigroup Names*
- **3.3.0 -** *Radio ID Talkgroup Allocation*
- **3.4.0 -** *Fleetmap Standards*
- **3.5.0 -** *Statewide Wide Area Talkgroup Access and Management*
- **3.6.0 -** *Radio Site Access Permission - Subsystem Roaming*
- **3.7.0 -** *Scanning*
- **3.8.0 -** *Emergency Button*
- **3.9.0 -** *Multigroup Announcement*
- **3.10.0 -** *Talkgroup and radio user priority*
- **3.11.0 -** *Talkgroup Site Access and Roaming*
- **3.12.0 -** *CAD and ATIA Connectivity*
- **4.1.0 -** *Outage Responsibility*
- **4.2.0 -** *Agency Maintenance*
- **4.3.0 -** *Preventative Maintenance*
- **4.4.0 -** *Record Keeping Requirements*
- **4.5.0 -** *Contact Information Procedures*
- **4.6.0 -** *System Maintenance Programming and Qualifications*
- **5.1.0 -** *Hospital Access*
- **7.1.0 -** *Standards Compliance Process*

- **Documents published and/or adopted in 2018:**
  - **ISICSB TR-2018-001** – *Programming Guide Technical Recommendation*
  - **ISICSB TR-2018-002** – *Multi-Key Equipped Subscriber Units*

- **Whitepaper** – *Encryption Needs in Iowa*

ISICSB will continue to promote interoperability policies and other documents to assist agencies comply with state and federal standards.

Additional policy statements, standards and technical recommendation documents are in various degrees of completion in committee work and positing for interested stakeholders.

4. Allocate and oversee state appropriations or other funding received for interoperable Communications.

In August, 2013, the ISICSB, on behalf of the State of Iowa, received a $1.67 Million federal grant to plan future build-out of the Nationwide Public Safety Broadband Network (NPSBN) in Iowa called SLIGP. NPSBN is being undertaken by a federal agency, FirstNet. NPSBN will be a national public safety grade, wireless broadband data network. This grant was restricted to specifically this initiative and includes planning, outreach, education of public safety and elected officials, inventory of existing assets that could be leveraged for this broadband data network, and funding for any personnel costs directly related to this initiative, e.g., a percentage of the SWIC's salary directly attributable to his work on broadband. This grant expired on March 1, 2018.

In state fiscal years 2014 through 2017, ISICSB received $154,661 annually in state appropriations to conduct State of Iowa interoperability matters not covered by federal grants.

For state fiscal year 2018 and 2019, ISICSB's appropriation was reduced to $115,661 to conduct State of Iowa interoperability matters not covered by federal grants. The ISICSB plans to request increased appropriations for future fiscal years in order to help sustain and expand interoperable efforts in Iowa.

SWIC Maiers continues to work in collaboration with ISICSB members and interoperability stakeholders to identify potential long term funding mechanisms to enhance interoperability in Iowa.

In 2018 SLIGP 2.0 was rolled out, awarded to Iowa and will run through 2020. Iowa was awarded funding to help sustain the SWIC and administrative assistant positions. This grant continues to fund approximately 50% of the SWIC position, and administrative assistant and FirstNet Outreach Specialist. SLIGP 2.0 activities[5] include:

- *Single officer (or governmental body) and staff to, at a minimum, provide for ongoing coordination with NTIA and implementation of grant funds.*
- *Existing governance body to provide input to the single officer and to contribute towards planning activities to further identify potential public safety users of the NPSBN and prepare for data sharing.*
- *Data collection in specific areas identified to be helpful as requested by FirstNet.*

[5] SLIGP 2.0 Frequently Asked Questions

- *Development of policies and agreements to increase sharing of data between existing public safety systems across various agencies within the State or territory using the NPSBN.*
- *Individuals, such as the single officer and governing body members, to perform planning activities to help FirstNet and its partner further identify potential public safety users of the NPSBN.*
- *Planning efforts to help FirstNet gain inclusion on applicable statewide contract vehicles.*
- *Planning activities to prepare for emergency communications technology transitions.*
- *Activities to identify and plan for the transition of public safety applications, software, and databases.*
- *Identifying and documenting on-going coverage needs/gaps within the State.*
- *Activities to convene stakeholder outreach events to continue planning for NPSBN implementation, as requested by FirstNet.*

5. **Identify sources for ongoing, sustainable, longer-term funding for communications interoperability projects, including available and future assets that will leverage resources and provide incentives for communications interoperability participation, and develop and obtain adequate funding in accordance with a communications interoperability sustainability plan.**

   Many of these activities are also covered in Part 4 above. They include the previously listed grants.

   With the passage of the Federal Nationwide Public Safety Broadband Network (NPSBN) legislation, Iowa will continue participating in planning for Iowa's portion of build-out of FirstNet, a nationwide broadband data network to supplement public safety's land mobile-radio communications networks with interoperable wireless data capabilities.

   ISICSB continues to seek ways to identify sustainable, long-term funding and cost containment measures for communications interoperability. Continued state funding for ISICSB allows this board to continue to seek federal grant opportunities. Without this funding, ISICSB will be denied many grant opportunities due to inability to meet grant requirements specifying a local match.

   Local, county and state funding is essential for sustainability of any interoperable communications system. State funds will continue to be used to train, educate, and where possible build and maintain infrastructure.

   ISICSB will continue to seek grants and outside funding; however, federal grants specifically for interoperable communications are diminishing making state support all the more crucial in receiving such funding.

ISICSB has completed the final year of SLIGP Grants for the rollout of FirstNet, a nationwide broadband data network. ISICSB was awarded SLIGP 2.0 grants as Iowa was the fifth state to "Opt-In" to FirstNet. The SLIGP 2.0 grant will run from 2018 through 2020. (See more on SLIGP in section 6 below.)

ISICSB will develop ideas for potential funding streams that could be ready for legislative consideration in the 2019 or 2020 session. If enacted, the funding streams would allow the ISICSB to maintain and expand ISICS infrastructure, and administer grants to local municipal and county public safety agencies to promote and expand interoperability. These grant monies could include allocations for training and educational opportunities, procurement of subscriber units and/or expansion of local LMR infrastructure.

Any new funding mechanisms and resulting programs would be structured to be consistent with all state and federal laws regarding grant awards, accounting and distribution of funds.

6. **Develop and evaluate potential legislative solutions to address the funding and resource challenges of implementing statewide communications interoperability initiatives.**

Potential legislative items noted in Section 5 regarding the restoration of the appropriations and development of future funding streams would address costs associated with funding interoperability in Iowa by supporting ISICSB. New funding could be used to fund grants that local agencies could use to expand interoperable capabilities. These grants could be used by volunteer fire departments and emergency medical services, municipal police departments, schools and other interoperability stakeholders.

Work continues on developing a five and ten year financial plan for the ISICSB. Implementation of those plans would require legislation to be put in to effect.

7. **Develop a statewide integrated public safety communications interoperability system that allows for shared communications systems and costs, takes into account infrastructure needs and requirements, improves reliability, and addresses liability concerns of the shared network.**

In 2012, the Department of Public Safety (DPS), Department of Transportation (DOT), and Department of Corrections (DOC), began working together with ISICSB to develop a plan and issue a Request for Proposal (RFP) for using state infrastructure and leveraging any other state resource that could be used to develop a communications interoperability radio system**.**

In 2013, ISICSB management monitored and assisted with an RFP for a statewide Project 25 700 MHz Phase 2 land-mobile radio (LMR) statewide platform tying together the seven existing countywide LMR systems. The winning vendor chose two of those county based systems as the basis for initial coverage. Those two systems selected were WESTCOM in the West Des Moines Metro which spans Polk, Warren and Dallas counties, and STARCOM, a multi-state communications system based in Woodbury County.

During 2016 a contract was signed and construction began of the Iowa Statewide Interoperable Communications System (ISICS) platform. ISICS is scheduled to be completed in early 2019. ISICSB members believe by working with state and local agencies to create a "shared interoperable" Project 25 (P25), 700 MHz, Phase 2 LMR statewide platform, both interoperability and a very significant cost savings for state and local governments can occur.

ISICSB has worked to expand and engage county and local membership on all seven committees, Finance, Governance, Operations, Outreach, Technology, Training and Exercise, and User Group, to make sure the Board's on-going process to gather input from local users on a continuous basis is maintained and to ensure that the actual state-wide system operational protocols remain up to date. To date, ISICSB has over 100 county and local committee member representatives. Various sub committees have aided in investigation and expansion of interoperability in Iowa for LMR and broadband and will address future needs of the ISICSB and stakeholders across Iowa.

A list of agencies that have completed the process to use ISICS as of December 2018. Some counties have opted to build out infrastructure on the ISICS system but have not yet gone through the official approval process. As such, those counties are not listed here but are shown in Figure 1 if site locations have been identified.

- 10th District Federal Reserve Law Enforcement
- 185th Iowa Air National Guard
- Adair Guthrie EMA
- Air Methods
- Boone County
- Buchanan County
- Buena Vista County
- Buena Vista EMA
- Carlisle Fire Department
- Carroll County
- Chickasaw County 911
- Chickasaw County EMA
- Crawford County
- Dallas County
- Delaware Township Fire Department
- Des Moines Police Department
- U.S Department of Homeland Security Emergency Communications Division
- Dickinson County Emergency Management
- Drug Enforcement Administration
- Grundy County
- Hamilton County
- Harrison County
- Humboldt County

- Ida County
- Iowa Department of Natural Resources
- Iowa Department of Public Health
- Iowa Department of Public Safety
- Iowa Department of Transportation
- Iowa Department of Homeland Security and Emergency Mgmt.
- Jackson County EMA
- Jasper County
- Jewell Fire Rescue
- Johnson County JECC
- Kossuth County
- Linn County Sheriff's Office
- Madison County
- Mahaska County
- Marion County Sheriff
- Mercy Ambulance Des Moines
- Metropolitan Incident Command Radio Network (MICRN)
- Mills County
- Monona County
- Montgomery County EMA
- Muscatine County
- Northern Warren Fire
- Page County
- Shelby County
- Tipton Ambulance Service
- Urbandale Schools
- Union County LEC
- U.S. Marshal's Service
- Unity Point Des Moines
- University of Iowa Public Safety
- University of Northern Iowa
- U.S. Army Corps of Engineers Red Rock
- Van Buren County 911
- Virginia Township Fire Rescue
- Warren County
- Worth County
- Wright County

A map of the current ISICS buildout as of December 2018 (Figure 1).

8. Investigate data and video interoperability systems.

In 2010, Iowa was one of twenty-one jurisdictions (one of seven states) to be granted an FCC license to build a public safety high speed wireless network for data and video

interoperability, the precursor to the NPSBN. The ISICSB applied for, but did not receive a federal grant to initiate construction of this network. The grant was denied because the ISICSB lacked the 20% matching fund requirement and had no sustainable state appropriations.

With the passage of the Nationwide Public Safety Broadband Network (NPSBN) legislation by Congress in February of 2013, the ISICSB created a FirstNet Broadband Subcommittee to address Iowa's portion of planning and technology issues of this coming national network. This subcommittee was Co-Chaired by then ICN Executive Director and State of Iowa CIO. Members included SWIC Allen, SWIC Maiers, state and local subject matter experts, Department of Management, 911 Communications Council Chair, Connect Iowa, and representatives of police, fire and emergency management.

The FirstNet Broadband Subcommittee is scheduled to reconvene in January 2019 to begin discussions of how to leverage public safety broadband data networks that are now or will be available to address current operability and interoperability issues. This activity will help assist agencies in planning necessary for successfully adopting new technology.

In November 2015 ISICSB Chair Thomas Lampe, along with ICN staff met with Marshalltown School officials to launch the Wi-Fi Internet for School Emergencies pilot project at Marshalltown High School. Using existing high speed ICN fiber connections at the Marshalltown school and other schools across Iowa will provide public safety responders with a dedicated, secure, private, broadband wireless connection through Wi-Fi for devices available during day to day operations and emergencies at the school. This pilot project is intended to serve as a model for Iowa demonstrating protection of our schools with existing technology. This also simulates a FirstNet broadband connection in that only public safety has access to it. This pilot project with Marshalltown schools expanded to two additional schools, Norwalk and Martensdale. Overall feedback from the program was positive. The pilot program was marked as complete in 2018.

9. Expand, maintain, and fund consistent, periodic training programs for current communications systems and for the statewide integrated public safety communications interoperability system as it is implemented.

The ISICSB has established and maintained a periodic training program for Iowa's public safety officials through a series of regional workshops annually funded by the Department of Homeland Security (DHS) Emergency Communications Division (ECD). These Technical Assistance grants can be presented throughout the state. The ISICSB has acquired several national DHS/ECD interoperability tools for these efforts, such as:

- In previous years, ISICSB hosted a Communication Training Session in Des Moines and participated in one National Guard sponsored events where several COML and COMT participants were able to complete their task books to apply for credentialing through ISICSB.
- SWIC Maiers assisted with the planning for the next National Guard communications training events scheduled for 2018.

- ISICSB Training Committee in collaboration with DHS/ECD are actively planning more communication training opportunities scheduled for calendar year 2019. This follows Audio Gateway, ISICS Regional Training, ICS 300 and Incident Tactical Dispatch classes in calendar year 2018. Objectives for 2019 include an expansion of the COML and COMT classes and cybersecurity. These offerings in 2019 are expected to compliment further ISICS interoperability training.
- In May 2013, a multi-state workshop was held in Des Moines to put together a standard recognition and credentialing process for the COML and COMT positions in Iowa, Missouri, and Kansas. This process ensures trainees take the relevant courses and then demonstrate their skills so that they are not only better prepared to use these skills in Iowa, but regionally and nationally, if requested. So far, several individuals have successfully completed this COML or COMT process and received credentials from the ISICSB.

The above efforts are those training initiatives which can help Iowa public safety improve interoperability in pre-planned or emergency situations where public safety uses many disparate radio systems to communicate. ISICSB has credentialed over 17 COMLs and COMTs since 2013.

10. Expand, maintain, and fund stakeholder education, public education, and public official education programs to demonstrate the value of short-term communications Interoperability solutions, and to emphasize the importance of developing and funding long-term solutions, including implementation of the statewide integrated public safety communications interoperability system.

Many of these activities are also covered in Part 9 above.

Besides the ISICSB's efforts regarding improving interoperability with traditional land-mobile radio (LMR) systems, the ISICSB has initiated stakeholder education regarding the new Nationwide Public Safety Broadband Network (NPSBN) system called FirstNet being built in every state as part of a single nationwide high-speed wireless broadband network designed to supplement and complement public safety's LMR systems. A federal grant was obtained in 2013, which will fund stakeholder education and planning for this coming network through 2018. Another grant application for NPSBN has been submitted and accepted that provides additional funding sources through 2020.

The educational opportunities did not just include local subject matter experts (SME). This included the Inter Sub System Interface (ISSI) Summit that was held in March of 2017 in which SMEs from TIA/TR-8, the Federal Partnership for Interoperable Communications (FPIC)[6] and vendors attended. This summit provided extremely valuable information

[6] FPIC serves as a coordination and advisory body to address technical and operational wireless issues relative to interoperability within the public safety emergency communications community, interfacing with voluntary representatives from federal, state, local, territorial and tribal organizations. FPIC is a technical advisory resource to Emergency Communications Preparedness Center (ECPC) Steering Committee, NCSWIC and National Public

regarding the complexities, required time, expenses and pitfalls associated with an ISSI connection between two LMR systems, and guided the ISICSB in the drafting of the *Staff Study - ISSI Committee Recommendation for Iowa Statewide Interoperable Communication System (ISICS) use of ISSI connection*.

Other projects include the efforts in 2018 to investigate encrypted interoperable communications pathways. These efforts defined current technological and procedural barriers to effectively deploying and managing encrypted interoperable talkgroups. The resulting work products were the ISICSB technical recommendation (TR-2018-002) *Multi-Key Equipped Subscriber Units* and a whitepaper *Encryption Needs in Iowa*. The whitepaper was presented at a recent P25 User Needs Subcommittee in San Antonio, Texas that was attended by LMR system administrators, users from other states along with federal partners and manufacturers. The presentation was well-received and expected to see further action in future meetings and working sessions.

A series of meetings were held in 2017 to develop a new and updated Statewide Communications Interoperability Plan (SCIP) using the Enhanced SCIP Process developed by the Office of Emergency Communication in the U.S. Department of Homeland Security. The process included representatives from DHS OEC who facilitated the events. Events were attended by members of the ISICSB including board members, committee members and the SWIC. Iowa's 911 program manager, Blake DeRouchey, also attended several of the meetings.

Planning aspects of the Enhanced SCIP included a strengths, weaknesses, opportunities and threats assessment of interoperability in Iowa, several phone calls with OEC personnel and several committee meetings. Some of those meetings were specific such as the Iowa Funding Webinar held in May of 2017. Other meetings included outlining each committee's action plan that fits in with its goals, metrics and objectives.

This new SCIP not only laid out a strategic plan for Iowa interoperable communications that outlines a vision, objectives and goals for the ISICSB, it also contains action plans to drive activities which make results a reality. This SCIP will be updated with DHS annually and monitored and adjusted as necessary to adapt to changing communications environments.

In 2018, various meetings were held with ECD to check on Iowa's progress through its listed goals in the SCIP. Measured progress was observed for each committee, and a couple of the goals are now completed. Several perpetual goals are listed as well to ensure that the ISICSB committees remain active.

A SCIP refresh is being discussed for calendar year 2019 that may update the goals of the various committees to reflect the current interoperable status in Iowa. This refresh will also aid in aligning Iowa's SCIP with the 2019 update to the NECP.

Safety Telecommunications Council (NPSTC) and a collaborative partner with SAFECOM and NCSWIC. (taken from https://www.dhs.gov/safecom/fpic/)

SWIC Maiers routinely visits counties to listen to local needs and discuss interoperability challenges and explain the benefits of an interoperable radio network like ISICS provides. He plans to visit all 99 counties and primary dispatch centers by the conclusion of calendar year 2021.

SWIC Maiers has also attended numerous county 911 service board meetings, several county level meetings and various state-level organizations comprised of local public safety personnel to discuss interoperable communications and answer questions regarding ISICS and FirstNet. In addition, SWIC Maiers provided technical assistance to counties regarding interoperability.

11. Identify, promote, and provide incentives for appropriate collaborations and partnerships among government entities, agencies, businesses, organizations, and associations, both public and private, relating to communications interoperability.

Part 10 above regarding a single unified SCIP (strategic plan) for Iowa between the ISICSB, 911 Program, and 911 Communications Council addresses this requirement.

Part 7 covers the collaboration and issuance of a statewide multi-state agency RFP for a land-mobile radio (LMR) system. The ISICS Platform will be completed in 2019 and completely fulfill this requirement.

Board Management and the SWIC presented at several events in 2018. The goal of the presentations was to update stakeholders on the ISICS Platform and the FirstNet initiative and create new potential partnerships for the FirstNet network in Iowa.

12. Provide incentives to support maintenance and expansion of regional efforts to promote implementation of the statewide integrated public safety communications interoperability system.

Part 7 touches on the multi-state agency land-mobile radio RFP.

The ISICSB is examining ways to expand the ISICS Platform to support regional efforts and bring to fruition the implementation of a statewide integrated public safety interoperable communications system. This may include work being done to identify long-term funding mechanisms.

13. In performing its duties, consult with representatives of private businesses, organizations, and associations on technical matters relating to data, video, and communications interoperability; technological developments in private industry; and potential collaboration and partnership opportunities.

In the past, ISICSB members and the SWIC met with all six Homeland Security regions creating six Regional Interoperability Committees (RICs) to advise ISICSB on issues of local concern, in addition to many county and city public safety groups regarding a statewide

LMR system. The SWIC also made presentations to various organizations across Iowa on ISICSB activities and the FirstNet NPSBN initiatives.

These outreach efforts continue as non-traditional stakeholders are engaged to discuss interoperability needs and ISICS access. These entities include for-profit ambulatory services, utility companies and other non-traditional public safety and public service stakeholders.

Another past accomplishment included the ISICSB Technology Committee and FirstNet Broadband subcommittee hosting a public private meeting inviting in telecommunications industry stakeholders to discuss options and concerns as FirstNet gets planned for Iowa. One outcome of that meeting was a letter to FirstNet recommending that the Iowa business community have an opportunity to compete for any business FirstNet may do in Iowa.

The ISICSB Operations Committee is currently maintaining a Public/Private subcommittee that meets as necessary to bridge concerns of private businesses providing communication resources to Iowa public safety community. This group did not meet in 2018, but it is probable that they will reconvene in 2019 as the ISICS Platform is completed and FirstNet continues to be deployed at a federal level.

The ISICSB Chair and SWIC expanded the ISICSB meeting model to include use of a conference line for all meetings, both Board and Committee, posting meetings times, dates and locations on the ISICSB website such that any interested party can listen into the meetings and comment under public comment periods. A virtual meeting room is used when necessary for document review and note-taking.

Former SWIC Allen and SWIC Maiers in addition to being part of TIA/TR-8 also participated in and are members of the Federal Partnership for Interoperable Communications (FPIC) and the National Council of Statewide Interoperability Coordinators (NCSWIC). FPIC is a federal group that is under the Emergency Communications Division (ECD) that meets regularly to investigate and solve problems pertaining to interoperability on a national level.

Participation in and feedback from FPIC has been vital in committee research into complex issues such as whether to use the ISSI on the ISICS Platform. Members of FPIC have also offered assistance and guidance regarding encryption on interoperable talk groups on ISICS and associated subscriber unit features via conference calls and meetings.

NCSWIC is a partnership with SWICs from all 50 states and six territories that evaluate interoperability challenges and coordinate with stakeholders to solve problems. These can range from establishing training opportunities to approving grants. NCSWIC also was vital in providing a pathway towards the Enhanced SCIP process that Iowa completed in 2017. The Enhanced SCIP process was viewed as an improvement over the previous methodology in developing a SCIP.

14. **Submit a report by January 1, annually, to the members of the general assembly regarding communications interoperability efforts, activities, and effectiveness at the local and regional level, and shall include a status report regarding the development of a statewide integrated public safety communications interoperability system, and funding requirements relating thereto.**

    This report satisfies this requirement.

VI. ISICS Deployment

1. Request for Proposal, Construction and System Acceptance

The request for proposal (RFP) for the ISICS Platform was released in 2013. Three companies bid on the RFP. Motorola Solutions was awarded the bid in 2015.

The contract for the deployment of the ISICS Platform was finalized and went into effect on May 1, 2015. Within the contract language, specific deadlines were established for the buildout of the system and final system acceptance is expected in early 2019.

Other stipulations of the contract included a 50% discount on all equipment using a statewide master purchasing contract. That same discount is accessible to local agencies that wish to purchase subscriber units or other LMR equipment.

The initial regulatory approval seeking process and construction commenced in late-2015 and early 2016. All regulatory processes are were completed in the summer of 2018. The status of the construction as of December 13, 2018 is shown in Figure 1 (larger map in Attachment 2). All sites are expected to be radiating signal in early 2019, and the vast majority of them are already as of December 2018. The lines connecting the sites represent the microwave backhaul paths that connect all the tower sites to the individual cores. The microwave backhaul paths make it possible for communications on talkgroups to carry across the state.

The ISICSB has commissioned a subcommittee to evaluate the effects of wind farms on the microwave backhaul paths. The subcommittee will develop a plan and policy to present to the Legislature regarding the protection of those paths to prevent interference on LMR networks in Iowa.

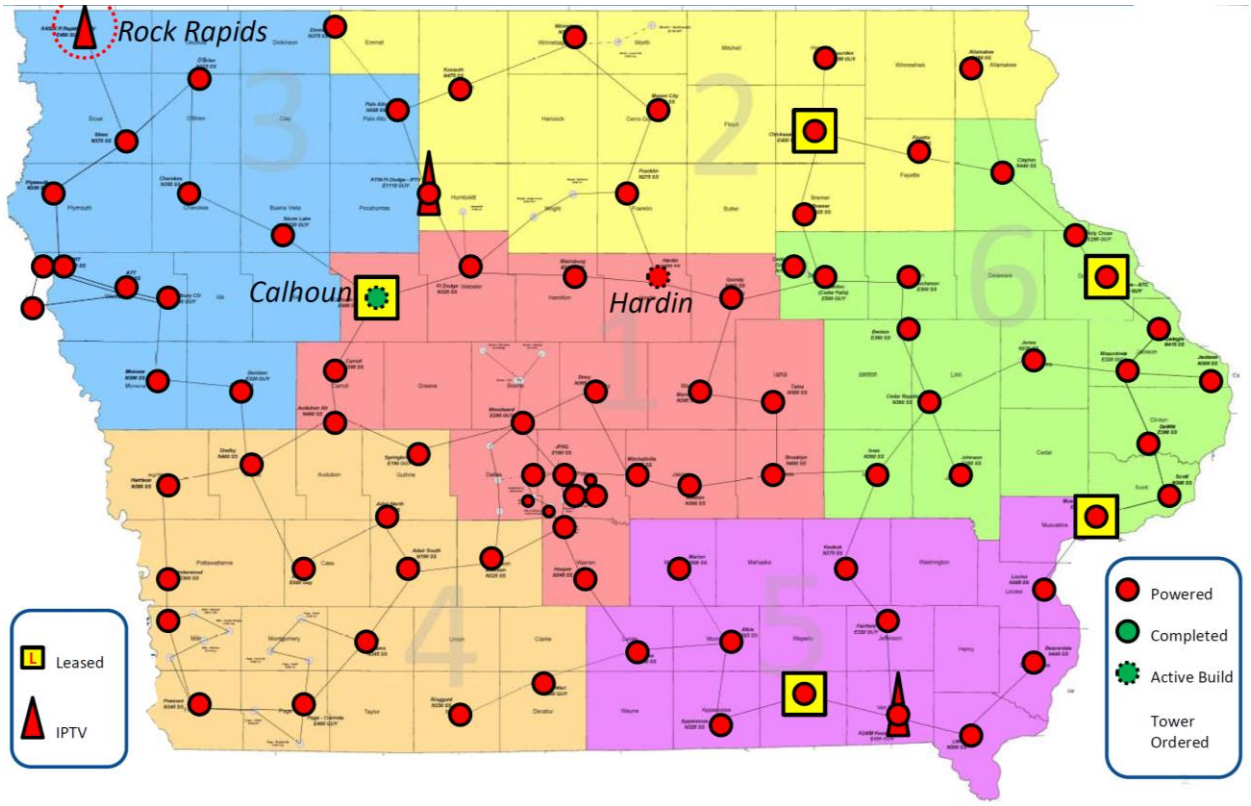


Figure 1. Current status of the ISICS Platform buildout as of December 13, 2018. Red dots are sites that have been completed and are fully powered. The labeled sites are in varying stages of completion. Rock Rapids is an Iowa Public Television site that is being built. Calhoun is under active construction, and the Hardin site is undergoing some final civil work before it is considered fully completed and powered.

Optimization of the ISICS Platform and acceptance testing is on-going and expected to be completed in early 2019. At that point, ISICS will be live for all public safety and public service personnel to use for interoperable communications.

2. Governance, Standards and User Approval

ISICSB and its committees are tasked with defining the governance structure and operation aspect of ISICS. In 2018 the discussion of several aspects commenced.

a. Governance
    i. The ISICS Platform Requires a complex set of standards, processes and procedures. To this end, ISICSB established a subcommittee to focus exclusively on policy and procedures for ISICS users as guidance for all users.
b. Approval of Users
    i. The User Group Committee (UGC) is tasked with reviewing an agency that applies for access to the ISICS Platform. The UGC reviews the agency's letter of intent, completed memorandum of agreement and matrix of users

documentation. Once those documents are reviewed, the UGC votes to approve the agency's access to ISICS.

c. Operations
    i. The Operations Committee is tasked with evaluating how the ISICS Platform should operate. The Operations Committee will pass polices to ensure that expected functionality is achieved.

3. Agency Use of the ISICS Platform

State agencies such as Iowa Department of Transportation (DOT), Iowa Department of Natural Resources (DNR), Iowa State Patrol (ISP), Iowa Department of Public Safety (DPS), Iowa Department of Corrections (DOC), Iowa Department of Public Health (DPH) and others are expected to use ISICS for operability as well as interoperability. Local entities such as Westcom in West Des Moines and the City of Des Moines along with counties of Boone, Dallas, Fremont, Hamilton, Humboldt, Mills, Montgomery, Page, Union, Worth, Woodbury and Wright have also chosen to use ISICS for operability and add tower sites to locally enhance the network. Numerous other agencies at a local, county and federal level have opted to use the ISICS infrastructure for some level of operability that does not include the addition of infrastructure. Several other counties have opted to join at increased levels for operability.

Local entities such as counties, sheriff offices and others have free access to ISICS and many have signed on to use ISICS for interoperability. Basic use of ISICS for interoperability comprises a Level 1 User. This is exemplified by a local agency that may have their own LMR network, but still needs to have radio communications with an outside entity like a neighboring county or state agencies.

In the summer of 2018, all Public Safety Answering Points (PSAPs) were pre-approved as Level 1 Users of ISICS. This allows for and helps facilitate the deployment of control stations to get them connected to ISICS for interoperability.

A Level 2 User of ISICS consists of a local agency using basic free access and ability to interoperate with other agencies, but also wants an enhancement of features of ISICS system which would include custom talk groups for their local operations (operability). Several local public safety entities and federal agencies have joined ISICS as a Level 2 user.

A Level 3 User brings all the features of Level 1 and Level 2, but adds in direct connection to the ISICS core computers via a hardline or hardwire connection to the system. This direct connection to the system requires significant engineering and coordination and allows for extra features for use by this local agency. Agencies that have opted to join as a Level 3 or

higher user include: Boone County, City of Des Moines, Dallas County, Fremont County, Greene County, Hamilton County, Humboldt County, Hancock County, Harrison County, Monona County, Mills County, Montgomery County, Page County, Union County, University of Northern Iowa, Warren County, Westcom, Woodbury County, Worth County and Wright County.

Level 4 Users have chosen to add infrastructure to the network such as additional towers, at the local agency cost to enhance performance and/or expand the coverage offered by ISICS in their community. Enhancements may be needed to guarantee a feature like in-building coverage. Agencies or counties that have opted to use ISICS as Level 4 Users are Boone County, City of Des Moines, Dallas County, Fremont County, Hamilton County, Humboldt County, Mills County, Montgomery County, Page County, Union County, University of Northern Iowa, Westcom, Woodbury County, Worth County and Wright County.

4. Local Cost Savings

The ISICS Platform can present significant cost-saving opportunities to local counties if they currently need to update or replace their existing LMR infrastructure or improve interoperability. Many counties are still using very high frequency (VHF) networks that have been narrow banded by the FCC. Narrow banding greatly reduced the capability and coverage of VHF networks and caused most Iowa communities to reevaluate their public safety communications systems. Since ISICS provides an average mobile coverage of 95% across the state, ISICS could serve as a starting point for local agencies when considering options in replacing their current radio systems and improve statewide interoperability. As just one example, if an ISICS tower is located within their county, that existing tower has the potential to cut local costs of a local LMR project by $500,000 to $1,000,000 in many cases. Using ISICS for many communities could eliminate this need for additional communication towers and therefore reduces community tax burden.

Letters were sent to all public safety answering points (PSAP) in early 2018 that outlined preparatory steps that can be taken for ISICS access. This was intended to allow for long-term planning strategies that local entities can use for their interoperable communications plans. A follow-up letter was sent in the summer of 2018 with a survey. In the fall of 2018, a grant program that was run with partners from HSEMD and DPS to help provide equipment to PSAPs that did not already have a connection to ISICS for interoperability.

There is a potential role for the Iowa Legislature to further promote interoperability in Iowa by financially empowering the ISICSB to assist counties, PSAPs and other dispatch centers in identifying a pathway to ISICS access.

VII. Attachments for 2018

1. **2017 SCIP**
2. **Map of ISICS Network**
3. **List of agencies and counties that have joined ISICS for interoperability and/or operability.**
4. **Standards adopted in 2018:**
5. **Documents published in 2018:**
   - **Technical Recommendation – ISICSB TR-2018-001** – *Programming Guide Technical Recommendation*
   - **Technical Recommendation – ISICSB TR-2018-002** – *Multi-Key Equipped Subscriber Units*
   - **White Paper –** *Encryption Needs in Iowa*

Attachment 1: 2017 SCIP

Iowa Statewide Interoperable Communications System Board (ISICSB)

STATEWIDE COMMUNICATION INTEROPERABILITY PLAN

2017-2020

Developed with Support from the
US Department of Homeland Security, Office of Emergency Communications

DRAFT-INTERNAL WORKING DOCUMENT

THIS PAGE INTENTIONALLY BLANK

LETTER FROM THE SWIC

Greetings,

I am pleased to present to you the 2017 Iowa Statewide Communication Interoperability Plan (SCIP). This SCIP represents Iowa's continued commitment to improving emergency communications and supporting the public safety practitioner community. The 2017 SCIP marks the next step towards achieving the National Emergency Communications Plan's (NECP) vision for interoperable communications at the local, regional, state, and federal level.

With support from the Department of Homeland Security's Office of Emergency Communications (OEC), representatives from the Iowa Statewide Interoperability Communications System Board (ISICSB) and several other state and local public safety agencies from across Iowa collaborated to redefine and enhance the SCIP. As a result of the efforts to update the SCIP, you will find both new and ongoing interoperability initiatives in the SCIP.

The State of Iowa faces complex challenges as we work towards achieving public safety interoperability. For the next three-to-five years, this strategic plan will guide our efforts provide robust, reliable, and interoperable communications to the entities that protect and serve the 3 million citizens and communities throughout Iowa through effective governance, enhanced technology, and sensible funding for emergency communications.

As we move toward our goal of interoperability, we must remain dedicated and strive to improve our ability to communicate among disciplines and across jurisdictional boundaries. With help from public safety practitioners statewide, we will work to achieve the goals set forth in this SCIP and become a nationwide model for statewide interoperability.

Sincerely,

Chris Maiers
Statewide Interoperability Coordinator
Iowa Statewide Interoperable Communications System Board
Iowa Department of Public Safety

DEVELOPED WITH SUPPORT FROM THE DHS OFFICE OF EMERGENCY COMMUNICATIONS

Iowa SCIP Workshop, June 28, 2017

On June 28-29, 2017, Iowa hosted a SCIP Workshop to develop goals to improve interoperable emergency communications in three key areas: Governance, Technology, and Funding and Sustainment. Stakeholders leveraged the successes and gaps that were previously identified during the Governance, Technology, and Funding and Sustainment engagements to assign goals and tactics, account for planning activities involving new technologies and the emergency communications ecosystem, and incorporate national efforts and strategies as needed.

The Iowa Statewide Communication Interoperability Plan (SCIP) is a stakeholder-driven, multi-jurisdictional, and multi-disciplinary strategic plan to enhance interoperable and emergency communications across the state. The Enhanced SCIP is a critical mid-range (three to five years) strategic planning tool to help Iowa prioritize resources, strengthen governance, identify future investments, and address interoperability gaps.

Figure 1: Enhanced SCIP

Development of the Iowa Enhanced SCIP was a collaborative process among Iowa Statewide Interoperable Communications System (ISICS) Board members and public safety stakeholders from across disciplines, agencies, and jurisdictions within the State Iowa. This process followed a systematic approach to identify successes, gaps and challenges in governance, technology, and funding and sustainment through the process identified in figure 1. The process began with the Governance Engagement to review and discuss efforts on how they can be improved to make governance more efficient and effective. The next step involved a webinar discussing funding and sustainment requirements that included sharing various funding practices from across the country. The third and final engagement prior to the SCIP Workshop was the Technology Engagement. The Technology Engagement identified Iowa's current technologies for Land Mobile Radio (LMR), Broadband, Next Generation 9-1-1 (NG9-1-1) and Alerts and Warnings. For each of the identified technologies, participants mapped out what one would expect these technologies to be in the next three to five years to address the anticipated needs of public safety and the public's expectations given today's understanding of those technology capabilities.

Through this collaborative process stakeholders from across disciplines, agencies, and jurisdictions within the State Iowa's successes, gaps and challenges in governance, technology, and funding and sustainment were identified and captured

Data gathered during engagements was then leveraged during the Strategic Goals and Implementation Plan engagement, also referred to as the SCIP Workshop, to guide the goal development efforts of participants. The resulting goals are provided within this strategic plan. The Evaluation and Progress Management component represents Iowa's completion of the Annual SCIP Snapshot Report which measures the progress made towards Iowa's goals.

TABLE OF CONTENTS

INTRODUCTION

Guiding Approach / Principles

Modernization of emergency communications components is facilitating the flow of information and communications among government agencies, the private sector, the public, and in some cases, with entities from neighboring counties.

The deployment of FirstNet, wireless broadband networks and applications will greatly influence incident operations as they become more prevalent and are more widely adopted by emergency responders. In addition to FirstNet, there are also efforts to update the Nation's 9-1-1 infrastructure to Next Generation 9-1-1 (NG9-1-1), and the recent deployment of a nationwide public alerting system that uses traditional media, such as broadcast and cable, as well as Internet Protocol-based technologies to transmit alerts to mobile phones and other devices. When considering and preparing for these changes to the emergency communication's landscape, Iowa has developed the Enhanced SCIP using a more holistic approach to strategic planning that incorporates the emergency communications ecosystem and the Interoperability Continuum.

The broader emergency communications ecosystem consists of many inter-related components and functions, including communications for incident response operations, notifications and alerts and warnings, requests for assistance and reporting, and public information exchange. The primary functions of the emergency communications ecosystem are depicted in the 2014 National Emergency Communications Plan[1].

Vision

All emergency response entities in and around Iowa can access common standards-based interoperable statewide communications systems within established public safety guidelines and adhering to industry best practices.

The Interoperability Continuum[2] was developed by SAFECOM and serves as a framework to address challenges and continue improving operable/interoperable and emergency communications. It is designed to assist emergency response agencies and policy makers with planning and implementing interoperability solutions for voice and data communications. In an effort to align the lanes of the continuum to Iowa's committees, an updated interoperability continuum shown in Figure 2 was developed during the Governance engagement to include the Finance and Security lanes. These new lanes include milestones to guide progress towards improving interoperability. The emergency communication's ecosystem and the updated

Mission

In accordance with the code of Iowa and established laws, develop standardized interoperable communications through established governance structures. Provide standards-based public safety communications through strategic direction to enhance and achieve the highest level of interoperable public safety and emergency communications.

[1] The 2014 National Emergency Communication Plan is available here: https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf

[2] OEC's Interoperability Continuum is available here: http://www.safecomprogram.gov/oecguidancedocuments/continuum/Default.aspx

Interoperability Continuum were used as the foundation to guide the development of Iowa's goals and future objectives towards enhancing interoperable communications. This combined framework has resulted in a strategic plan that coordinates the mutually-supportive strategies of Land Mobile Radio (LMR), NG9-1-1, FirstNet, nationwide public alerting systems, and other major capabilities that are being deployed across the nation.

During the Iowa SCIP Workshop, participants developed goals based on the priorities of the Iowa Statewide Interoperable Communications System Board's (ISICSB) committees, which are: Finance, Governance, Operations, Outreach, Technology, Training and Exercise, and User Group. Stakeholders leveraged the successes and gaps that were previously identified in the Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis, depicted in Appendix B, and during the Governance, Technology, and Funding and Sustainment engagements. Stakeholders then assigned goals, metrics for success, objectives and action plans to account for planning activities involving new technologies, state priorities, and Code of Iowa obligations. Each developed goal is assigned to a committee, however, in order to accomplish a specific action item or objective committees often collaborate on projects.

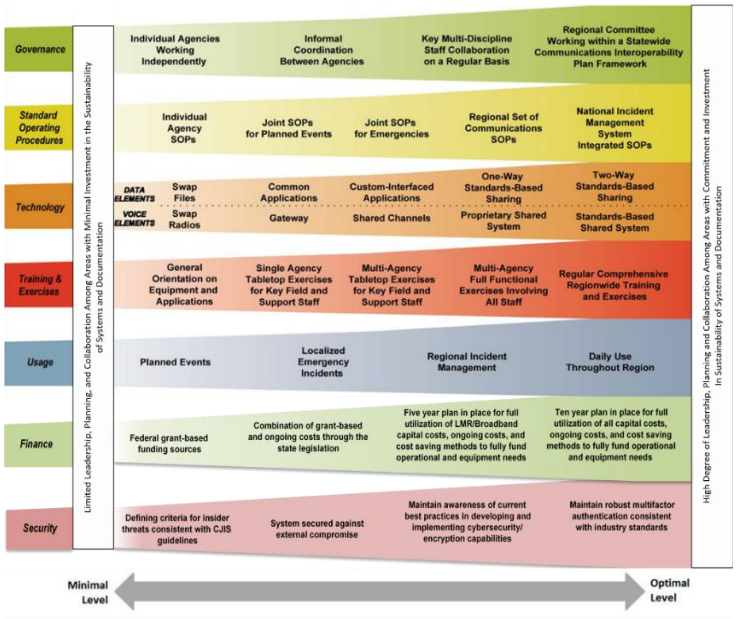


Figure 2: Iowa Interoperability Continuum

Iowa Enhanced SCIP Overview

- **Overview of Strategic Goals, Objectives and Benefits –**
  - Provides an executive summary of the SCIP goals and objectives and their intended benefits. Iowa developed goals, objectives, and metrics for success for each of the seven committees during its SCIP workshop.
- **Governance & Coordination –**
  - Describes the current mechanisms for communications interoperability governance within the state along with successes, challenges, and priorities for improving governance within the evolving landscape.
- **Technology & Operations –**
  - Describes the core systems used to support public safety communications within the state and the technological and operational enhancements needed to maintain and enhance interoperability across the emergency communications ecosystem.
- **Funding & Sustainment –**
  - Describes the funding sources and allocations that support interoperable communications capabilities within the state along with methods and strategies for funding sustainment and enhancement of needed capabilities into the future.
- **ISICSB Committee Mission Statements and SCIP Goals & Objectives –**
  - Provides each of the seven committee mission statements and their goals and objectives.
- **Implementation Plan –**
  - Describes how Iowa plans to implement, maintain, and update the SCIP to enable continued evolution of and progress toward its interoperability goals.

OVERVIEW OF STRATEGIC GOALS & OBJECTIVES

Governance & Coordination

Develop appropriate governance through creation of mission statements and assigned goals for each ISICSB committee.

Technology & Operations

Maintain existing systems and adopt emerging technologies with a focus on statewide LMR, Broadband, NG9-1-1, and Alerts and Warnings systems.

Funding & Sustainment

Develop a 5-year financial plan for the operation of Iowa's statewide system and broadband planning.

GOVERNANCE & COORDINATION

Current State of Governance

Iowa established the Iowa Statewide Interoperable Communications System Board (ISICSB) in 2007. Under Code of Iowa sections 80.28 and 80.29, ISICSB's purpose is to develop, implement, and oversee policy, operations, and fiscal components of communications interoperability at the state and local level, as well as coordinate similar efforts at the federal level. The ultimate objective of the board is to develop and oversee the operation of a statewide integrated public safety communication interoperability system. See Appendix D for the Code of Iowa sections 80.28 and 80.29.

The Code of Iowa has established an annual reporting requirement on the status of the ISICSB. The Board has 19 voting members, including nine state department representatives, 10 local public safety members (police, fire, EMS), one at-large member, and four ex officio legislative members, all of which are not voting members. The current governance structure is depicted in figure 3.

During the Iowa Governance Engagement on May 9, 2017, participants developed mission statements for each of its seven committees. They also determined a need to add financial and security lanes to the SAFECOM Interoperability Continuum and create a new ISICSB Security Committee. Appendix C includes an overview of each committee and its assigned goals and measurement of success.

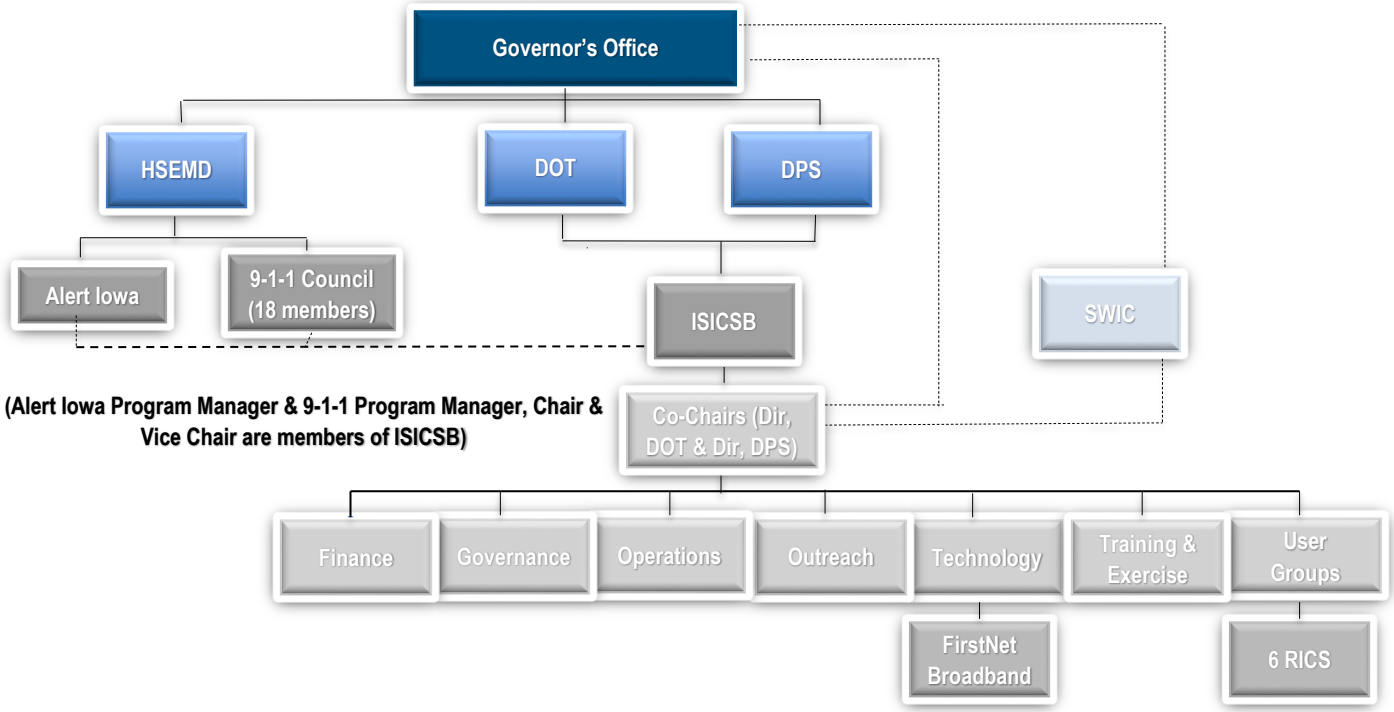


Figure 3: Governance Organization Chart

Creation of a Security Committee

The creation of a new committee will require the Board to identify a Chair and Vice Chair of the committee. Since the ISICSB receives its direction from the Code of Iowa, they do not have a charter. Instead the ISICSB has administrative rules that only require a simple vote of the Board to elect the positions of the Chair and Vice Chair.

General membership of the new committee, including the Chair and Vice Chair, will need to include people with cybersecurity expertise. The state will work to identify these members outside of its current structure because they currently do not have the specific skill sets required. This effort may pose the opportunity for the ISICSB's first public/private partnership. The Board will consider partnering with the agencies or universities to identify a mixed group of specialists who may or may not have any knowledge of public safety.

There is the possibility that this security committee will be a subcommittee of Technology much like the Broadband subcommittee. Under the Technology Committee, the Security subcommittee's primary goal will be to assist the Regional Interoperability Committees (RICs), which are subcommittees of the User Group Committee.

TECHNOLOGY & OPERATIONS

During the Iowa Technology Engagement conducted on May 10, 2017, participants identified the current and desired states of technology involving: Land Mobile Radio, Broadband/Data, Next Generation 9-1-1 and Alerts and Warnings. An overview of the desired state of technology in Iowa is shown in figure 4. Findings through this exercise have helped inform the development of Iowa SCIP goals and objectives, and can be found in Appendix C. Appendix A also includes a list of systems used in the state.

Land Mobile Radio

The State of Iowa has many different LMR systems in place. Many are stand-alone, some are on the State's ISICS system or have the ability to be on that system, and most have the ability to use the VHF conventional interoperability channels statewide.

- About 70% of the State of Iowa is on non-P25 VHF conventional systems with a few areas having VHF P25 systems.
- Most of the state has access to two standard VHF interoperability channels, Point-To-Point (155.3700MHz) and VLAW31 (155.4750 MHz).
- The state has many stand-alone 700 & 800 MHz systems, some of them are Frequency Division Multiple Access (FDMA) while others are Time Division Multiple Access (TDMA).
- Some agencies use a private vendor to provide their radio system infrastructure.
- The state has developed and is currently deploying their new 700MHz statewide system. The system is still in its infancy stages as more sites and users are added.

Desired Technology State

- 100% of radio systems interface with ISICS and use the same nomenclature
- Program all radios with a standard interoperability template
- Have less local reliance on vendors
- Greater public safety use of FirstNet
- 98% or better coverage of both indoor and outdoor
- Convergence of the Wireline and Wireless networks
- Establish SOPs for NextGen 9-1-1
- Improve security of warnings systems
- Update alerts and warnings
- Coordinate with agencies to push out alerts and warnings to the public

Figure 4: Desired Technology State

Broadband

Iowa currently uses multiple commercial vendors to support broadband use. Data for public safety is currently being used for:

- Mobile data in the field
- Computer Aided Dispatch (CAD)
- Live streaming video
- OTAR (Over the Air Rekeying) of radios that allows the ability to send new encryption keys over the air vs. physically touching each radio.
- Over the Air Programming (OTAP) of radios that allows the ability to reprogram or update talk groups over the air vs. physically touching each radio.
- AVL (Automatic Vehicle Location), this is the ability to track vehicle movement which is one feature that is part of the State of Iowa's MACH (Mobile Architecture for Communications Handling) mobile data system for law enforcement.
    - TraumaHawk App -This is a smartphone app designed by the University of Iowa that allows first responders in the field the ability to send pictures of an accident to the receiving hospital to give the hospital a greater awareness of the extent of injuries and/or vehicle damage.
    - Iowa is has completed a pilot called Wi-Fi for School Emergencies (WISE). The WISE Pilot is designed around increasing police presence at schools by establishing outdoor wireless access points that law enforcement can use to upload dash and body camera video. The network may also be used during a school emergency

9-1-1 / Next Generation 9-1-1

The 911 Communications Council was established to serve in a consultative role with the 911 Program Manager and the Director of the Homeland Security and Emergency Management Department (HSEMD). The goal of the Council is to advise and make recommendations to the Director and Program Manager regarding implementation and development of the 911 system in Iowa. The ISICSB and 911 Communications Council lead and support interoperable and emergency communications-related efforts in Iowa. These two groups exist as separate but as closely coordinated entities who share a common vision and mission. In fact, the majority of the Council members sit on at least one of the ISICSB seven committees.

Alerts & Warnings

The Alert Iowa Notification System is the state's primary alert system, but is not used by every agency. Other systems used include: Code RED, Reverse 9-1-1 and Everbridge. Iowa stakeholders have stated the value of incorporating alerts and warnings and National Weather Service's Forecast Offices on its statewide LMR system – ISICS.

FUNDING & SUSTAINMENT

Current State of Funding

ISICSB, as well as other commissions in Iowa, are not given a stand-alone budget, rather funds are distributed through the state's Department of Transportation (DOT) and the Department of Public Safety (DPS). Currently, the Board receives $154,000 to lead enhancements in statewide interoperability. From 2007 to 2010, the Board also received a total of $12.1 million in grants, primarily from the Public Safety Interoperability Communications Grant (PSIC) and the Interoperable Emergency Communications Grant Program (IECGP). In Fiscal Year (FY) 2016, House File 651 appropriated $4 million from the E911 Emergency Communications Fund to the Homeland Security and Emergency Management Department (HSEMD) to pay for the lease costs associated with the Iowa Statewide Interoperable Communications System (ISICS). For FY 2017, $4.4 million was appropriated for the lease costs in Senate File 2326. For FY 2018, HF 643 appropriated $4.4 million from the Rebuild Iowa Infrastructure Fund. This platform will be under the joint purview of the DPS and the DOT[3].

911 Surcharges

Iowa operates off a one-dollar surcharge on wire and wireless phones for 911. Wireline 911 surcharge funds go directly to the counties, while the wireless 911 surcharge funds go to the state who then pays for the management of the networks. Remaining funds are distributed to counties to support their efforts.

State and Local Implementation Grant Program (SLIGP)

Iowa is currently using a State and Local Interoperability Grant Program's (SLIGP) grant to fund a full-time SWIC under DPS as well as a FirstNet Outreach Coordinator.

Maintenance Costs for the ISICS Platform

Maintenance has been built into a 10-year contract with Motorola for the ISICS platform. After the warranty ends in the third year the state will be responsible for the maintenance costs which are $1.6 million annually. Funding needs to be identified to pay for the maintenance when it arises. The estimated power costs for the platform will be $275,000 a year for all 90 sites present when this document was drafted. DPS is also responsible for the cost.

Five-Year Funding Plan

Iowa has identified a need to develop a five-year funding plan to establish processes and procedures involving expenditures on ISICS and a broadband data network, which will include the following:

- Identify what role the board should take regarding the sustainability and maintenance of the system
- Include the $1.6 million in annual maintenance costs after the third year
- Funding of control stations

Once the plan is complete, the governance and finance committees will work with the SWIC to present it during the November 2017 meeting and then the ISICSB will approve it during the December 2017 meeting. Then the approved plan must be uploaded into a website through the Legislative Services Agency (LSA).

[3] Source: https://www.legis.iowa.gov/docs/publications/FT/692724.pdf

ISICSB COMMITTEE MISSION STATEMENTS AND SCIP GOALS & OBJECTIVES

Finance Committee

Mission Statement: The Finance Committee identifies potential funding streams and coordinates existing funds for interoperable communications priorities.

Goal #	Goals	Objectives	Benefits
1.	*Develop appropriate process and procedures for acquiring resources, administering processing payments using state and grant funds for enhancement, deployment and operation of ISICS and a five-year financial plan by June 2018*	• Develop annual fiscal processes which meets GAAP/GAAS requirements for ISICS Project	• Process developed and implemented for acquiring resources, processing payments using state or grant funds promotes transparency • Development and administration of a 5-year financial plan promotes transparency
2.	*Develop appropriate process and procedures for acquiring resources, administering processing payments using state and grant funds for enhancement, deployment and operation of broadband data network and a five-year plan by June 2018*	• Develop annual fiscal processes which meets GAAP/GAAS requirements for statewide data network	• Process developed and implemented for acquiring resources, administering and processing payments of state or grant funds promotes transparency • Development and administration of a 5-year financial plan promotes transparency
3.	*Develop appropriate process and procedures for administering all financial assets consistent with national best practices in accounting and auditing*	• Develop annual fiscal process which meets GAAP/GAAS for administering state and federal funds consistent with Code of Iowa and grant guidelines • Align with the grant process developed by the ISICSB	• Establishes known processes and procedures for budgeting, accounting, inventorying and auditing all financial assets of ISICSB whether state or grant funds

Governance Committee

Mission Statement: The Governance Committee develops and coordinates the policy and procedural operations of the ISICSB and ensures it functions within the law in a public and transparent manner.

Goal #	Goals	Objectives	Benefits
4.	*Develop appropriate governance through creation of policy and procedure statements for enhancement, deployment and operation of ISICS*	• Develop policies as requested • Disseminate policies as needed	• Promotes a shared understanding of governance involving the statewide system
5.	*Develop appropriate governance through creation of policy and procedure statements for enhancement, deployment and operation of a statewide broadband network*	• Develop policies as requested • Disseminate policies as needed	• Promotes a shared understanding of governance involving statewide broadband network
6.	*Establish a process to administer grant funds or communications assets*	• Develop policies as requested • Disseminate policies as needed	• Promotes awareness of how grant funds and communications assets are invested

Operations Committee

Mission Statement: The Operations Committee collaborates and develops the operational protocols and procedures for interoperable communications.

Goal #	Goals	Objectives	Benefits
7.	*At the end of five years 95% of all dispatch centers have access to ISICS*	• Identify dispatch centers that need access • Establish operational policies for ISICS access • Deliver recommendation/documentation to ISICSB	• Advances interoperability statewide by connecting dispatch centers to ISICS
8.	*To review the ISICS draft policies and make recommendations to Standards Working Group*	• Review and document recommendations to the Standards Working Group representative	• Creates an opportunity to update ISICS policies
9.	*Align and update legacy plans, including system failures*	• Identify, review and update existing communications plans and include a system failure plan • Deliver recommendation/ documentation to ISICSB	• Creates an opportunity to address issues with existing communications plans

Outreach Committee

ISICSB
911
Iowa Statewide Interoperable Communications System Board

Mission Statement: The Outreach Committee builds coalitions to support and promote interoperable public safety and emergency communications by providing clear and pertinent information to stakeholders and decision makers.

Goal #	Goals	Objectives	Benefits
10.	*To develop and deliver outreach materials for use in making decisions to become a user of ISICS (by final system acceptance) by June 2018*	• As needed, identify if a plan needs to be developed to respond to changes with ISICS • Develop outreach materials specific to elected officials and targeted audiences	• Promotes awareness of benefits of becoming an ISICS user
11.	*To develop and deliver outreach materials for use in making decisions to become a user of broadband network by 90 days after adoption of the state plan or by Spring 2018.*	• Leverage guidance and input from the Broadband sub-committee • As needed, identify if a plan needs to be developed to respond to changes with broadband • Develop Iowa-specific materials from broadband providers • Develop outreach materials specific to elected officials and targeted audiences	• Promotes awareness of benefits of becoming a broadband network user
12.	*Develop a plan for utilizing social media relative to ISICSB activities and interoperability issues*	• Adoption of social media plan • In five years, the ISICSB website or the SWIC becomes the primary and central point for information	• Allows for a wide audience to be reached with information pertaining to interoperability.
13.	*Approach and educate elected officials*	• Develop a training plan • Engage association partners	• Creates “interoperability champions” to advocate on behalf of ISICSB priorities involving funding and other needs to advance interoperability statewide

Technology Committee

Mission Statement: The Technology Committee researches emerging technologies and standards to develop technical recommendations and procedures to enhance interoperable public safety and emergency communications.

Goal #	Goals	Objectives	Benefits
14.	*To lead technological solutions for voice interoperability*	• To develop standards for ISICS communications equipment • Create minimum standards for ISICS interoperable communications equipment	• Supports interoperability involving voice across communications equipment
15.	*To lead technological solutions for data interoperability*	• Create minimum standards for interoperable communications equipment • Make recommendation to ISICSB to adopt standards	• Supports interoperability involving data across communications equipment
16.	*Investigate voice and data convergence and differentiating the needs of public safety*	• Investigate technology • Choose best course of action • Make recommendations	• Identifies planning considerations for the convergence of voice and data

Training & Exercises Committee

Mission Statement: The Training and Exercise Committee provides training opportunities on interoperable communications and procedures for planned and unplanned events.

Goal #	Goals	Objectives	Benefits
17.	*Develop and provide standard core training for interoperable communications across the various state regions*	• Establish guidelines defining standard core training • Embed communications training within existing state training institutions	• Promotes consistent training across state regions
18.	*Expand the statewide core group of trainers who would be able to teach necessary COMU positions classes and increase COMU awareness*	• Create a COMU awareness outreach program for dissemination through the Outreach Committee • Seek Train-the-Trainer classes	• Increases the number of trainers to promote more training and organization of statewide COMU program
19.	*Develop a cost analysis of training to augment future budgetary planning*	• Obtain training funding	• Identifies funding needs for training

User Group Committee

Mission Statement: The User Group Committee, comprised of authorized users, coordinates access and usage policies for use of or interfacing with the ISICS platform and public safety broadband systems.

Goal #	Goals	Objectives	Benefits
20.	*Develop processes and vet the application process for access to the ISICS interoperable communications platform within state or grant resources.*	• Add efficiencies to application process • Determine resource needs for an objective evaluation of Level 3 and 4 resource users	• Decreases application process time relative to number of applications per user level • Encourages increased number of users
21.	*Develop processes for guidance on broadband data interoperable communications platform within state or grant resources.*	• Identify and deploy process to assist in the application for broadband access	• Decreases application process time relative to number of applications per user level • Encourages increased number of users
22.	*Strengthen all RICs*	• Travel to every county to conduct outreach to all stakeholders • Listen and accept feedback • Identify meeting frequency and appropriate tasks	• Increases RIC user attendance, participation, and investment

IMPLEMENTATION PLAN

Evaluation and Progress Measurement

Iowa's SCIP is owned and managed by the ISICSB. Through the Code of Iowa, the ISICSB has both authority to, and is responsible for, making decisions regarding the SCIP and is responsible for its implementation and maintenance. The SCIP goals align with the Code of Iowa in order to ensure compliance and tied to a budget funding stream to ensure their completion.

The ISICSB will add the goals assigned to the committees as a formal agenda item for its regular meetings. Appendix C outlines each committee's mission, assigned SCIP goal and objective, metrics of success and action plan based on the 2017 workshop. Committee members are expected to utilize developed action plans to implement their respective areas of the SCIP.

Each Committee Chair or their designee will provide regular status updates to monitor work, or lack thereof, done by the Committee, subcommittee or working group to track progress and address as needed. These status updates will contribute to the state's Annual Report to the Governor and to the Annual SCIP Snapshot.

The ISICSB will also conduct a thorough review of the SCIP on a biennial basis to update goals and objectives to address identified needs and advancements involving statewide emergency communications capabilities.

DHS Support

Each year, OEC works with all 56 states and territories in measuring progress towards implementing SCIP goals through the annual SCIP Snapshot process. Findings from the reporting help identify successes and challenges in meeting goals, and help OEC provide targeted technical assistance in the form of training and resources offered through its Interoperable Communications Technical Assistance Program (ICTAP).
ICTAP offerings of interest include:

- Formal Governance Documentation Review, Assessment and Development
- Communications Unit (COMU) Planning and Policies, Project Management
- Tactical Interoperable Communications Plan (TICP) Field Operations Guide (TIC-FOG) Review and Development
- Next Generation 9-1-1 / Strategic Planning Support
- Communications Unit Leader (COML) Training
- Communications Unit Technician (COMT) Training
- Communications Assets Survey and Mapping (CASM) Tool – Next Generation

Requests for technical assistance are coordinated through the Iowa SWIC on an annual basis.
For more information, states/territories are encouraged to contact OEC at: SCIP@hq.dhs.gov.

APPENDIX A: List of Acronyms

Below is a list of acronyms used throughout this document.

COML	Communications Unit Leader
COMT	Communications Unit Technician
COMU	Communications Unit
DHS	Department of Homeland Security
GAAP	Generally Accepted Accounting Practices
GAAS	Generally Accepted Auditing Standards
HSEMD	Homeland Security and Emergency Management Department
ISICS	Iowa Statewide Interoperable Communications System
ISICSB	Iowa Statewide Interoperable Communications System Board
LMR	Land Mobile Radio
MHz	Megahertz
NECP	National Emergency Communications Plan
NG9-1-1	Next Generation 9-1-1
OEC	Office of Emergency Communications
P25	Project 25
PSAP	Public Safety Answering Point
RIC	Regional Interoperability Committee
SCIP	Statewide Communication Interoperability Plan
SWIC	Statewide Interoperability Coordinator
VHF	Very High Frequency

APPENDIX B: SWOT Analysis

	LMR	Broadband	Code of Iowa Duties	Alerts & Warnings
Strengths	• Deployed Iowa Statewide Interoperable Communications System (ISICS), P25 Statewide Radio System • Deploying LMR backbone across the state • Local participation • Procedures and policies address and prepare for conventional systems and new technologies (i.e., eliminating interference issues) • Public Safety Answering Points (PSAPs) are preparing for the ISCIS	• Established broadband committee • Collaborating with Governor's Office • State public safety uses data frequently • Dedicated broadband for public safety at school locations (WISE) • One of the first states to define public safety grade	• Guiding 700Mhz network buildout • Dedicated funding stream • Current committee structure is responsive to planning needs • Established public/private partnerships (Motorola – LMR) • FirstNet Broadband subcommittee hosting fourth public/private partnerships summit • Strived to partner with local exchange carriers for FirstNet • Collaborating with local utility companies • Outreach and information sharing • Adopted FPIC encryption • Strong collaboration between 911 Board and state interoperability board	• Most counties use Alert Iowa--Statewide system for alerts and warnings, incorporates reverse 911, integrates IPAWS • Outdoor and indoor warning systems • Paging systems
Weaknesses	• Diversity of radio frequency use • Tactical Interoperability Communications Plan (TICP) not current • Funding • Outreach and education on ISCIS • CASM adoption • No master RFP to provide to local stakeholders • Legislature allocated surplus 911 funds to build and implement statewide radio • Unpredictability of long-term funding	• Stakeholders have limited broadband technical knowledge • Reliance on commercial carriers for information • No dedicated funding stream	• No authority to enforce decisions • No ability to administer grants • Interoperability continuum does not emphasize cybersecurity • Need additional subject matter expertise for new and evolving technology • Lack of succession planning	• Multiple points of contact for alerts and warnings • Lack of standards

Opportunities	• Identifying funding to pay for 8-year commitment to Motorola • Clearly define interface • Inclusion of public service as users • Identifying overall funding stream/source of revenue for grants to continue expanding system • Access to ISCIS from every PSAP and department • Create buy in and involve local stakeholders with new and evolving technology • Adding a representative from each county (99) on subcommittees • Developing a regional governance system	• Expanding ICSIC • Adopting FirstNet • Development of applications • Sharing information with all stakeholders and decision makers	• Leveraging voting seat on Telecommunications Industry Association (TIA) • Create grant funding method to push grants to locals	• Some counties still have the opportunity to join Alert Iowa • Addressing Alerts & Warnings in the SCIP
Threats	• Funding • Not been strategic in the deployment of grant resources • Sensitivities between LMR and 911 due to allocation of surplus 911 funds • Other vendors pre-P25 system and subscribers' loyalty agencies rely on consultants to address technology • Lacking technical expertise • Local stakeholders listen to vendors rather than technical experts • Vendor recommendations may not serve vision for interoperability • Lacking enforcement of public safety grade • Cost of service and devices • General distrust of state and federal solutions			

APPENDIX C: ISICSB Committee SCIP Goal Implementation & Measurement

FINANCE COMMITTEE			
Mission Statement: The Finance Committee identifies potential funding streams and coordinates existing funds for interoperable communications priorities.			
Goals	**Metrics for Success**	**Objectives**	**Action Plan**
Develop appropriate process and procedures for acquiring resources, administering processing payments using state and grant funds for enhancement, deployment, and operation of ISICS and a five-year financial plan by June 2018	• Process developed and implemented for acquiring resources • Process in place for administering and processing payments of state or grant funds • Development and administration of a five-year financial plan.	• Develop annual fiscal processes which meet GAAP/GAAS requirements for ISICS Project	• Identify costs of operation and sustainment • Identify more resources or efficiencies to ensure the budget aligns with the Board's goals • Each committee, at the direction of the Board, will submit priorities to the Finance Committee, making sure they align with the budget process, to decide whether it is within the budget • Compare last few years of expenditures to project the five-year plan and continue to revise it on an annual basis
Develop appropriate process and procedures for acquiring resources, administering processing payments using state and grant funds for enhancement, deployment and operation of broadband data network and a five-year financial plan by June 2018	• Process developed and implemented for acquiring resources • Process in place for administering and processing payments of state or grant funds • Development and administration of a five-year financial plan.	• Develop annual fiscal processes which meet GAAP/GAAS requirements for statewide data network	• Identify costs of operation and sustainment • Identify more resources or efficiencies to ensure the budget aligns with the Board's goals • Each committee, at the direction of the Board, will submit priorities to the Finance Committee, making sure they align with the budget process, to decide whether it is within the budget • Compare last few years of expenditures to project the five-year plan and continue to revise it on an annual basis
Develop appropriate process and procedure for administering all financial assets consistent with national best practices in accounting and auditing	• Coordinate with other committees to identify their on-going financial needs • Procedure in place and working for budgeting, accounting, inventorying and auditing all financial assets of ISICSB whether state or grant funds.	• Develop annual fiscal process which meet GAAP/GAAS and GASB for administering state and federal funds consistent with Code of Iowa and grant guidelines • Align with the grant process developed by the ISICSB	• Compliance with state and grant policies • Ensuring records are available for audits/oversight

GOVERNANCE COMMITTEE			
Mission Statement: The Governance Committee develops and coordinates the policy and procedural operations of the ISICSB and ensures it functions within the law in a public and transparent manner.			
Goals	**Metrics for Success**	**Objectives**	**Action Plan**
Develop appropriate governance through creation of policy and procedure statements for enhancement, deployment and operation of ISICS	• Review ISICSB policies within 60 days	• Develop policies as requested • Disseminate policies as needed	• Actively communicate with other committee chairs • Identify the policies needed • Utilize an online project manager website to disseminate policies
Develop appropriate governance through creation of policy and procedure statements for enhancement, deployment and operation of a statewide broadband network	• Review ISICSB policies within 60 days	• Develop policies as requested • Disseminate policies as needed	• Actively communicate with other committee chairs • Identify the policies needed • Utilize an online project manager website to disseminate policies
Establish a process to administer grant funds or communications assets	• Process is adopted by ISICSB	• Develop policies as requested • Disseminate policies as needed	• Maintain knowledge of other states best practices and lessons learned while being mindful of the IA grant process • Work with and support the ISICSB and relevant committees • Develop a process for the planning, drafting, and execution of grants

OPERATIONS COMMITTEE			
Mission Statement: The Operations Committee collaborates and develops the operational protocols and procedures for interoperable communications.			
Goals	**Metrics for Success**	**Objectives**	**Action Plan**
At the end of five years 95% of all dispatch centers have access to ISICS	• The number of dispatch centers connected to ISICS	• Identify dispatch centers that need access • Establish operational policies for ISICS access • Deliver recommendation/documentation to ISICSB	• Define what access to ISICS means • Define what a dispatch center is • Determine roles and responsibilities of dispatch centers • Promote the goal to the dispatch centers • Request potential opportunities for funding dispatch centers from the Finance Committee • Work with the Outreach Committee to provide information on how PSAPs can join ISICS.
To review the ISICS draft policies and make recommendations to Standards Working Group	• Throughput. The number the ISICSB received from the committee vs the number delivered	• Review and document recommendations to the Standards Working Group representative	• Operations representative receives draft policies and then provides them to the Operations committee members for feedback • Collaborate with other committees and provide initial feedback during the drafting of policies prior to being submitted for review
Align and update legacy plans, including system failures	• Completion of plan	• Identify, review and update existing communications plans and include a system failure plan • Deliver recommendation/ documentation to ISICSB	• Compile copies of all known legacy communications plans • Develop rubric for assessment • Identify the lines of authority for the plans • Make recommendations to the entity that has authority of the plan • Incorporating the RPCs in the ISICSB structure • Make a recommendation to the Governance Committee for the realignment of the plans

OUTREACH COMMITTEE			
Mission Statement: The Outreach Committee builds coalitions to support and promote interoperable public safety and emergency communications by providing clear and pertinent information to stakeholders and decision makers.			
Goals	**Metrics for Success**	**Objectives**	**Action Plan**
To develop and deliver outreach materials for use in making decisions to become a user of ISICS (by final system acceptance) by June 2018	• Outreach materials developed for ISICS, then distributed and posted on the website, reviewed and updated by the end of the state fiscal year	• As needed, identify if a plan needs to be developed to respond to changes with ISICS • Develop outreach materials specific to elected officials and targeted audiences •	• Seek out feedback from various stakeholders and their respective agencies to determine if a plan needs to be developed • Identify key targeted audiences, tailor message for the specific groups • Monitor changes and progress and ensure our message is representative of the current status • Tailor messages specifically for state and local elected officials, boards and committees, containing statistics, cost-analysis, and benefits to public safety personnel.
To develop and deliver outreach materials for use in making decisions to become a user of broadband network by 90 days after adoption of the state plan or by Spring 2018.	• Outreach materials developed for broadband then distributed and posted on the website, reviewed and updated by the end of the calendar year	• Leverage guidance and input from the Broadband sub-committee • As needed, identify if a plan needs to be developed to respond to changes with broadband • Develop Iowa-specific materials from broadband providers • Develop outreach materials specific to elected officials and targeted audiences	• Establish a communications process between the Outreach Committee and other committees to obtain more information for distribution • Seek board approval for any materials to be developed identifying public safety broadband connectivity in the State of Iowa • Tailor messages specifically for state and local elected officials, boards and committees, containing statistics, cost-analysis, and benefits to public safety personnel. • Identify key legislators on funding committees and invite them to trainings and other communications-related events
Develop a plan for utilizing social media relative to ISICSB activities and interoperability issues	• Plan is developed and adopted • 25% increase in website/social media traffic, inquiries, and retweets/likes/shares every year for the next three years • Increase newsletter readership	• Adoption of social media plan • In five years, the ISICSB website or the SWIC becomes the primary and central point for information	• Determine which branches of social media to utilize, and which platforms to avoid • Research and develop a social media communications plan • Develop a strategy to elevate the ISICSB Website and the SWIC's office as a focal point for ISICS and interoperable communications information • Identify group leaders, agencies, organizations and vendors to create social media inter-linking (follows, likes, etc.)

OUTREACH COMMITTEE			
Goals	Metrics for Success	Objectives	Action Plan
Approach and educate elected officials	• Training program development complete • Number of engagement/participants involved in training program	• Develop a training plan • Engage association partners	• Tailor messages specifically for state and local elected officials, boards and committees, containing statistics, cost-analysis, and benefits to public safety personnel. • Identify key legislators on funding committees and invite them to trainings and other communications-related events

TECHNOLOGY COMMITTEE			
Mission Statement: The Technology Committee researches emerging technologies and standards to develop technical recommendations and procedures to enhance interoperable public safety and emergency communications.			
Goals	**Metrics for Success**	**Objectives**	**Action Plan**
To lead technological solutions for voice interoperability	• Publish state specific findings	• To develop standards for ISICS communications equipment • Create minimum standards for ISICS interoperable communications equipment	• Determining minimum and optimal ISICS system capabilities when it is fully built out • Develop the minimum standards for subscriber equipment to operate on system • Develop programming and configuration standards to include current and legacy technologies • Maintaining awareness of new and emerging communications technologies
To lead technological solutions for data interoperability	• Publish state specific findings	• Create minimum standards for interoperable communications equipment • Make recommendation to ISICSB to adopt standards	• Identify minimum and optimal broadband capabilities • Establish minimum technical rules for operational conduct • Develop a policy for bring your own device • Identify which devices public safety will use • Evaluating applications, data interoperability, and application interaction • Maintaining awareness of new and emerging data technologies and applications
Investigate voice and data convergence and differentiating the needs of public safety	• Publish staff studies on findings	• Investigate technology • Choose best course of action • Make recommendations	• Attend conferences • Keeping up on trade publications • Networking with others • Best practices • Increase information sharing efforts in simplified terms

TRAINING AND EXERCISE COMMITTEE			
Mission Statement: The Training and Exercise Committee provides training opportunities on interoperable communications and procedures for planned and unplanned events.			
Goals	**Metrics for Success**	**Objectives**	**Action Plan**
Develop and provide standard core training for interoperable communications across the various state regions	• Development of training materials • Number of people trained	• Establish guidelines defining standard core training • Embed communications training within existing state training institutions	• Define what standard core training courses would be • Develop lesson plans for those courses that do not already have them • Divide classes across the state for easier access
Expand the statewide core group of trainers who would be able to teach necessary COMU positions classes and increase COMU awareness	• Increase number of trainers so that at least two COML classes can be scheduled per year • Number of people trained •	• Create a COMU awareness outreach program for dissemination through the Outreach Committee • Seek Train-the-Trainer classes •	• Continue the partnership with OEC and increase regional Train-the-Trainer opportunities to increase cadre of instructors • Identify trainers in strategic regions throughout the state
Develop a cost analysis of training to augment future budgetary planning	• Delivery of a cost analysis document	• Obtain training funding	• Research and apply for grant opportunities • Reduce the cost of travel to attend trainings • Provide coverage of trainee backfill expenses for agencies
Increase the number of credentialed COMU personnel	• Increasing the number of people on the credentialing list	• Increased opportunities to complete position task book • Increase regional training opportunities	• Minimize the costs of the initial training • Increase the number of communications related full-scale and table top exercises/trainings • Covering the expenses of currently credentialed person to provide opportunities • Coordinate training with the Homeland Security and Emergency Management Department State Training Officer

USER GROUP COMMITTEE			
Mission Statement: The User Group Committee, comprised of authorized users, coordinates access and usage policies for use of or interfacing with the ISICS platform and public safety broadband systems.			
Goals	**Metrics for Success**	**Objectives**	**Action Plan**
Develop processes and vet the application process for access to the ISICS interoperable communications platform within state or grant resources.	• In five-ten years, 100% of eligible users have access to the ISICS platform • Decrease application process time relative to number of applications per user level	• Add efficiencies to application process • Determine resource needs for an objective evaluation of Level 3 and 4 resource users	• Create single point of coordination for all applications and necessary paperwork • Develop electronic repository for paperwork and workflow for all the paperwork • Identifying who has expertise for coverage needs for Level 3 and 4 users. System administrator • Revisit applicant review panel concept
Develop processes for guidance on broadband data interoperable communications platform within state or grant resources.	• Process developed • Number of users assisted, applied for and approved	• Identify and deploy process to assist in the application for broadband access	• Develop a process or certification for applicants for PSBN to confirm they are a true Public Safety entity (as needed) • Provide options of vendors and vendor information to applicants (as requested)
Strengthen all RICs	• Increase in RIC user attendance, participation, and investment	• Travel to every county to conduct outreach to all stakeholders • Listen and accept feedback • Identify meeting frequency and appropriate tasks	• SWIC to visit every county in State over the next two years to conduct outreach, assist with PSBN issues, and assess interest level in joining RICs • Identification of role and benefit of a strong RIC- possibly a white paper showcasing successes in Iowa • Encourage Outreach Committee to push out useful information to relevant associations • Encourage those involved in RIC to provide some reporting mechanism back to the full board • Create place where RICs can post information, ask questions, share resources. Establish RIC reporting process • Promote RIC as conduit for locals into ISICS board; a place for information to be exchanged between the board and the end users/local agencies

APPENDIX D: Code of Iowa

80.28 Statewide interoperable communications system board — established — members.

1. A statewide interoperable communications system board is established, under the joint purview of the department and the state department of transportation. The board shall develop, implement, and oversee policy, operations, and fiscal components of communications interoperability efforts at the state and local level, and coordinate with similar efforts at the federal level, with the ultimate objective of developing and overseeing the operation of a statewide integrated public safety communications interoperability system. For the purposes of this section and section 80.29, *"interoperability"* means the ability of public safety and public services personnel to communicate and to share data on an immediate basis, on demand, when needed, and when authorized.

2. The board shall consist of nineteen voting members, as follows:

a. The following members representing state agencies:

(1) One member representing the department of public safety.
(2) One member representing the state department of transportation.
(3) One member representing the department of homeland security and emergency management.
(4) One member representing the department of corrections.
(5) One member representing the department of natural resources.
(6) One member representing the Iowa department of public health.
(7) One member representing the office of the chief information officer created in section 8B.2.
(8) One member representing the Iowa law enforcement academy created in section 80B.4.

b. The governor shall solicit and consider recommendations from professional or volunteer organizations in appointing the following members:

(1) Two members who are representatives from municipal police departments.
(2) Two members who are representatives of sheriff's offices.
(3) Two members who are representatives from fire departments. One of the members shall be a volunteer fire fighter and the other member shall be a paid fire fighter.
(4) Two members who are law communication center managers employed by state or local government agencies.
(5) One member representing local emergency management coordinators.
(6) One member representing emergency medical service providers.
(7) One at-large member.

3. In addition to the voting members, the board membership shall include four members of the general assembly with one member designated by each of the following: the majority leader of the senate, the minority leader of the senate, the speaker of the House of Representatives, and the minority leader of the House of Representatives. A legislative member serves for a term as provided in section 69.16B in an ex officio, nonvoting capacity and is eligible for per diem and expenses as provided in section 2.10.

4. The voting members of the board shall be appointed in compliance with sections 69.16 and 69.16A. Members shall elect a chairperson and vice chairperson from the board membership, who shall serve two-year terms. The members appointed by the governor shall be appointed to three-year staggered terms and the terms shall commence and end as provided by section 69.19. If a vacancy occurs among the voting members, a successor shall be appointed to serve the unexpired term. A successor shall be appointed in the same manner and subject to the same qualifications as the original appointment to serve the unexpired term. The voting members of the board are entitled to receive reimbursement for actual expenses incurred while engaged in the performance of official duties from funds appropriated to the department of public safety and the state department of transportation for that

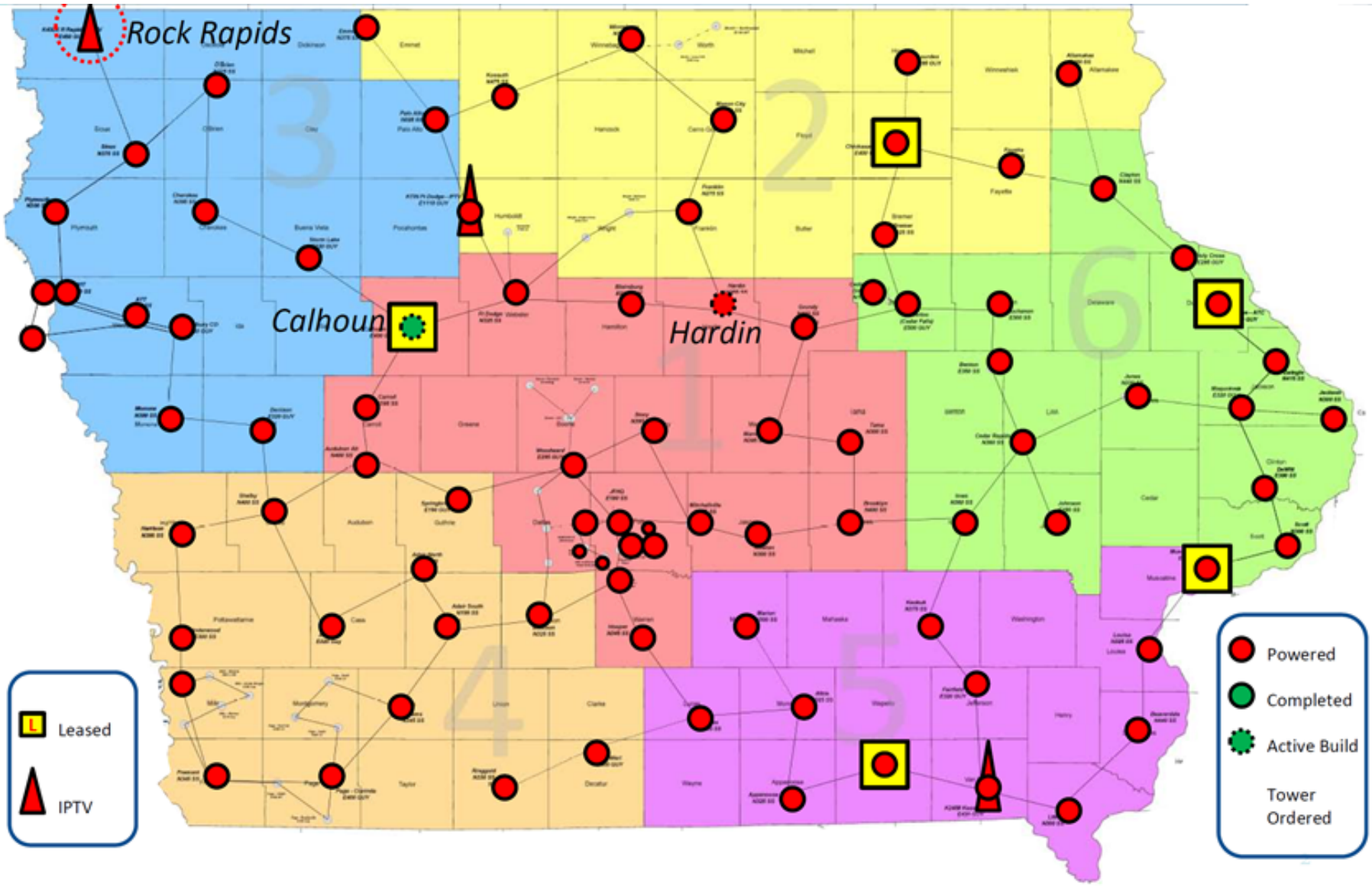
purpose. The departments shall enter into an agreement to provide administrative assistance and support to the board.

DEPARTMENT OF PUBLIC SAFETY, §80.29

80.29 Board duties.

The statewide interoperable communications system board established in section 80.28 shall:

1. Implement and maintain organizational and operational elements of the board, including staffing and program activity.
2. Review and monitor communications interoperability performance and service levels on behalf of agencies.
3. Establish, monitor, and maintain appropriate policies and protocols to ensure that interoperable communications systems function properly.
4. Allocate and oversee state appropriations or other funding received for interoperable communications.
5. Identify sources for ongoing, sustainable, longer-term funding for communications interoperability projects, including available and future assets that will leverage resources and provide incentives for communications interoperability participation, and develop and obtain adequate funding in accordance with a communications interoperability sustainability plan.
6. Develop and evaluate potential legislative solutions to address the funding and resource challenges of implementing statewide communications interoperability initiatives.
7. Develop a statewide integrated public safety communications interoperability system that allows for shared communications systems and costs, takes into account infrastructure needs and requirements, improves reliability, and addresses liability concerns of the shared network.
8. Investigate data and video interoperability systems.
9. Expand, maintain, and fund consistent, periodic training programs for current communications systems and for the statewide integrated public safety communications interoperability system as it is implemented.
10. Expand, maintain, and fund stakeholder education, public education, and public official education programs to demonstrate the value of short-term communications interoperability solutions, and to emphasize the importance of developing and funding long-term solutions, including implementation of the statewide integrated public safety communications interoperability system.
11. Identify, promote, and provide incentives for appropriate collaborations and partnerships among government entities, agencies, businesses, organizations, and associations, both public and private, relating to communications interoperability.
12. Provide incentives to support maintenance and expansion of regional efforts to promote implementation of the statewide integrated public safety communications interoperability system.
13. In performing its duties, consult with representatives of private businesses, organizations, and associations on technical matters relating to data, video, and communications interoperability; technological developments in private industry; and potential collaboration and partnership opportunities.
14. Submit a report by January 1, annually, to the members of the general assembly regarding communications interoperability efforts, activities, and effectiveness at the local and regional level, and shall include a status report regarding the development of a statewide integrated public safety communications interoperability system, and funding requirements relating thereto.



Attachment 2. Current status of the ISICS Platform buildout as of December 13, 2018. Red dots are sites that have been completed and are fully powered. The labeled sites are in varying stages of completion. Rock Rapids is an Iowa Public Television site that is being built. Calhoun is under active construction, and the Hardin site is undergoing some final civil work before it is considered fully completed and powered. Local county additions to ISICS (white dots) are not included in these status updates.

Attachment 3: List of agencies and counties that have joined ISICS for interoperability and/or operability as of December 13, 2018.

- 10th District Federal Reserve Law Enforcement
- 185th Iowa Air National Guard
- Adair Guthrie EMA
- Air Methods
- Boone County
- Buchanan County
- Buena Vista County
- Buena Vista EMA
- Carlisle Fire Department
- Carroll County
- Chickasaw County 911
- Chickasaw County EMA
- Crawford County
- Dallas County
- Delaware Township Fire Department
- Des Moines Police Department
- Department of Homeland Security Emergency Communications Division
- Dickinson County Emergency Management
- Drug Enforcement Administration
- Grundy County
- Hamilton County
- Harrison County
- Humboldt County
- Ida County
- Iowa Department of Natural Resources
- Iowa Department of Public Health
- Iowa Department of Public Safety
- Iowa Department of Transportation
- Iowa Department of Homeland Security and Emergency Mgmt.
- Jackson County EMA
- Jasper County
- Jewell Fire Rescue
- Johnson County JECC
- Kossuth County
- Linn County Sheriff's Office
- Madison County
- Mahaska County
- Marion County Sheriff
- Mercy Ambulance Des Moines
- MICRN
- Mills County
- Monona County
- Montgomery County EMA
- Muscatine County
- Northern Warren Fire
- Page County
- Shelby County
- Tipton Ambulance Service
- Urbandale Schools
- Union County LEC
- U.S. Marshal's Service
- Unity Point Des Moines
- University of Iowa Public Safety
- University of Northern Iowa
- U.S. Army Corps of Engineers Red Rock
- Van Buren County 911
- Virginia Township Fire Rescue
- Warren County
- Worth County
- Wright County

Attachment 4: Standards adopted in 2017:

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Talkgroup and Multigroup Ownership**		Date Created:		**02-01-18**	
Standard Policy #	**1.2.0**	**Section** Title**:**	**Interoperability Standards**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this standard is to define the ownership of private, shared, and interoperability talkgroups and multigroups. This provides standard, written documentation so subsystem administrators have firm guidelines as to who is permitted to have particular talkgroups and multigroups programmed into their radios.

2. Technical Background

Capabilities

Constraints

3. Operational Context

Private and shared talkgroups and multigroups are owned by the agency creating, or requesting the creation of, the talkgroup/multigroup. The process can be documented through a Memorandum of Understanding (MOU).

4. Recommended Protocol/ Standard

There are three tiers of talkgroups and multigroups that will be programmed into the system:

Private

These are defined as private talkgroups or multigroups owned by individual user agencies and used for normal day-to-day operations. They are not shared with any other agencies.

Private Talkgroups and multigroups are either "Listed" or "Unlisted". Only those private talkgroups/multigroups used for undercover operations or other highly sensitive confidential law enforcement activities may be "Unlisted."

The naming of private talkgroups will be in accordance with State Standard 3.2.0.

Shared
These are defined as private talkgroups and multigroups owned by individual user agencies, shared by mutual agreement. These will generally be used for routine or pre-planned activities between the sharing agencies.

The underlying principle of private and shared talkgroups and multigroups is that they are owned by a particular agency or group of agencies, and the talkgroup or multigroup will not be programmed into another agency's radios unless specifically authorized by the owner. Subsystem administrators shall not allow a talkgroup or multigroup to be programmed into a radio without such authorization.

Before a talkgroup or multigroup can be shared, the owning agency must pre-authorize the sharing arrangement through a MOU.

The naming of shared talkgroups will be in accordance with State Standard 3.2.0.

Interoperability
Interoperability talkgroups and multigroups are intended for interagency communications and assistance and fall into two categories: those used for 700 MHz communication only and those that are patched to conventional radio frequency (RF) resources.

These interoperability talkgroups and multigroups may be statewide or regional.

Statewide interoperability talkgroups and multigroups are not to be owned by any specific agency and will not require agency letters of authorization.

Regional interoperability talkgroups and multigroups are owned and managed by the ISICS Board. Regional interoperability resources will be prefixed with regional prefix (see State Standard 3.2.0).

The Iowa Statewide Interoperable Communications System Board will govern the standards for which radios may have regional interoperability talkgroups and multigroups, as well as standards regarding use of these resources.

5. Recommended Procedure

The procedure regarding pre-authorizing talkgroup sharing is defined in State Standard – Use of Shared Talkgroups.

6. Management

The Subsystem Administrators will be responsible to see that this policy is implemented as defined in the system standards manual. Identified issues and concerns will be brought to the System Administrator or the ISICSB.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Statewide Interoperable Plain Language Policy**		Date Created:		**03-27-2018**	
Standard Policy #	**1.3.0**	Section Title**:**	**Interoperability Standards**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**04/12/2018**	Reviewed:	**04/12/2018**

1. Purpose or Objective

Plain Language (clear speech) Compatibility:
The ability of emergency response personnel from different disciplines, jurisdictions, organizations, and agencies to work together depends greatly on their ability to communicate with each other. The use of plain language is about the ability of emergency response personnel to communicate clearly with one another and effectively coordinate activities, no matter the size, scope, location, or complexity of the incident.

The use of plain language (clear speech) in emergency management and incident response is a matter of public safety, especially the safety of emergency response personnel and those affected by the incident. It is critical that all those involved with an incident know and utilize commonly established operational structures, terminology, policies, and procedures. This will facilitate the achievement of interoperability across agencies / organizations, jurisdictions, and disciplines, which is exactly what the National Incident Management System (NIMS) and the Incident Command System (ICS) is seeking to achieve.

2. Technical Background

Capabilities

Integrated Communications
Incident communications are facilitated through the development and use of a common communications plan and interoperable communications processes and architectures. The ICS 205 Form is available to assist in developing a common communications plan. This integrated approach links operational and support units of agencies involved and is necessary to maintain communications and enable common situational awareness / interaction. Preparedness planning

should address the equipment, systems, and protocols necessary to achieve integrated voice and data incident management communications.

Constraints
N/A

3. Operational Context

Any communications between organizational elements during an incident should be in plain language in order to ensure that information dissemination is timely, clear, acknowledged, and understood by all intended recipients. Codes should not be used, and all communications should be confined to essential messages. The use of acronyms should be avoided during incidents requiring the participation of multiple agencies or organizations. Policies and procedures that foster compatibility should be defined to allow information sharing among all emergency response personnel and their affiliated organizations to the greatest extent possible.

Encryption or Tactical Language
When necessary, emergency response personnel and their affiliated organizations need to have a methodology and systems in place to encrypt information so that security can be maintained. Although plain language may be appropriate during response to most incidents, tactical language is occasionally warranted due to the nature of the incident (e.g., high-risk incident, such as active shooter.) The use of specialized encryption and tactical language should be incorporated into any comprehensive incident action plan (IAP) or incident management communications plan (IMCP).

4. Standardized Policy

The use of plain language is about the ability of area commanders, state and local Emergency Operations Center (EOC) personnel, federal operational coordinators, and responders to communicate clearly with each other and effectively coordinate response activities, no matter what the size, scope, or complexity of the incident. The ability of responders from different jurisdictions and disciplines to work together depends greatly on their ability to communicate with each other.

It is required that plain language be used for multi-agency, multi-jurisdictional, and multi-discipline events, such as major disasters and exercises. Beginning in the fiscal year that starts on Oct. 1, 2006, federal preparedness grant funding is contingent on the use of plain language in incidents requiring assistance from responders from other agencies, jurisdictions, and functional disciplines.

Primary Intended Use
Multi-agency or multi-jurisdictional emergency response or exercise.

Best Practices Encouraged
The use of plain language in emergency response is a matter of public safety, especially the safety of first responders and those affected by the incident. It is critical that all responders, including

those from other jurisdictions or states, as well as the federal government, know and utilize commonly operational structures, terminology, policies, and procedures.

Incident Scope and Geographic Area

Regional and statewide interoperability talkgroups are available for use everywhere the ISICS platform provides geographic coverage, regardless of incident size or scale. Interoperability incidents may be localized or dispersed in area. Participating personnel and resources may be local, regional, statewide, or national. Incidents may be pre-planned or emergent in nature.

5. Standardized Procedure

While the NIMS Integration Center does not require plain language for internal operations, it is strongly encouraged. It is important to practice every day terminology and procedures that will need to be used in emergency incidents and disasters. NIMS implementation is a long-term effort. Though it is not practical to expect a change of ingrained habits overnight, it is expected that over time, everyone will understand the importance of using plain language for day-to-day operations.

Unit Identification

When operating on the regional and statewide interoperability talkgroups, users should initially identify in the following manner using plain language: Agency name and service branch or function designation, followed by call sign or unit number. Examples: “North EMS 512”, “Elk River Police 512,” “Washington County Public Works 512,” “State Patrol 512,” etc. Once established, ongoing communications between the same units may be shortened.

Use of 10-Codes and Acronyms

The use of 10-codes, signals, unique acronyms, and other codes should not be used on the regional and statewide interoperability talkgroups because there is no standardized set of codes. Plain language should be used in all cases.

6. Management

N/A

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Statewide Pursuit Communications**		Date Created:		**4-18-2018**	
Standard Policy #	**1.4.0**	**Standard Title:**	**Interoperability Standards**		Status	**Approved**
Approval Authority:	**ISICSB**		Adopted:	**05-10-2018**	Reviewed:	**05-10-2018**

1. Purpose or Objective

The purpose of this standard is to establish the guidelines and procedures for vehicle pursuit communications.

2. Technical Background

Capabilities

The Iowa Statewide Interoperable Communications System Board (ISICSB) has established standards for use of the statewide interoperability talkgroups.

Constraints

Experience has shown that all agencies have used many different processes in the past. This standard strives for statewide consistency among all law enforcement agencies.

3. Operational Context

Pursuits are dynamic in nature and it is imperative to have a simplified communication strategy for mission success.

4. Recommended Protocol / Standard

All statewide interoperability talkgroups are required for public safety communication centers with full connectivity to ISICS, and statewide interoperability talkgroups are required for public safety communication centers using control stations to integrate with ISICS in a manner consistent with ISICSB policy.

5. Recommended Procedure

- Whenever a vehicle pursuit is initiated, the pursuing agency's current operating channel will be patched to the first available statewide TAC talk groups in the appended list, as determined by pursuing agency's dispatcher via the StatusBoard.
- The pursuing agency's dispatcher will perform the patch or multi-select function so all audio is heard on the talkgroups as needed.
- Further procedures will be outlined as needed.

6. Management

The ISICSB Training and Exercise Committee will ensure that a training module is created for this ISICS Standard.

Appended List of TAC talk groups for Pursuits

STATE / REGIONAL TG				
Phantom TGID	**Alias**	**Comment**	**Region**	**Talkgroup**
Statewide				
2	IATAC2	Iowa Statewide Tactical 2	Statewide	Tactical
3	IATAC3	Iowa Statewide Tactical 3	Statewide	Tactical
4	IATAC4	Iowa Statewide Tactical 4	Statewide	Tactical
5	IATAC5	Iowa Statewide Tactical 5	Statewide	Tactical
6	IATAC6	Iowa Statewide Tactical 6	Statewide	Tactical

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**ISICS Regional & Statewide Interoperability Talkgroups**		Date Created:		**04-17-2018**	
Standard Policy #	**1.5.0**	**Section Title:**	**Interoperability Standards**		Status	**Approved**
Approval Authority:	**ISICSB**		Adopted:	**05-10-2018**	Reviewed:	**05-10-2018**

1. Purpose or Objective

The purpose of this standard is to establish policy and procedures for use of ISICS regional and statewide interoperable talkgroups in all user radios. The regional and statewide interoperability talkgroups are a resource intended to facilitate communications among and between different agencies and service branches which need to coordinate their operations during major incidents, pre-planned events, and task force operations. These resources are not intended for localized day-to-day interoperability,

This policy will provide standardized incident response radio communications capabilities for all service branches and, most importantly, will support the redeployment of mutual aid resources throughout the state. This policy will provide the radio communications structure necessary to enable effective situational awareness, command and control, and resource coordination in support of the incident command and management structure specified under the National Incident Management System (NIMS). This policy will also serve to minimize usage conflicts when regional and statewide interoperability talkgroups are needed for multiple incidents.

2. Technical Background

Capabilities

ISICS regional and statewide interoperability talkgroups provides the highest level of interoperability for public safety and public service users respectively. Lower and less effective

levels of interoperability include switching to shared conventional frequencies, dispatch console patches, deployable portable gateways, and radio caches (swap radios).

Constraints
The availability of and the use of the regional and statewide interoperability talkgroups must be easily understood by radio user personnel, who are primarily concerned with their mission and not with the operation of complex radios under stressful conditions. Standardization of capabilities will provide responding agencies with an assurance that they will have operational compatibility with any other agency they need to work with.

3. Operational Context

Universal access to the six (6) non-encrypted talkgroups for each region and statewide zone by all end-users and communication centers. Encryption is supported by the ISICS platform, however, implementation and use is under consideration. Any future encryption on interoperable talkgroups will be Advanced Encryption Standard (AES) 256. APCO Project 25 (P25) 700 / 800 MHz AES 256 equipped radios and communication centers guarantees fully compatible, interoperable communications among agencies and service branches for major incidents, pre-planned events, and task force operations.

4. Standardized Policy

ISICS INTEROPERABILITY TALKGROUPS

Talkgroup Requirements	For Whom?
Required	All ISICS Users – All Radios – All communication centers (All regional and statewide interoperable talkgroups)
Recommended	N/A
Optional	Site Access - Sub Regional
Not Allowed	N/A
Site Access - Statewide	System Wide – All Sites
Site Access - Regional	Regional Sites + One

Cross Patch Standard	Approval Needed	To Talk Groups
Temporary Patch	No	As Needed
Permanent Patch	Yes	

Primary Intended Use
Regional and statewide interoperability talkgroups should be used as the primary resource for mutual aid incidents involving joint response from multiple agencies and/or service branches.

Incident Scope and Geographic Area

The regional and statewide interoperability talkgroups are available for use in incidents anywhere ISICS provides geographic coverage, regardless of incident size or scale. Interoperability incidents may be localized or dispersed in area. Participating incident personnel and resources may be localized, regional, statewide, or national. Incidents may be pre-planned or emergent in nature.

Non-intended Use

The statewide talkgroups are not to be used for daily routine operations.

Priorities for Use and Multiple Incidents

In the event that multiple interoperability incidents occur simultaneously, exhausting the regional and statewide interoperability talkgroups, assignment of regional and statewide interoperability talkgroups in incident radio communications plans will be prioritized for: (1) mutual aid incidents, and (2) those incidents involving resources spanning multiple regions. Secondary use and localized or single region mutual aid incidents initially assigned to statewide interoperability talkgroups should be reassigned to regional talkgroups. This reassignment will be coordinated between the affected incident commanders and dispatch centers controlling the incidents.

Console Resource Requirements and Patching

Integrated ISICS dispatch consoles shall have the regional and statewide interoperability talkgroups in the console configuration available for patching. Regional and statewide interoperability talkgroups should not be patched to other regional and statewide interoperability talkgroups. In order to meet the communications needs for an event, the regional and statewide interoperability talkgroups may be patched to:

- Conventional radio frequency (RF) resources, such as VHF, UHF, etc.
- Private agency talkgroups, such as dispatch mains, tactical talkgroups, pools, etc.
- Regional or local tactical talkgroups (TACs), although this would not be preferred as a method of resolving communications needs because it reduces the number of talkgroups available for an incident.

Assignment Tracking

Use of the NIMS/ ICS-205 Incident Radio Communications Plan format is highly recommended to assist with assignment tracking for pre-planned incidents, incidents utilizing more than one of the statewide talkgroups, and for incidents of long duration.

Multi-Group Prohibition

Regional and statewide interoperability talkgroups shall not be part of any announcement or other pre-programmed multi-group.

5. Standardized Procedure

Notification
If the StatusBoard is unavailable, contact a communication center with access to the StatusBoard to reserve a talkgroup.

Order of Use
The usage of regional and statewide interoperability talkgroups for Preplanned Non- Emergency interoperability events should use the highest numbered talkgroup and descend.

The usage of regional and statewide interoperability talkgroups for Unplanned Emergency Incidents use the lowest numbered talkgroup and ascend.

Training Exercises
Preplanned use of regional and statewide interoperability talkgroups for training should be encouraged.

Unit Identification
When operating on the regional and statewide interoperability talkgroups, users should initially identify in the following manner using plain English: agency name, followed by service branch or function designation, followed by call sign or unit number. Once established, ongoing communications between the same units may be shortened to agency name and unit number.

Use of 10-Codes and Acronyms
The use of 10-codes, signals, unique acronyms, and other codes should not be used on the regional and statewide interoperability talkgroups, because there is no standardized set of codes. Plain language should be used in all cases.

Termination of Use
At the end of the event, the initiating dispatch center will remove any patches that were placed for the event, if any, and clear the StatusBoard so other communications centers will know this resource is available for use.

6. Management

Communications Center Managers and Supervisors for agencies on the ISICS platform, Incident Commanders, and Communications Unit Leaders (COML) shall ensure that the policy and procedure for usage and assignment of the regional and statewide interoperability talkgroups is followed.

Communications center operators and Incident Command System (ICS) Communications Unit Leaders (COML) shall receive initial training and periodic refresher training on the use of this procedure.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Transport Interoperability**		Date Created:		**05-20-2018**	
Standard Policy #	**1.5.1**	**Section Title:**	**Interoperability Standards**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**8/9/18**	Reviewed	Approved

1. Purpose or Objective

The purpose of this standard is to establish the guidelines and procedures for communications needed during transport of including but not limited to prisoners, arrested individuals, medical and mental health patients.

2. Technical Background

Capabilities

The Iowa Statewide Interoperable Communications System Board (ISICSB) has established standards for use of the statewide interoperability talkgroups.

Constraints

Experience has shown that agencies have used many different processes in the past. Through best practices this standard strives for consistency among agencies that utilize ISICS.

3. Operational Context

Transport of prisoners, arrested individuals, medical and mental health patients present dynamic communications challenges for public safety agencies.

4. Recommended Protocol/ Standard

Minimum programming requirements as outlined in ISICS Standard 1.7.0 shall be followed by public safety communication centers and users with connectivity to ISICS.

5. Recommended Procedure

Public Safety Communications Center

- Public safety communications centers should announce any hazards for transport vehicles and traveling public safety and public service personnel via regional calling talkgroup listed in the appended State/Regional Call Talkgroup list.
- If check-ins are necessary for a high risk transport, a public safety communications center with Levels 2, 3 and 4 participation will have a single talkgroup that is allowed to roam statewide. Check-ins should be kept to a minimum to reduce system loading.

Transport Drivers

- If a transport driver encounters a reportable incident or requires assistance while in transit, the driver may call in the report on a geographically appropriate regional or statewide calling talkgroup listed in the appended State/Regional Call Talkgroup list.
- It is recommended that transport vehicles monitor the geographically appropriate regional or statewide calling talkgroup listed in the appended State/Regional Call Talkgroup list.

6. Management

The ISICSB Training and Exercise Committee will ensure that a training module is created for this ISICS Standard.

Appended List of Calling Talkgroups for Transports

STATE / REGIONAL CALL TALKGROUP			
Alias	**Comment**	**Region**	**Talkgroup**
IACALL1	Iowa Statewide Calling	Statewide	CALL
IACALL11	Iowa Region 1 Calling	Region 1	CALL
IACALL21	Iowa Region 2 Calling	Region 2	CALL
IACALL31	Iowa Region 3 Calling	Region 3	CALL
IACALL41	Iowa Region 4 Calling	Region 4	CALL
IACALL51	Iowa Region 5 Calling	Region 5	CALL
IACALL61	Iowa Region 6 Calling	Region 6	CALL

Appended List of TAC Talkgroups for Transports

STATE / REGIONAL TAC TALKGROUP			
Alias	**Comment**	**Region**	**Talkgroup**
IATAC2	Iowa Statewide TAC	Statewide	TAC
IATAC3	Iowa Statewide TAC	Statewide	TAC
IATAC4	Iowa Statewide TAC	Statewide	TAC
IATAC5	Iowa Statewide TAC	Statewide	TAC
IATAC6	Iowa Statewide TAC	Statewide	TAC
IATAC7E	Iowa Statewide TAC	Statewide	ETAC
IATAC8E	Iowa Statewide TAC	Statewide	ETAC
IATAC9E	Iowa Statewide TAC	Statewide	ETAC
IATAC12	Iowa Region 1 TAC	Region 1	TAC
IATAC13	Iowa Region 1 TAC	Region 1	TAC
IATAC14	Iowa Region 1 TAC	Region 1	TAC
IATAC15	Iowa Region 1 TAC	Region 1	TAC
IATAC16	Iowa Region 1 TAC	Region 1	TAC
IATAC17E	Iowa Region 1 TAC	Region 1	ETAC
IATAC18E	Iowa Region 1 TAC	Region 1	ETAC
IATAC19E	Iowa Region 1 TAC	Region 1	ETAC
IATAC22	Iowa Region 2 TAC	Region 2	TAC
IATAC23	Iowa Region 2 TAC	Region 2	TAC
IATAC24	Iowa Region 2 TAC	Region 2	TAC
IATAC25	Iowa Region 2 TAC	Region 2	TAC
IATAC26	Iowa Region 2 TAC	Region 2	TAC
IATAC27E	Iowa Region 2 TAC	Region 2	ETAC
IATAC28E	Iowa Region 2 TAC	Region 2	ETAC
IATAC29E	Iowa Region 2 TAC	Region 2	ETAC
IATAC32	Iowa Region 3 TAC	Region 3	TAC
IATAC33	Iowa Region 3 TAC	Region 3	TAC
IATAC34	Iowa Region 3 TAC	Region 3	TAC
IATAC35	Iowa Region 3 TAC	Region 3	TAC
IATAC36	Iowa Region 3 TAC	Region 3	TAC
IATAC37E	Iowa Region 3 TAC	Region 3	ETAC
IATAC38E	Iowa Region 3 TAC	Region 3	ETAC
IATAC39E	Iowa Region 3 TAC	Region 3	ETAC
IATAC42	Iowa Region 4 TAC	Region 4	TAC
IATAC43	Iowa Region 4 TAC	Region 4	TAC
IATAC44	Iowa Region 4 TAC	Region 4	TAC
IATAC45	Iowa Region 4 TAC	Region 4	TAC

STATE / REGIONAL TAC TALKGROUP			
Alias	**Comment**	**Region**	**Talkgroup**
IATAC46	Iowa Region 4 TAC	Region 4	TAC
IATAC47E	Iowa Region 4 TAC	Region 4	ETAC
IATAC48E	Iowa Region 4 TAC	Region 4	ETAC
IATAC49E	Iowa Region 4 TAC	Region 4	ETAC
IATAC52	Iowa Region 5 TAC	Region 5	TAC
IATAC53	Iowa Region 5 TAC	Region 5	TAC
IATAC54	Iowa Region 5 TAC	Region 5	TAC
IATAC55	Iowa Region 5 TAC	Region 5	TAC
IATAC56	Iowa Region 5 TAC	Region 5	TAC
IATAC57E	Iowa Region 5 TAC	Region 5	ETAC
IATAC58E	Iowa Region 5 TAC	Region 5	ETAC
IATAC59E	Iowa Region 5 TAC	Region 5	ETAC
IATAC62	Iowa Region 6 TAC	Region 5	TAC
IATAC63	Iowa Region 6 TAC	Region 6	TAC
IATAC64	Iowa Region 6 TAC	Region 6	TAC
IATAC65	Iowa Region 6 TAC	Region 6	TAC
IATAC66	Iowa Region 6 TAC	Region 6	TAC
IATAC67E	Iowa Region 6 TAC	Region 6	ETAC
IATAC68E	Iowa Region 6 TAC	Region 6	ETAC
IATAC69E	Iowa Region 6 TAC	Region 6	ETAC

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Use of Statewide and/or Regional Interoperability Talkgroups - Air Ambulance Emergency Landing Zone Coordination**		Date Created:		**07-04-2018**	
Standard Policy #	**1.5.2**	**Section Title:**	**Interoperability Standards**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**8/9/18**	Reviewed:	8/9/18

1. Purpose or Objective

The purpose of this standard is to specify the use of the ISICS statewide and regional interoperability talkgroups for establishing and maintaining air ambulance emergency landing zones.

2. Technical Background

Capabilities

The Iowa Statewide Interoperable Communications System Board (ISICSB) has established a standard for use of the ISICS statewide and regional interoperability talkgroups in ISICS Standard 1.5.0. This standard encourages interoperable communications among first responders and establishes common ISICS statewide and regional interoperability talkgroups to facilitate interoperability.

Constraints

Experience has shown that agencies have used many different processes in the past. Through best practices this standard strives for consistency among agencies that utilize ISICS.

3. Operational Context

Communications with aircraft on a trunked network can sometimes be problematic if the aircraft radio does not roam to an appropriate site or if there are other circumstances affecting air-to-

ground communication. This standard works to facilitate successful air-to-ground communications in emergency landing zones.

4. Recommended Protocol/ Standard

Coordination regarding talkgroup usage is vital to ensure successful communications. A public safety communication center, in-field public safety personnel or incident commander should be in contact with any aircraft and assign them an appropriate ISICS Regional or Statewide Interoperable talkgroup if possible.

If the aircraft does not have an ISICS connected radio, use of channels outlined in the ISICSB ICS-217A is recommended. Those channels can then be patched into ISICS statewide and/or regional talkgroups as needed.

5. Recommended Procedure

It is imperative to allow for communication between the responding aircraft and the designated person (law enforcement, fire personnel, first responder, etc.) on the ground that will be coordinating the landing zone (LZ) consistent with ICS structures. The exact location of the LZ, any hazards, wind direction, and any other pertinent information needs to be communicated to the aircraft to allow for a safe scene landing. If it becomes necessary to abort the landing, the individual on the ground will need to be able to quickly communicate this information to the aircraft.

For Aircraft that are equipped with ISICS radios:

If the aircraft and personnel on scene coordinating the landing both have ISICS statewide and regional interoperability talkgroups, they will use the ISICS statewide or regional interoperability that has been assigned to them by the appropriate, controlling public safety communication center, in-field public safety personnel or incident commander.

In the event of a technical constraint, the incident may be switched over to other talkgroups or channels as appropriate.

For Aircraft that are NOT equipped with ISICS radios:

If the aircraft does not have ISICS radios, but personnel on scene coordinating the landing do, the controlling, primary public safety communications center will assign an ISICS statewide and regional interoperability and patch the responding air ambulance operating to an appropriate channel outlined in the ISICSB ICS-217A. Note: Public safety communications centers will patch to conventional resources according to their local protocol.

Note: An announcement on the patched resources will be made at the time of the patch origin AND just prior to the patch removal.

Order of Use of ISICS statewide and regional interoperability Talkgroups (per ISICS Standard 1.5.0):

The use of ISICS statewide and regional interoperability talkgroups for PREPLANNED NON-EMERGENCY interoperability events involving LZ coordination should use the appropriate regional interoperability talkgroups in descending order, e.g. IA TAC 36, IA TAC 35, IA TAC 34 etc., in that order. For users who do not have the full complement of ISICS statewide and regional interoperability talkgroups programmed in their radios, these non-emergency LZ events should be assigned the "highest" number ISICS statewide and regional interoperability first.

The use of ISICS statewide and regional interoperability talkgroups for UNPLANNED EMERGENCY incidents involving LZ coordination should use the appropriate ISICS statewide and/or regional interoperability in ascending order, e.g. IA TAC 12, IA TAC 13, IA TAC 14, etc.

6. Management

Nothing in this standard shall be construed as a limitation of use of the ISICS statewide and regional interoperability talkgroups for incidents other than air ambulance emergency landing zone coordination.

Nothing in this standard shall be construed as a limitation of use of any appropriately assigned conventional resource for an air ambulance emergency landing zone coordination by non-ISICS users.

For Management, see ISICS Standard 1.5.0 (*ISICS Regional & Statewide Interoperability Talkgroups*) for additional information.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Minimum Programming Requirements**		Date Created:		**06-19-2018**	
Standard Policy #	**1.7.0**	**Section** Title**:**	**Interoperability Standards**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	**7/12/18**

1. Purpose or Objective

The purpose of this standard is to establish minimum programming requirements for subscriber radios and consoles.

2. Technical Background

Capabilities
The ISICS Platform provides regional and statewide resources for interoperable communications to occur should multiple events occur simultaneously.

Constraints
If programming of subscriber radios is not coordinated, situations may arise in which subscriber radios and consoles may not have the proper talkgroups or channels programmed to appropriately handle the event. For consoles and subscriber radios to be effective, programming must be consistent and follow proven guidelines.

3. Operational Context

Consistent programming will facilitate interoperable communications during the vast majority of scenarios.

4. Recommended Protocol/ Standard

Consoles:

- Communication centers with full connectivity to ISICS will program their regional talkgroups in addition to adjacent regional and the statewide interoperability talkgroups.

Control Stations:

- Communication centers using only control stations to connect to ISICS will at a minimum program their regional talkgroups and the statewide interoperability talkgroups.

Subscriber Radios:

- Subscriber radios connecting to ISICS will program all regional talkgroups and the statewide interoperability talkgroups.
- Subscriber radios connecting to ISICS will be programmed with all channels consistent with ISICSB ICS-217A.

System Administrator:

- The System Administrator or designee will ensure that seed code plugs are current for public safety and public service radio equipment.

5. Recommended Procedure

Upon successful application to the ISICS Platform, the user shall provide an advanced system key that will be provisioned by the System Administrator or designee. That system key shall include permissions for programming all statewide and regional interoperability talkgroups.

The System Administrator or designee will then ship the system key to the applying entity or the listed programming vendor. Tracking and delivery confirmation must be included in the shipping process.

Upon completion of programming of the entity's subscriber equipment and consoles, the entity or its designated programmer will notify the SWIC that programming has been completed and all regional and statewide interoperable talkgroups and channels listed on the ISICSB ICS-217A were programmed into the radios and consoles/control station/consolettes. The SWIC shall then notify the System Administrator and store the record in the appropriate repository.

6. Management

The System Administrator will maintain records of all system keys provisioned for entities consistent with current records retention policies.

The SWIC will ensure that verification of programming of regional and statewide interoperable talkgroups are recorded and maintained consistent with current records retention policies.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Event and Exercise Communications Planning**		Date Created:		**05-08-2018**	
Standard Policy #	**1.8.0**	**Section Title:**	**Interoperability Standards**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	7/12/18

1. Purpose or Objective

The purpose of this standard is to establish protocols and procedures to be used for planning communications for full-scale or functional exercises and pre-planned events that affect multiple agencies or jurisdictions.

2. Operational Background

Full-scale or functional exercises and pre-planned events that include multi-jurisdictional, multi-agency disciplines, and use of more than one statewide interoperability talkgroup require an All-Hazards, Type III Communications Unit Leader (COML) to establish a communication plan when possible. If no COML is available, the State System Administrator may approve a submitted plan.

A full-scale exercise (FSE) is a multi-agency, multi-jurisdictional, multi-discipline exercise involving a functional and "boots on the ground" response. A functional response could include a joint field office (JFO), emergency operations center (EOC), etc. A "boots on the ground" response could include firefighters or other first responders at a scene, along with mock victims, etc.

A functional exercise (FE) examines and/or validates the coordination, command, and control between various multi-agency coordination centers, such as an EOC, JFO, etc. A functional exercise does not involve any "boots on the ground" responders.
Refer to ISICSB Policy 2014-04 for State Credentialing as a Communications Unit Leader Type III, for more information about COML responsibilities

3. Operational Context

Event and Exercise Communications Planning
State Standard 1.8.0
ISICSB Approval: 7/12/18

Full-scale or functional exercises and pre-planned events of any size can include complex communications issues. There is also a potential for any event to grow quickly into a large-scale incident.

Since full-scale/functional exercises and pre-planned events have the potential to affect system capacity, a COML and/or State System Administrator should ensure that the event does not inadvertently affect normal, daily operational needs by negatively impacting the availability of ISICS platform resources.

4. Recommended Procedure

When an entity develops a plan for a full-scale/functional exercise or pre-planned event that involves the use of ISICS resources, these procedures will be followed:

- The StatusBoard calendar schedule feature must be utilized. When the exercise or event is planned farther out that seven days, the requested resource will be reserved on the StatusBoard at least one week in advance.
- Exercise or event planners may include the local city or county radio system manager in the exercise development process from the beginning so local system resources are properly utilized.
- During full-scale/functional exercises or pre-planned events using more than one statewide interoperability talkgroup, planners may utilize the services of an Iowa credentialed COML when possible. If no COML is available, the State System Administrator may approve a submitted plan.
- An ICS 205 Communication Plan must be completed. The completed ICS 205 will be provided to event participants and the local radio system manager.
- When more than one statewide interoperability talkgroup is used, the ICS 205 must be sent to the State System Administrator so the Department of Public Safety (DPS) Interoperability Communications Bureau can distribute it to the entire state. This standard does not apply to 205's using regional talkgroups.
- If modifications to a communications plan need to be implemented during an exercise, the incident commander (IC), COML or appropriate individual may coordinate with the State System Administrator to ensure that needed resources are available.

If the event or exercise planner does not have access to a COML, they can contact the SWIC or designee for assistance with locating and providing COML services. The State Duty Officer can also be used as a resource for contacting a COML.

5. Management

The sub-system administrators and users will all be responsible to see that this policy is implemented as defined. Identified issues and concerns will be brought to the Operations Committee for resolution. Maintenance of this standard will be the responsibility of the SWIC.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Cross Spectrum Interoperability**		Date Created:		**06-13-2018**	
Standard Policy #	**1.10.0**	**Section Title:**	**Interoperability Standards**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**8/9/18**	Reviewed	8/9/18

1. Purpose or Objective

The purpose of this standard is to establish procedures for use and patching of VHF/UHF/700/800 (V/U/7/8) MHz interoperability resources. Conventional resources (CR) include local operability resources and interoperability channels in this standard.

2. Technical Background

Capabilities

Conventional resources may include:

- Nonfederal national V/U/7/8 interoperability channels.
  - These are derived from FCC rules, ANSI standards and NTIA rules. These channels can be found in the NIFOG.
- Statewide V/U/7/8 interoperability channels.
  - LEA, Iowa Channel, Point-to-Point and other interoperability channels that are unique to Iowa.
  - Local V/U/7/8 interoperability channels.

Constraints

- Conventional radio users should have the capability to communicate on conventional V/U/7/8 radio channels—e.g., VCALL10, VLAW31, 8CALL90 or 8TAC91—as long as they are approved to transmit on those channels.
- An ISICS talkgroup should only be in one patch at a time.
- A patch between an ISICS talkgroup and a CR will result in the CR being able to reach ISICS users. However, users should not expect the footprint of the CR to expand.

- The coverage area when patching a simplex channel (e.g. VLAW31, UTAC42D, 7TAC52D, 8TAC92D) will have limited range when compared to a repeated conventional channel. Users of simplex channels and ISICS talkgroups may have to accept interference from other users on that simplex channel that are within range of their radios.

3. Operational Context

These communications pathways may be used for day-to-day coordination, urgent or emergency mutual aid situations, task forces, tactical teams, and for other purposes. While existing conventional subscriber radios can be used, additional equipment may be required for patches.

Patches between CR national interoperability resources, legacy state resources and the corresponding ISICS regional and statewide interoperability talkgroups should only be used when there is a need for communications between personnel that are on conventional radios and personnel that are users of the ISICS Platform. Use must be in compliance with the rules governing the selected frequency on the national mutual aid resource and be authorized by dispatch, the Incident Command (IC) or Unified Command (UC) structure at the scene of the incident or planned event.

A CR national interoperability resource and an associated patched ISICS talkgroup may be used for short-term high intensity events and for long-term extraordinary events.

4. Recommended Protocol/ Standard

Patches are generally allowed between ISICS talkgroups and CR. A soft patch is typically an ad-hoc patch done through a console that is temporary. A hard patch is typically fixed through hardware and is typically intended to be perpetual. Hard patches are discouraged for interoperability talk groups. Audio gateway devices will pass audio from the CR to ISICS talkgroups and vise-versa and may be field deployed or in a public safety communications center. There may be instances where a hard patch is necessary on a local level. The System Administrator should be consulted before any hard patches are created.

5. Recommended Procedure

The national interoperability resources and legacy state resources primarily provide interoperability for a conventional or disparate radio system user that cannot access ISICS trunked system resources. Conventional radio users may be moved onto a separate radio channel for a specific incident.

Once an incident using an ISICS regional or statewide interoperability talkgroup or conventional interoperability channel ends, the local dispatcher should also release this resource on the ISICS StatusBoard Application if available.

6. Management

The development and management of statewide rules for use of statewide interoperability channels are the responsibility of the Iowa Statewide Interoperable Communications System Board (ISICSB).

The System Administrator working with the ISICSB is responsible for managing this standard.

The agencies on the ISICS Platform and CR shall ensure that there is a procedure for use of a patch between CR and the ISICS regional and/or statewide interoperable talkgroups or local resource in the dispatch center for which they are responsible.

System users should receive initial and continuing training on the use of this procedure as part of their regular or routine training.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Use of 700/800 MHz Scene of Action (SOA) Channels**		Date Created:		**07-05-2018**	
Standard Policy #	**1.11.0**	**Section Title:**	**Interoperability Standards**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**10/11/18**	Reviewed:	10/11/18

1. Purpose or Objective

The purpose of this standard is to provide standards, protocols, procedures, and operating parameters for short range simplex Scene of Action (SOA) channels.

2. Technical Background

Capabilities

- SOA channels allow the ability to communicate radio-to-radio without using system resources.
- There are three statewide analog 800 MHz SOA channels.
- There are three statewide P25 700 MHz SOA channels.

Constraints

- The public safety/service interest is best served by creating an operating procedure that maintains safety of personnel in situations. The limitation of this resource due to the range of mobiles and the potential "walk over" issue is a critical point. Once a radio is keyed, there is no way to control the footprint of the transmission other than limiting the power of that transmission. Personnel talking on a mobile radio may have no way of knowing if they are walking over a portable in the next community, because they will not be able to receive it or realize that the channel is in use by the portable.
- The 700/800 MHz SOA channels are only licensed for use within Iowa.
- Portable units will have limited range of operation, depending on the situation and conditions, while mobile units will have a greater range but may cause inadvertent interference to SOA portable users in adjacent areas.

- SOA channels included in a multi-mode (trunked and conventional) scan list of a radio unit will not allow that unit to priority scan. SOA channels may be included in scan lists. However, personnel will need to be aware that if the SOA channel is included in the scan list, the radio could lose the priority revert feature. If they are scanning, they may miss important radio traffic even on the channel selected.
- Since these SOA channels are not licensed for base station use, dispatch centers are not authorized to transmit on or patch the SOA channels into other resources using fixed stations.
- Dispatch centers normally will not be able to monitor SOA channels due to the limited range of these channels.
- 700 MHz SOA channels licensed to the State of Iowa are limited to 2 Watts Effective Radiated Power (ERP) per Federal Communications Commission (FCC) Rule 90.531 (portables or mobiles programmed to low power.)
- CAUTION: If radios are incorrectly programmed, it is possible for radio units to inadvertently walk over or interfere with other radio units in close proximity to one another, endangering personnel operating on emergency scenes.

3. Operational Context

The three general purpose 800 SOAs and three 700 SOAs shall be designated for use on scene by the incident commander or controlling public safety communications center. Units requiring use of a SOA channel shall verify that the channel is available via on-air announcement before use.

4. Recommended Protocol/ Standard

Names and uses of the SOA channels shall be as indicated in the table below:

Name	Eligibility	Which Radios	Recommendation Level	Encryption
7ITALK1D	Public Safety*	2 Watt ERP Max	Required in all mobiles and portables	Clear Only
7ITALK2D	Public Safety*	2 Watt ERP Max	Required in all mobiles and portables	Clear Only
7ITALK3D	Public Safety*	2 Watt ERP Max	Required in all mobiles and portables	Clear Only
8ITALK1D	Public Safety*	All Radios	Required in all mobiles and portables	Clear Only
8ITALK2D	Public Safety*	All Radios	Required in all mobiles and portables	Clear Only
8ITALK3D	Public Safety*	All Radios	Required in all mobiles and portables	Clear Only

*These frequencies are licensed by ISICSB and authorizes any public safety agency possessing a FCC part 90 license.

All parameters on the ICS-217A shall be followed.

Elevated external or gain antennas connected to portable or mobile radios for portable radios may be allowed on the 700/800 MHz SOA channels, but a communications technician should be consulted prior to utilizing an elevated antenna.

5. Recommended Procedure

Unit-to-unit communications using the SOAs is initiated when necessary or during an event or incident when assigned by an incident commander. The dispatch centers will normally not be able to monitor each SOA channel to assign them for use. On scene units requiring the use of an

SOA channel should announce their intent to use the channel. SOA channel location on portable radios will be set by Sub-system administrators in their fleetmaps.

6. Management

Sub-System Administrators will be responsible for ensuring compliance with this standard.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Operational Management**		Date Created:		**12-14-2017**	
Standard Policy #	**2.4.0**	**Standard Title:**	**Management of System**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this standard is to define agency roles in the operational management of the ISICS platform.

2. Technical Background

Capabilities

Subsystem owner applies to level 3 and 4 Iowa Statewide Interoperable Communications System (ISICS) user.

Constraints

3. Operational Context

Each subsystem owner and/or interconnected dispatch system owner will formally designate a Subsystem Administrator. This Administrator will have the authority to represent their respective agency/agencies' interests and make decisions on issues related to the day-to-day operation of the system and any urgent or emergency system operational or repair decisions. The Statewide System Administrator will represent the state-owned portion of the system. Each Subsystem Administrator shall designate a backup, who will have the authority to represent their respective Subsystem in the absence of the primary System Administrator.

An urgent or emergency situation would be where immediate decision authority is needed to allow the system as a whole, or any of the subsystem components, to continue supporting normal wide-area communications services. It is recognized that each System Administrator may have to

obtain authorizations from higher levels of their own organization to make longer-term or non-emergency capital or repair expenditure decisions.

Each Subsystem Administrator will be responsible for the day-to-day management, operation, and oversight of the subsystem components within their portion of the system. While specific duties will not be detailed in this document, the general duties will include:

- Monitoring the subsystem and its components for normal operations.
- Participating in the diagnosis of subsystem performance problems and the development of corrective action recommendations.
- Dispatching appropriate repair services in the event of a malfunction in subsystem equipment.
- Managing the database elements, including subscriber ID's, talkgroup ID's, console ID's, and the various parameters that relate to their effective operation.

Due to the complexity and distributed administration and maintenance of the system, problems can appear when changes are made to hardware or software. In order to keep all representatives informed of any updates, notifications will need to be sent to all primary and alternate Subsystem Administrator representatives in the event of any of the following:

- Any planned maintenance work being done on the regional or subsystem systems that would affect the system performance for other representatives should be preceded with reasonable notification of the maintenance work being done.
- Any equipment malfunctions, software malfunctions, early symptoms of malware/virus/intrusions or other failures that would affect system performance for other representatives of the subsystems or regional system.
- Any configuration changes in equipment or software by any one of the representatives that may affect system performance for the other representatives.

In addition to the responsibilities as a Subsystem Administrator, the ISICS System Administrator will also be responsible for:

- System Administrator meetings, periodically, to review operations of the system and share ideas or issues with their respective subsystems that may be of interest to the other System Administrators.
- Being available to work with any other System Administrators or technical staff of any of the subsystems to diagnose and resolve system operational problems that involve parameter changes, maintenance, or repair of equipment.

- Being the identified point of contact with "contracted vendor(s)" for issues related to the network equipment.

- Providing timely information to other System Administrators about system equipment repair or maintenance issues.

- Monitoring the performance of the entire network for normal operations, particularly the performance of the equipment.

- Monitoring the configuration of the system database for normal operations, particularly the properties of the equipment and database objects, in addition to conducting periodic database backups.

4. Recommended Protocol/ Standard

This is an ongoing process for the management of the system.

5. Recommended Procedure

If specific procedures for performing these functions are not defined in other State Standards, they are at the discretion of the Operations Committee with User Group Committee (UGC) input/feedback.

The noted designees in this document will be queried annually or if there is a change.

6. Management

The ISICS System Administrator or their designee is responsible for the operational management of the system.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Network Management**		Date Created:		**12-14-2017**	
Standard Policy #	**2.5.0**	**Standard Title:**	**Management of System**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this standard is to define the responsibilities for Network Management. The network is composed of, but not limited to switches, routers, servers, local area networks at the equipment locations, and wide area links connecting sites together consisting of the microwave and fiber optic equipment, and the network management tools provided by the equipment manufacturer.

2. Technical Background

Capabilities

The system architecture is primarily constructed around an internet protocol (IP) based network.

The network is composed of industry standard equipment, which also provides flexibility and a large variety of management and diagnostic tools.

Motorola Solutions will provide equipment configuration information as part of the system documentation.

Constraints

The system network is complex, and unusual problems may be difficult to identify and resolve. The system documentation will have to be kept up-to-date to maintain its value in supporting the system network.

The system network is protected from other agency data networks, and shall remain so, to protect the security and functionality of the system. If there is a connection to another data network, it shall be through an appropriately designed and maintained firewall.

3. Operational Context

The components of the network shall be considered "owned" by one of the appropriate owners of the subsystem. The individual owners will then be responsible for the maintenance of the sites (per memorandum of agreement (MOA)) and equipment they own. Agreements between the owners and/or maintenance contractors are at each agency's discretion, but the owner is still ultimately responsible for their portion of the subsystem.

The system is structured on the integrated network; any infrastructure hardware and software upgrades or changes that may impact the system network will need prior Iowa Statewide Interoperable Communications System Board (ISICSB) approval. The request submitted for approval by the Operations Committee with User Group Committee (UGC) input/feedback.

All maintenance work being scheduled that may affect the system and/or subsystem's performance shall be preceded by reasonable and appropriate notification to the other System Administrators and Subsystem Administrators.

The equipment configurations of the network components will need to be documented. This is primarily for the purpose of maintenance but also affects future planning. Motorola Solutions will provide the original as-built documentation.

The other defined standards for maintenance, documentation, notification, changes, security, and training also pertain to the network portion of the system.

4. Recommended Protocol/ Standard

This will be an ongoing task in the operation and management of the system.

5. Recommended Procedure

The methods for performing detailed network operations are defined in the technical resource manuals and training for the system. The technical resource manuals are classified as "Security Information" and "General Non-Public Data", pursuant to Iowa Code section 22.7(50) and Iowa Administrative Code 661-80.13(22.5).

Details on procedures not otherwise defined are at the discretion of the ISICSB and will be recommended by the Operations Committee who will define the flow and input of information by other committees.

6. Management

The System and Subsystem Administrators are responsible for managing and maintaining their agency's data attributes. The Statewide System Administrator shall be responsible for the statewide portion of the network.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Database Management**		Date Created:		**12-14-2017**	
Standard Policy #	**2.6.0**	**Standard Title:**	**Management of System**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this standard is to define the responsibilities for managing the system database by the ISICS System Administrator or designee.

The database contains objects for the system and subsystems defining the operational characteristics "personality" such as but not limited to:

- Subscriber radios
- Talk groups and multi-groups
- Profiles for radio users and talk groups
- Storm plans
- System and subsystem equipment operational parameters
- Security group structures
- Login user accounts and privileges

2. Technical Background

Capabilities

The system and subsystems contain a central database; however, the management of the database can be distributed among the agencies/staff responsible for the various aspects of the data in the database.

Constraints

The database contains the operational personality of the entire system. Because of this critical function, the data must be properly managed for system functionality and archived in case of data loss or corruption.

3. Operational Context

The system database will be partitioned to facilitate the distributed management of the data contained in the database; each Subsystem Administrator shall manage the portions of the above-listed data they are responsible for. Subsystem Administrators may, at their discretion, make mutual arrangements with other Subsystem Administrators for the management of their data.

Individual agencies will be responsible for maintaining and archiving their own radio codeplug data as defined by the agency's internal procedures.

The ISICS System Administrator, at a minimum of every other week, will back up the system database. Additional backups may be requested by Subsystem Administrators if large volumes of data have been entered or changed.

Multiple revisions of backups will be dated and kept in a rotating stock so a restore would be possible from an earlier backup if the need arises. Multiple database backups will be made and kept on-site at the backup location. Database backups will also be kept off-site in the event of a building disaster.

Database restores will only be done by the ISICS System Administrator and only in the event of one of the following: system software reloading and version changes, system database corruption, or as defined in the "Disaster Recovery" section of the ISICS Standards Manual.

Database restores may also be performed where there is a need, in a non-critical condition, if there is a reasonable consensus from the appropriate Subsystem Administrator(s).

ISICS System Administrators and Subsystem Administrators shall notify other Subsystem Administrators of any database issues they encounter that may adversely impact them.

4. Recommended Protocol/ Standard

This will be an ongoing task in the operation and management of the system.

5. Recommended Procedure

The methods for performing detailed database management are defined in the technical resource manuals and training for the system. The technical resource manuals are classified as "Security Information" and "General Non-Public Data", pursuant to Iowa Code section 22.7(50) and Iowa Administrative Code 661-80.13(22)

Details on procedures not otherwise defined are at the discretion of the ISICSB and will be recommended by the Operations Committee who will define the flow and input of information by other committees.

6. Management

The ISICS System and Subsystem Administrators are responsible for managing and maintaining their agency's data attributes. The ISICS System Administrator shall be responsible for the statewide portion of the network.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Training Radio Telecommunicators**		Date Created:		**02-01-2018**	
Standard Policy #	**2.7.0**	Standard Title:	**Management of System**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this standard is to establish the minimum training standards for all radio Telecommunicators. This will ensure that system dispatch operations, as they apply to each agency, are performed by properly and consistently trained dispatch personnel.

Radio Telecommunicator is defined as those individuals whose sole or primary job responsibility is utilizing either ISICS or interoperability radio equipment in the capacity of a public safety dispatcher.

2. Technical Background

Capabilities

Constraints

3. Operational Context

System functionality and integrity must be maintained by ensuring that properly trained personnel perform dispatch functions.

4. Recommended Protocol/ Standard

Each agency operating on the ISICS System is responsible for the training of their personnel and compliance with State, Regional, and Local Operating Standards.

Dispatch personnel shall successfully complete, at a minimum, training on the console or interoperability equipment installed by the user agency, as well as each topic listed below.

The following topics will be the minimum required training for Radio Telecommunicators at the User Levels 1 and 2 of the ISICS System in the state of Iowa. This level of detail on each topic is to be considered an awareness level of training.

- Console fleetmaps
- Unit numbering convention
- Cross band repeaters, if applicable
- Emergency button operation
- Encryption
- Incident Command System (ICS) form 205
- Talkgroup priority levels
- Iowa Public Safety VHF Interoperability Frequency Plan
- Use of gateway equipment as it relates to establishing interoperability between disparate radio systems
- NIMS ICS training
- Radio Alias
- Scene-of-Action (SOA) channels
- Talkgroup assignments
- Interoperability
- Talkgroup naming process

The following topics will be the minimum required training for Radio Telecommunicators at the User Levels 3 and 4 of the ISICS System in the state of Iowa. This level of detail on each topic is to be considered an enhanced level of training.

All training requirements at the User Levels 1 and 2 in addition to the following requirements:

- Paging procedures
- Agency backup radio plan
- Alert tone
- Elevating talkgroup priority
- Emergency button operation
- Failsoft
- Fleetmaps of dependent agency or agencies (as it affects interoperability within and outside agency's jurisdiction)
- Interagency hailing talkgroups
- Management of talkgroups
- Dispatcher's role in selection of talkgroups
- Dispatcher's role in directing responders to talkgroups
- Multi-select

- Patching
- Site trunking - agency operation
- Talkgroup affiliation

In addition to the above topics, the following state standards are required for dispatcher training that cover the following topics:

- 700/800 MHz Statewide STAC Interoperability Talkgroups
- Use of Statewide 700/800 MHz STAC 1-12 Talkgroups – Air Ambulance Emergency Landing Zone Coordination
- Event and Exercise Communications Planning
- Statewide Pursuit Communications
- National Weather Service ISICS Radio Operations

Training may involve interactive scenarios, whether tabletop or software simulation. Scenarios should include Local Interoperability, County Interoperability, Regional Interoperability, Statewide Interoperability, National Interoperability Channels, and ISICS to non-ISICS Interoperability.

Each agency is responsible to communicate policy changes to their Radio Telecommunicators as they occur.

Each agency shall be responsible for maintaining adequate records documenting compliance with the provisions of this standard. These records will include the following information:

- End user roster
- Training syllabus
- Online certification - optional

It is highly recommended that agencies keep accurate and complete records, which will be produced at the request of the local system administrator within a reasonable amount of time.

Refresher Training

Radio Telecommunicators shall receive refresher training every two years, at a minimum, or any time there is a significant change to procedure or equipment being used. Refresher training shall ensure competency of all skills taught in initial training and should specifically include skills that are infrequently used.

5. Recommended Procedure

It is highly recommended that all Radio Telecommunicators read and familiarize themselves with the Telecommunicators Best Practice Guide and all applicable State Standards as part of their training.

For Radio Telecommunicators in agencies migrating to ISICS or implementing interoperability measures with ISICS users from other systems, training for agency- specific dispatch consoles, if applicable, is required prior to completing field training and operating independently.

6. Management

Dispatch agency management will be responsible to ensure that:

- Radio Telecommunicators have received all necessary training.
- Only qualified personnel perform dispatch functions.
- Radio Telecommunicators are familiar with all applicable sections of the ISICS State Standards.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Requesting Access and Participation Plan Revisions**		Date Created:		**03-27-2018**	
Standard Policy #	**2.8.0**	Section Title**:**	**Management of System**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**4/12/2018**	Reviewed:	**4/12/2018**

1. Purpose or Objective

The purpose of this standard is to establish the procedure for an eligible entity to apply for participation in the Iowa Statewide Interoperable Communications System (ISICS) and for a participant to request changes to their participation plan.

2. Technical Background

The following definitions apply to this standard:

- "Requesting entity" means an entity that wishes to gain access to the ISICS platform for voice communication purposes. Entities that are not eligible ISICS participants may not apply for access. Each entity solely applies for itself unless accompanying authorization documentation from sub applicants is submitted with the application.
- "Level 1 users" means interoperability use only.
- "Level 2 users" means local operational use with no enhancements.
- "Level 3 users" means local operational use with additional channel capacity.
- "Level 4 users" means local operational use with additional channel capacity and local coverage enhancements.

3. Operational Context

Since changes to ISICS may affect other participants, the addition of new participants must be reviewed for possible performance or cost impacts to some or all users of the system prior to implementation. The access plan provides the information needed to evaluate system impacts of taking on the new participant and ensures that new users will have sufficient training and procedures in place to properly use the shared system and interoperate with other users.

Similarly, whenever existing participants change the nature of their use of the system, those changes need to be documented in a participation plan amendment and evaluated for system impacts prior to implementing those changes.

Only those issues that affect the operation of ISICS are governed by this ISICS Standard. Changes that affect only local resources may be managed at the local or regional level.

The ISICS platform is designed with a certain amount of capacity in anticipation of the addition of future participants joining the system. However, if a participation plan requires the addition of new ISICS resources or triggers a major technical change, the technical change management procedures of Change Management Standard may also apply.

4. Recommended Protocol/ Standard

All participants accessing the ISICS platform must have a current, approved access plan or be included in the approved access plan of another entity.

5. Recommended Procedure

A. Plan Contents

a. When an entity elects to become a participant, it shall submit a Letter of Intent (LOI), Memorandum of Agreement (MOA) and Participation Plan to ISICSB.

B. Interoperability Participation

a. When an entity elects to become an Interoperability Participant, Participation Plans should contain the following information:
   i. The type and quantity of equipment
   ii. Whether the agency has Public Safety Answering Point (PSAP) equipment capable of accessing ISICS
   iii. A narrative description of the entity's intended use
   iv. A list of public safety agencies that the entity would anticipate communicating with over ISICS

b. The requesting entity may be granted access to these talkgroups:
   i. Statewide interoperability talkgroups
   ii. Regional interoperability talkgroups
   iii. Statewide system patches to Legacy communication systems
   iv. Other talkgroups whose owners have granted permission to the requesting entity

C. Plan Review

a. The User Group Committee (UGC) may determine whether the requesting entity's plan is consistent with regional and statewide plans. The UGC may resolve inconsistencies by seeking adjustments to the requesting entity's proposal. The UGC may not recommend the approval of plans where there is an inconsistency between regional and statewide plans and the requesting entity's plan. Once the requesting entity's plan is found to be consistent with regional and statewide plans, the UGC may recommend approval and submit it for approval to ISICSB.

b. ISICSB will review the requesting entity's plan to ensure these requirements are met:
    i. The plan accurately reflects any impacts on ISICS that would result from its implementation.
    ii. The plan is consistent with the capacity and operational constraints of the ISICS platform.
    iii. The plan is consistent with the currently adopted plan and standards of the ISICSB.
c. If ISICSB determines that the requirements are met, they may approve the applicant for access to ISICS.
d. If ISICSB determines that the requesting entity's plan does not meet these requirements, they shall communicate their objection of the plan to the requesting entity. The requesting entity may then revise and resubmit their plan. The UGC shall review the plan and load assessment and make a recommendation to the ISICSB, who shall have final authority over acceptance of the plan. Appeals of UGC decisions may be brought to ISICSB.
e. The requesting entity gains access to the system when their request for participation is approved and the entity has received a welcome letter from ISICSB.

D. Participation Plan Amendments

a. If a participant desires to make changes to their approved plan, the plan amendment shall be submitted for approval following the same procedure as for the initial approval of a plan. If the UGC determines that the plan amendment does not impact the ISICS platform, the UGC may recommend approval of the amendment to ISICSB.

6. Management

The Governance Committee is responsible for the management of this standard. ISICSB staff shall maintain a record of approved and amended local participation plan.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Requesting Participation by Non- Public Safety/Non-Public Service Organizations**		Date Created:		**04-17-2018**	
Standard Policy #	**2.9.0**	**Standard Title:**	**Management of System**		Status	**Approved**
Approval Authority:	**ISICSB**		Adopted:	**05-10-2018**	Reviewed:	**05-10-2018**

1. Purpose or Objective

The purpose of this standard is to establish a policy that will provide for non-public safety/non-public service organizations not specifically addressed in other ISICS standards, which in an emergency or under contract, require cooperation and coordination with public safety users, to be included as "Authorized Users" of the statewide 700 MHz trunked digital public safety radio system for communications services.

2. Technical Background

Capabilities

The system has robust support for many users and use cases, allowing non-public safety/non-public service organizations to use the system without negatively impacting primary first responders.

Constraints

- There are finite resources available on the system available to users; for example, site channel capacity or Radio User IDs or Talkgroup IDs.
- As the quantity of non-public safety/non-public services organizations on the system increases, the system has limited resources available for additional first responder users.
- Non-public safety/non-public service organizations introduce unique management, training, and funding challenges.

3. Operational Context

This standard provides a methodology for the User Group Committee (UGC) to make recommendations to the ISICS Board (ISICSB) in determining priorities for participation requests of non-public safety/non-public service organizations to join the ISICS system. Examples include, but are not limited to, railroads, utilities, pipelines, refineries, hazmat response contractors, vehicle recovery contractors, towing companies, commercial aviation, educational institutions, technicians etc.

Certain types of these entities work directly with public safety in emergency situations involving imminent safety to life or property. These organizations must be authorized and sponsored by a police, fire, or public safety entity.

The UGC reserves the right to review any application and make recommendations for approval or denial to ISICSB.

4. Recommended Protocol/ Standard

Agencies using ISICS may allow radios to be used by certain non-public safety/non-public service organizations with which the licensee requires cooperation and coordination during an emergency. This is allowed through Section 90.421 of the FCC rules.

Non-public safety/non-public service organizations not addressed specifically in other ISICS Standards which are sponsored by a user of the system may apply under either or both of the following categories:

1. Emergency coordination with other authorized users during an emergency event which is under incident command of a public safety entity.
2. Coordination among other authorized users in the performance of official governmental activities of the sponsoring agency.

Prohibited use includes internal day-to-day, administrative, and non-emergency communications, except where otherwise approved by the ISICSB.

All requests shall be reviewed by the UGC. However, any requests for new groups or individuals as defined in this standard will also be reviewed by the Steering Committee, and other committees as deemed appropriate, before submission for approval by the ISICSB.

Nothing in this Standard shall be construed so as to prohibit a user from temporarily issuing radios to non-public safety/non-public service entities as necessary in an emergency to protect life and property. Any such use shall be approved by an incident commander, Communications Unit Leader, or COML, or a Communications Unit Leader in Training, or COML-(T), and be included in an Incident Communications Plan (ICP). Such use exceeding 72 hours shall be reported to an Executive Member of the ISICSB.

For non-users of the ISICS Platform who would need temporary access in an emergency to protect life and property. Any such use shall be approved by an incident commander, Communications Unit Leader, or COML, or a Communications Unit Leader in Training, or COML-(T), and be included in an Incident Communications Plan (ICP). Such use exceeding 72 hours shall be reported to an Executive Member of the ISICSB.

The UGC reserves the right to review any application and make recommendations for revocation of access to ISICSB.

5. Recommended Procedure

Any proposed non-public safety/non-public service organization must provide a completed, sponsored participation plan and a letter of support by a sponsoring agency. (See sample Sponsored Agency Plant template after this standard.)

Required information includes the following criteria:

Criteria 1 – Background Information

- Organization(s) requesting access
- Reason for request / proposed uses
- Number of users and radios proposed, if applicable
- Deployment time requirements
- Training plan
- Fleetmap

Criteria 2 – Value of Participant Being on ISICS

- Business need and justification for immediate interoperability with public safety responders
- Basis and justification for the quantity of resources requested
- Area of impact (critically: e.g., emergency search and rescue, food, shelter, mental health services, clean-up, utility service storage)
- Whether the support is duplicative of that provided by another entity (e.g. whether there is overlap with the requestor's service with others already on the system; if so: the identity, location, and service area for the incumbent entity)
- Level of coordination needed with other entities
- Risk or impact of not providing resources for your service
- Risk or impact of providing fewer resources than requested.

Criteria 3 – Sponsorship (long-term support)

- Sponsor Name
- Sponsor's commitment:
    - Budget support: (e.g., none, initial, ongoing, initial and ongoing)
    - Training support: (e.g., none, initial, initial and ongoing)
    - Monitoring and enforcement of those resources for appropriate usage
    - Letter from sponsor with roles and responsibilities assumed

Criteria 4 – Technical Consideration

- Resources required (e.g., quantity of Radio user or Talkgroup IDs, existing talkgroups required, etc.)
- Anticipated traffic load, if applicable
- Capacity for additional users in the area, if applicable

6. Management

The Sponsoring Agency will be responsible for monitoring the use of resources involved in coordination with the System Administrator.

The Iowa Statewide Interoperable Communications System Board (ISICSB) will be responsible for maintaining this standard and a roster of the agencies that are a participant under this standard.

SAMPLE SPONSORED AGENCY PLAN
(Refer to Standard 1.10.2 for Full Requirements)

Whereas,_____Sponsoring Entity is a member of the _____Iowa Statewide Interoperable Communications System (ISICS).

Whereas, the_____, as the governing body of_____Sponsoring Entity has or will enter into a Sponsored Participation Plan with the ISICSB and the State of Iowa, permitting the operation of ISICS radio equipment by non-public safety/non-public service organizations within the County.

Whereas, a Sponsored Participation Plan must be approved by the Sponsoring Entity and submitted to the_____Iowa Statewide Interoperable Communications System Board (ISICSB) User Group Committee for approval.

Now, therefore, the_____, as the governing body of _____ Sponsoring Entity approves the following Sponsored Participation Plan applicable to the use of ISICS radios by non-public safety/non-public service organizations.

Any non-public safety/non-public service organization must provide a completed, sponsored participation plan and a letter of support by a sponsoring agency stating their roles and responsibilities. Required information includes the following 4 Criteria:

Criteria 1 – Background Information

- Organization(s) requesting access
- Reason for request / proposed uses
- Number of users and radios proposed, if applicable
- Deployment time requirements
- Training plan
- Fleetmap

Criteria 2 – Value of Participant Being on ISICS

- Business need and justification for immediate interoperability with public safety responders
- Basis and justification for the quantity of resources requested
- Area of impact (critically: e.g., emergency search and rescue, food, shelter, emotional, clean-up, utility service storage)
- Whether the support is duplicative of that provided by another entity (e.g. whether there is overlap with the requestor's service with others already on the system; if so: the identity, location, and service area for the incumbent entity)
- Level of coordination needed with other entities
- Risk or impact of not providing resources for your service
- Risk or impact of providing fewer resources than requested.

Criteria 3 – Sponsorship (long-term support)

- Sponsor Name
- Sponsor's commitment:
    - Budget support: (e.g., none, initial, ongoing, initial and ongoing)
    - Training support: (e.g., none, initial, initial and ongoing)
    - Monitoring and enforcement of those resources for appropriate usage
    - Letter from sponsor with roles and responsibilities assumed

Criteria 4 – Technical Consideration

- Resources required (e.g., quantity of Radio user or Talkgroup IDs, existing talkgroups required, etc.)
- Anticipated traffic load, if applicable
- Capacity for additional users in the area, if applicable

Sponsor

The following person is designated as the Sponsoring entity's contact for any issues related to operation and maintenance of ISICS subscriber equipment:

- (Name and title)
- (Telephone number)
- (Email address)

The Sponsoring Entity's request that upon qualification, in accordance with ISICS Standard 1.10.2, any Iowa Statewide Interoperable Communications System, etc., Standards and requirements of the ISICSB, the non-public safety/non-public service organization's contracted vendor will be provided with the system key and subscriber programming orientation necessary to allow the non-public safety/non-public service organization's contracted vendor to program and maintain ISICS subscriber radios.

Approved and adopted by the Sponsoring Entity on_____of_____, 20XX.

_____ _____

_____ _____

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**SYS-TECH Talkgroup**		Date Created:		**06-07-2018**	
Standard Policy #	**1.14.0**	**Section Title:**	**Interoperability Standards**		Status	**Approved**
Approval Authority:	**ISICSB**		Adopted:	**11-08-2018**	Reviewed:	**11-08-2018**

1. Purpose or Objective

The purpose of this standard is to define the function, purpose, and operation of the SYS-TECH talkgroups.

2. Technical Background

- **Capabilities**

This will provide talkgroups that are readily available for the support staff of multiple system agencies. These talkgroups will be enabled system wide for the coordination and communication of repair and maintenance activities on the 700/800 MHz ISICS Platform and associated equipment.

- **Constraints**

The purpose of the SYS-TECH talkgroups is for the repair and maintenance of the system. In order to use this talkgroup, the system has to be at least partially functional to carry the communications. All radios used for repair and maintenance activity coordination on the system will have encryption capability with the same encryption key loaded.

3. Operational Context

The SYS-TECH talkgroups are to be used for the repair and maintenance activities supporting the 700/800 MHz ISICS Platform. All agencies responsible for the service activities will have the appropriate regional SYS-TECH talkgroup available as a resource to communicate between agencies when providing support for the system.

4. Recommended Protocol/ Standard

It is recommended that all System Managers, System Administrators, and System Technical support staff have the SYS-TECH talkgroups programmed into their radios.

Due to the large geographic size of the 700/800MHz ISICS Platform and the amount of voice traffic used for maintenance activities in support of the system, the SYS-TECH talkgroups will be regionalized as follows:

SYS-TECH-SW	Statewide access
SYS-TECH-R1	Region 1
SYS-TECH-R2	Region 2
SYS-TECH-R3	Region 3
SYS-TECH-R4	Region 4
SYS-TECH-R5	Region 5
SYS-TECH-R6	Region 6
SYS-TECH-AG	Announcement group of all Regional SYS-TECH Talkgroups

The geographic SYS-TECH areas are generally defined by the Iowa Homeland Security Regional boundaries, with some adjustments for factoring in Zone Controller coverage areas, shown in the attached map.

Talkgroup Requirements	For Whom?
Mandatory	System Managers, System Administrators, and System Technical support staff
Recommended	None
Optional	None
Not Allowed	None

Cross Patch Standard	YES / NO	To Talkgroup(s)
Soft Patch	Yes, during repairs	As needed
Hard Patch	No	N/A

- SYS-TECH talkgroups will be programmed in the system to have site access/roaming privileges at all radio frequency (RF) sites on the system statewide.
- SYS-TECH talkgroups may be programmed for encrypted-only communications, with one commonly shared encryption key used for all the SYS-TECH talkgroups.
- For agencies not prepared for transitioning to the encryption of SYS-TECH, other agencies may have radios available depending on inventories.
- If an encryption capable radio is not available, cell phone communications are an option to inform an agency of activities or to have another agency make a SYS-TECH announcement.
- In radios where the emergency button is used, the emergency call should never be directed to SYS-TECH talkgroups.
- The SYS-TECH talkgroup is permitted to be programmed into dispatch consoles.

5. Recommended Procedure

All agencies responsible for repair and maintenance activities shall have the appropriate SYS-TECH talkgroups available for programming into their radios as an available tool to communicate between repair staff and agencies in the support of the system.

All technicians performing work on the system shall announce on appropriate SYS-TECH talkgroup(s) for the area(s) being affected what maintenance is being performed and at what agency/site. This announcement must be made prior to the commencement of work.

6. Management

The System and Subsystem Administrators are responsible for the management of the SYS-TECH talkgroups. Interagency issues involving the operation and use of the SYS-TECH talkgroups are open for review and resolution by the System Administrator.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Encryption Key Security**		Date Created:		**02-15-18**	
Standard Policy #	**2.12.3**	**Section** Title**:**	**Management of System**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	**7/12/18**

1. Purpose or Objective

The purpose of this standard is to establish policy and procedures for the security of encryption keys and the proper method of generating encryption keys used on the ISICS radio system network. This standard outlines the minimum steps that should be taken to secure any encryption key on the ISICS Platform.

2. Technical Background

- **Capabilities**

Encryption keys are used in end user equipment where encrypted voice communications are utilized. This includes, but may not be limited to, subscriber radios, dispatch consoles and radio voice logging equipment. Encryption keys are typically stored in Key Fill Devices (KFD), Key Management Facilities (KMF) or locked in a secure facility with limited access. Encryption utilizes a traffic encryption key (TEK) which is a string of hex characters of varying length depending on AES encryption protocol. Each TEK is assigned a Key ID (KID) and a Storage Location Number (SLN) that are used to select or index the desired TEK. Because modern subscriber units are capable of using several TEKs to encrypt transmissions, the SLN and KID are utilized so that the receiving equipment will know which encryption key to use to decode the transmission.

- **Constraints**

If a radio user or dispatch console utilizes encryption and other users on that talk group do not have the correct TEK, KID and SLN in their equipment, the user will not receive the message. Any radio voice logging equipment that does not have the appropriate TEK, KID and SLN will not log the voice traffic.

SLN/KIDs must be unique across the system.

While it is possible for more than one key to be identical, no two distinct encryption keys should use the same SLN/KID. E.g. if a region has SLN/KID "1" with a key of "00000000" and "0000000A"), this would cause the receiving unit (radio/console or voice logging equipment), to not accept one of the keys, or the unit would not know which key is appropriate for receiving an encrypted transmission with "SLN/KID 1".

3. Operational Context

The terminology "ISICS TEK(s)" references TEK(s) that are used for encrypted interoperability talk groups on the ISICS Platform.

4. Recommended Protocol/ Standard

ISICS TEKs and associated KIDs and SLNs used on the ISICS Platform must be kept secure.

No ISICS TEKs will be loaded or stored in any device where the key can be viewed. No ISICS TEKs will be stored in "plain text" in any device. It is also highly recommended that regional and locally owned and used TEKs not be allowed to be loaded or stored in a radio system device that stores the encryption keys in plain text.

No regional, local, or privately owned TEK may be loaded into any radio or console position without the approval of the owning Sub-System Administrator.

ISICS TEKs should only be distributed by the System Administrator, by using the following procedure to verify the identity of the sub-system administrator.

5. Recommended Procedure

The System Administrator or designee shall generate ISICS TEKs as necessary for their use. ISICS TEK(s) generated will be within the SLN/KID range designated and assigned by the System Administrator. The System Administrator(s) will be responsible for distributing the ISICS TEKs appropriately. ISICS TEKs used on the ISICS Platform must be kept secure. Subscriber radios, consoles, and logging solutions may require the use of a key loader/key fill device (KFD). The KFD is a device where the System Administrator or sub-system administrator enters the ISICS TEK(s) and associated SLN(s)/KID(s), and the key loader is then used to program the end user devices. KFDs used in conjunction with ISICS Platform must store the ISICS TEKs in an encrypted fashion and shall not display the individual key data.

The System Administrator shall only release an ISICS TEK to established sub-system administrators or designated personnel. Upon a request for an ISICS TEK, the System Administrator must look up the sub-system administrator in their files and call him/her at the phone number of place of employment. When satisfied that the correct sub-system administrator is reached, the System Administrator may verbally release the data. The ISICS TEK will not be emailed or transmitted electronically via plain text. The sub-system administrator shall then

store the written key in a secure location (e.g. locked safe with access to only the sub-system administrator or authorized designee) and destroy it once it has been added to a KFD. Any KFD should use an appropriate password to unlock the device for use.

The System Administrator will document the following for statewide TEKs:

- Which TEKs are allowed to be shared;
- Who the TEKs are shared with;
- When the TEKs were shared.

In special circumstances and with approval of the System Administrator, sub-system administrators can share ISICS TEKs with other sub-system administrators. The System Administrator will be notified so they may document the sharing of ISICS TEKs.

The TEKs should also be transferred from KFD to KFD or KMF to KMF, when technologically proven and practical, to minimize the chance for errors and to keep written copies of the keys to a minimum.

6. Management

Generation and storage of ISICS TEKs are the responsibility of the System Administrator or designee. Generation, storage and management of any local TEKs are the responsibility of the appropriate sub-system administrator.

The System Administrator is responsible for the correct programming of ISICS TEKs in all KFDs, KMFs. The sub-system administrators are responsible for console and subscriber radio programming.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Subscriber Radio Standards**		Date Created:		**05-08-2018**	
Standard Policy #	**2.13.0**	**Section Title:**	**Management of System**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	7/12/18

1. Purpose or Objective

The purpose of this standard is to:

- Set minimum technical and performance standards for subscriber radios allowed to operate on the Iowa Statewide Interoperable Communications System (ISICS).
- Provide procedures to measure, test, certify and/or publish a list of subscriber radios which are approved for use on the system.

2. Technical Background

Capabilities

The ISICS Platform uses the digital communications technology specified in the TIA-102 Series Standards, Interim Standards, and Telecommunications Systems Bulletins, commonly known as APCO Project 25 (P25). The P25 standards provide capability for full backward migration and limited forward migration along an evolving continuum of technologies and services assuming the radios operate on a common set of frequencies. P25 also permits different vendors of subscriber radios and infrastructure to provide value added vendor specific premium features and services. The ISICS Platform uses P25 Phase II Time Division Multiple Access (TDMA) modulation.

Constraints

Subscriber radios from vendors using different radio operating software will provide a variety of services, features, functionality, and performance to the users. Some radios will also interact differently with the infrastructure and could potentially exhibit undesirable operations.

It is possible that new, unproven radios and/or software may exhibit performance and functionality characteristics that are destructive to the overall performance, capacity and/or security of the ISICS platform.

This standard does not include paging equipment.

3. Operational Context

Participants using the system need access to radios that will meet their operational needs for the lowest cost. It is anticipated that radios capable of operation on the system will be available from multiple vendors over the life of the system. Users need the flexibility and knowledge to optimally choose from the radios available in the marketplace that would be operationally desirable and not cause problems for other users on the ISICS Platform.

4. Recommended Protocol/ Standard

All subscriber radios meeting the applicable P25 Standards that DO NOT exhibit operational, performance, or other characteristics that substantially and measurably negatively impact the system or its users will be approved for use on the system.

Before a new subscriber radio that is not on the vetted subscriber radio list is approved for use on the system, it shall undergo a vetting process in which the list of required P25 features are sent to the manufacturers for verification that the required functionality exists in their subscriber units and is compatible with the ISICS infrastructure. The manufacturers shall provide documentation confirming functionality and compatibility in conjunction with a list of required features.

5. Recommended Procedure

5.1 Verification of functionality of subscriber radios for operation on the system

- Identification of the radio proposed for use on the system. Radios or pre-production radios may be submitted for evaluation by any authorized user. Radio equipment manufacturers should work closely with an authorized user who is considering purchasing the proposed radio.
- Review of technical specifications to determine basic compliance with the P25 Standards.
- Review the specified functionality outlined in Appendix A with the manufacturer of the radio. Functionality should be verified based on the underlying ISICS infrastructure. Acceptable documentation can include P25 Compliance Assessment Program (CAP) results or other inter-manufacturer interoperability testing. The Technology Committee may review and update Appendix A as needed.
- Technology Committee reviews documentation of standards compliance and testing. If the stipulations are met, the Technology Committee acts to approve the radio for use on the system. Any potential concerns, limitations or constraints will be documented. If the Technology Committee has any concerns or questions that would preclude approval, follow-up documentation will be requested.
- The CAP and/or inter-manufacturer interoperability testing documentation and any additional actions taken by the Technology Committee will be submitted to the ISICSB for final action.

- A list of approved radios will be posted on the ISICSB web site.

5.2 Problems with Previously Approved Radios

5.2.1 *New problem with previously approved radio*
If a previously approved subscriber radio type begins to exhibit characteristics that are harmful to the operation of other users on the system, users are required to coordinate with the manufacturer and provide documentation when the problem is solved. The subscriber unit functionality outlined in Appendix A may be reviewed and updated by the Technology Committee to ensure proper testing of characteristic exhibited.

If a problem is due to the use of a new feature in the radio, that feature will not be allowed to be used until satisfactorily repaired and tested by the manufacturer for proper operation.

5.3 Purchase of second-hand and/or used radio equipment

Any purchase of second-hand or used radio equipment may require an inspection and software flash by the vendor to ensure that it is in proper working order. The purchaser is responsible for ensuring the radio is coming from a reputable vendor and in good working order.

6. Management

The Statewide System Administrator is responsible for managing this procedure, including maintaining all certification records, managing radio equipment manufacturer-initiated submittals, and coordinating activities of the Technology Committee.

Appendix A

List of Required Functionality on the ISICS Infrastructure

1. Group Call Receive
2. Group Call Transmit
3. Intra-system Roaming
4. Registration & Affiliation
5. De-registration & De-affiliation
6. Emergency Call

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Subscriber Radio Disposal**		Date Created:		**02-15-18**	
Standard Policy #	**2.13.1**	**Section** Title**:**	**Management of System**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	**7/12/18**

1. Purpose or Objective

To ensure that all subscriber radios are properly removed from the ISICS system when they are no longer needed or disposed of.

2. Technical Background

- **Capabilities**

Each programmed subscriber radio contains a listing of local, regional and statewide system information that falls under the categorization of critical infrastructure and not for public disclosure under Chapter 22.7(50) of Iowa Code.

- **Constraints**

If radios are not properly de-programmed, there is a potential for a number of system-level issues. These issues include, but are not limited to, duplicate radio ID's, talkgroup usage issues, talkgroup affiliation issues, and a potential compromise of traffic encryption keys (TEKs) and associated key ID (KID) and storage location number (SLN) data remaining in the radios, as well as ISICS system programming information.

3. Operational Context

Subscriber radios identified for disposal, which have not been de-programmed could be turned on and cause system issues. Duplicate IDs can create receive issues for an agency with the same radio ID. There is also the potential of releasing a significant amount of proprietary system information like control channel lists, wide area communications network (WACN), SYSTEM ID, network access codes (NAC), and other technical parameters. A radio with ISICS TEK(s)

still programmed into the device may allow an unauthorized user to hear sensitive audio transmissions.

4. Recommended Protocol/ Standard

Surplus subscriber radios must be de-programmed or destroyed to prevent unwanted consequences to the ISICS Platform. A sub-system administer shall notify the System Administrator whether the Subscriber ID for that radio will be re-used.

5. Recommended Procedure

All surplus subscriber radios must have all of the ISICS Platform programming information, talk groups and all of the conventional frequencies removed before they are marked for disposal, sold or scrapped. The crypto module shall be zeroized. The ID of the radios should be set to default. Final verification by subsystem administrator that the radios have been deprogrammed should be performed before the radios leave the possession of the owning agency.

In the event that a radio cannot be zeroized or deprogrammed, the System Administrator will be notified by the agency and verify that appropriate steps have been taken to mitigate any potential compromise of the encryption material.

6. Management

Sub-system administrators and subscriber radio owners will be responsible for ensuring that all radios are deprogrammed and disposed of correctly.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Radio Aliases**		Date Created:		**02-01-18**	
Standard Policy #	**3.1.0**	Standard Title:	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this standard is to set forth the principle by which all Subsystem Administrators and their radio users on the ISICS system will establish names for their radios. This will ensure there are no duplicate names and explain how radio alias names are created.

2. Technical Background

Capabilities

Constraints

Every Radio User ID in the system has to be unique and cannot be duplicated.

The Radio User Alias field will hold up to 14 characters; the system will accept upper case alpha, numeric, period, dash, forward slash, and the number sign.

3. Operational Context

With the exception of the first two characters, users are technically free to choose any name they wish for their radio aliases. However, since this is a shared system, Radio User Aliases programmed into the system must have naming conventions so aliases will not conflict with each other.

4. Recommended Protocol/ Standard

Radio User Aliases will be prefixed with unique agency identification. Because of the number of agencies using the system, the prefix would be a minimum of two alphanumeric characters in length.

Alias IDs shall begin with the first 2 characters:

- County/local – County Number Code
- State – IA
- Federal – US

Any deviations or exceptions to this naming standard must be approved by the Operations Committee.

The naming standard only governs the first two characters, and characters following the first two are at the individual agency's discretion. For example, the agency may opt to use more than two characters for the internal identifications.

The body of the subscriber alias name could include an agency identification for the individual or pool radio, e.g., possibly the radio user's call sign. If a radio user has multiple radios on the system, each radio must have a unique alias. The alias could be suffixed with identification for the radio itself, such as a "-P" for portable to differentiate between a mobile and portable radio used by the same person. This would allow dispatchers and System Administrators to readily identify radio users and whether the radio is a portable or mobile.

An example could include the following:

For any agency within Dallas County, the alias could be read as follows:

- 25 25-1 M → [Dallas County Number Code] [Dallas County Number Code-Badge Number] [M for Mobile]
- 25 ADPD 1 M → [Dallas County Number Code] [Adel Police Department] [Car Number] [M for Mobile]
- 25-172 P → [Dallas County Number Code] [Adel Police Department Badge Number] [P for Portable]
- 25 EMS 1 P → [Dallas County Number Code] [EMS County-wide] [Radio Number] [P for Portable]

For a federal agency, the alias could be read as follows:

- US DEA 23 M → [US Federal Agency] [Drug Enforcement Agency] [Agent #] [M for Mobile]

A master table of Radio User Aliases will be created and maintained in the system by the Statewide System Administrator. They will be readily accessible through the data terminal for all who have rights on that part of the system. As alias names are created and approved, they will be placed on this master list to assist with operations and planning. (See State Standard 2.6.0, "Database Management", under Section 2 – Management of System.)

The Statewide System Administrator will be responsible for creating and assigning two-character prefixes for all agency identification.

5. Recommended Procedure

N/A

6. Management

The Local System Administrators and Statewide System Administrator are responsible for compliance of this standard.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Talkgroup and Multigroup Names**		Date Created:		**02-01-2018**	
Standard Policy #	**3.2.0**	Standard Title:	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this section is to set forth the principle by which all administrators of ISICS will establish names for talkgroups and multigroups in order to ensure that there are no duplicate names, and to facilitate intuitive understanding of the talkgroup/multigroup name. This standard also allows radio users, dispatchers, and System Administrators to readily identify talkgroup ownership.

2. Technical Background

Capabilities

The ISICS system allows for talkgroups and multigroups to have any unique name up to sixteen characters in length.

Constraints

Each talkgroup name must use a unique name in the system, there can be no duplicates. Different radio models will display talkgroup/multigroup names of varying lengths. Most radios certified for use on ISICS will display a talkgroup/multigroup name of eight or more characters.

It is recommended that talkgroup/multigroup names be a maximum of eight characters in length but is up to the discretion of the agency. Shared interoperable talkgroups will be restricted to a maximum of eight characters and the formatting of the name will match exactly to the programming guide document.

3. Operational Context

Since this is a shared system, talkgroup/multigroup names must have naming conventions that will not conflict with other agencies. With the exception of the first two characters, users are free to name their talkgroup/multigroup according to their preference provided it is unique and uses no more than 16 characters total.

When choosing talkgroup/multigroup names users should choose names that clearly define the purpose of the talkgroup/multigroup, consider the display limitations of some radios, and follows a standard nomenclature. This is essential because some talkgroups/multigroups will be shared by multiple agencies.

4. Recommended Protocol/ Standard

The talkgroup/multigroup name will be prefixed with an agency identification that must be unique to that agency and will readily identify the agency the talkgroup is associated with. The agency IDs would be the same as those identified in Section 3.1.0 – Radio Aliases, and maintained by the Statewide System Administrator.

Regional interoperability talkgroups/multigroups would be prefixed with the appropriate two character regional prefix. The list of regional prefixes is maintained by the Statewide System Administrator.

Talkgroups and multigroups that are not owned by an individual agency or region would not have an agency/region specific identifying prefix. Examples of these would be non-agency owned mutual-aid talkgroups, interop talkgroups such as IACALL1 or external agency talkgroups that are interfaced with a control station.

5. Recommended Procedure

N/A

6. Management

The System Administrators are responsible for seeing that the defined standard is followed and maintained.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Radio ID & Talkgroup Allocation**		Date Created:		**02-01-18**	
Standard Policy #	**3.3.0**	Section Title:	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of allocating talkgroup ID ranges and radio ID ranges for the individual agencies allows the individual agencies to manage their pool of IDs as talkgroups and radio users / console positions are configured. This will simplify the management of the IDs and provide an easier indication of which IDs belong to what agency in the event that a radio user alias is not available.

2. Technical Background

Capabilities

Radio IDs must be in the range of 1 to 16,777,214. These IDs will be the same that users will enter in when doing private calls or call alert pages. Also, the IDs picked at this step will be the same that will be displayed on the subscriber radios if the "ID Display" feature is purchased and enabled. These IDs will also be displayed at the console if the console alias feature is not used.

Talkgroups must be in the range of 1 to 65,534. These are always prefixed with “800” so they will be entered and displayed on the manager as “80000001” to “80065534.”

Every dispatch console will also use a radio ID for each individual talkgroup at each individual position that is programmed into the console, and must be factored in the planning.
Every dispatch console will also use a single radio ID at each individual position.

Constraints

3. Operational Context

The Statewide Radio System will start at the beginning of the talkgroup range with "1" and at the beginning of the Radio ID range with "1" as indicated in the table of Allocated Talkgroup & Radio ID Numbers. The other regions of the state will follow the last entry.

In planning the values for the table, the individual agencies should use a realistic anticipation of the numbers of talkgroup & radio user IDs that are expected to be in use during their initial implementation plus a reasonable quantity for future growth for 3 years. These amounts will then be entered into the Allocated Talkgroup and Radio ID Numbers as the Fleetmap process progresses.

The system management structure of the ISICS system allows for the Statewide System Administrator and other approved Local System Administrators, defined in ISICS Standard 1.1.0, to create and load IDs into the system. While the Statewide System Administrator has full rights to create/edit all IDs in the system, the other Local System Administrators have access and creation rights to their defined security group.

4. Recommended Protocol/ Standard

At the time of ISICS application approval by the User Group Committee (UGC), a fixed number of Talkgroup and Radio IDs will be assigned to the requesting agency. This number is the planned number initially needed by the agency plus a reasonable quantity for future growth for three years. If more IDs are required in the future the agency will need to follow the procedures as outlined in ISICS Standards to request more IDs from the UGC. Refer to the Talkgroup and ID Allocation table for full information.

For programming radio users, talkgroups and console positions individual agencies will use the IDs that have been reserved for them in the Talkgroup and ID Allocation.

Approved Local System Administrators that have been assigned a system management account will load the appropriate IDs into the system as needed but not exceeding their allocation from the UGC.

Agencies must not use IDs that are not their own.

5. Recommended Procedure

At the time of application approval the UGC will approve a fixed number of talkgroup and radio IDs to the requesting agency. This number is the planned number needed by the agency plus a reasonable quantity for future growth for three years. If more IDs are required in the future the agency will need to follow the procedures for moves changes and additions to request more IDs from the UGC.

Approved Local System Administrators that have been assigned a system management account will load the appropriate IDs into the system as needed but not exceeding their allocation from the UGC.

Existing users will be required to submit a plan projecting the number of talkgroup and radio ID's that will be needed for future growth. The approved three year projection plans will then be used to update Talkgroup and ID Allocation.

6. Management

The Statewide System Administrator will maintain the Table of Allocated Talkgroup & Radio ID Numbers and the Table of Defined Ranges.

Subsystem Administrators will individually manage the ID ranges for day to day activities.

It is recommended that all Subsystem Administrators complete bi-annual self-audits outlining the amount of IDs currently in use by their agencies in reference to their allocations.

Subsystem Administrators will be required to attend a meeting called by the Statewide System Administrator, to discuss system management procedures and review audits in need of attention.

Between December 1 and December 31 of each year, all Subsystem Administrators shall submit a yearly report to the Statewide System Administrator, outlining the amount of IDs currently in use by their agencies in reference to their allocations and submit a three year plan projecting the number of talkgroup and radio ID's that will be needed for future growth.

All System Administrators found to be in violation of this standard will be held accountable for their actions in accordance with ISICS Standards.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Fleetmap Standards**		Date Created:		**02-01-18**	
Standard Policy #	**3.4.0**	Section Title:	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The Iowa Statewide Interoperable Communications System (ISICS) will contain a large number of talkgroups and multigroups to support the various agencies that will be subscribing to the system.

The system has multiple administrating agencies that will maintain fleetmaps and system programming information for agencies they are responsible for.

For effective management of the system, a defined process needs to be used to document the fleetmap information that each administrating agency is supporting. This information will be shared with other System Administrators, providing a resource for subscribing agencies to reference when planning interagency communications. System fleetmaps contain configuration information that is classified as "Security Information" and "General Non-Public Data," pursuant to Iowa Code section 22.7(50) and Iowa Administrative Code 661-80.13(22.5).

2. Technical Background

Capabilities

The fleetmap is parameter information programmed into the system infrastructure and into the subscriber radios to control how the radios will behave on the ISICS system.

The fleetmap itself contains the following detailed information:

Talkgroup	Name of the talkgroup & multigroup as it is programmed into the system.
Talkgroup ID	Numerical ID of the talkgroup or multigroup
Owner	The agency requesting the creation of the talkgroup
Description	General description of the talkgroup & multigroup
Multigroup	If the talkgroup is part of a multigroup, this will identify a multigroup
Priority	Priority level of the talkgroup
Logging	If the talkgroup is going to be recorded
Admin Agency	The agency that is responsible for the system administration for this talkgroup
Site # Access	Will be listing the RF sites individually and if the talkgroup is authorized
Media Access	If media access is permitted for this talkgroup
Global Sharing	The predefined global sharing authorizations
User Groups	The subscriber groups using the talkgroups, this becomes the matrix for the

The fleetmap spreadsheet will become a documented matrix of the talkgroups in the system and the subscriber groups that are using/sharing these talkgroups.

Constraints

Since the system will be administered by multiple agencies and access is controlled, no master list will be maintained.

3. Operational Context

The local System Administrator shall be responsible for managing the fleetmap information of the subscribers they are representing. This information is also shared with other System Administrators, and the ID information must be kept secure.

4. Recommended Protocol/ Standard

Each administering agency will maintain a master fleetmap spreadsheet containing data as outlined in Section 2 of this standard for whom they are responsible.

5. Recommended Procedure

System Administrators may omit listing any information in the master fleetmap spreadsheets for "unlisted" private talkgroups used for undercover operations and other highly sensitive confidential law enforcement and homeland security activities. Approval by the ISICS Board is required for a talkgroup to be designated "unlisted" and private. The request will include talkgroup system settings, names, priority level, and site access, if applicable. The existence of unlisted talkgroups is considered "Non- Public Data" and is not subject to disclosure in public meetings.

The disclosure of fleetmap spreadsheet information including talkgroup IDs, user IDs, user privileges, and other related system information would substantially jeopardize the security of

the system. Therefore, the master fleetmap spreadsheets shall be classified as “Security Information” and “Non-Public Data.”

6. Management

The Statewide System Administrator will manage the master fleetmap spreadsheet information and the details of the process for communicating the information.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Statewide Wide Area Talkgroup Access and Management**		Date Created:		**02-01-2018**	
Standard Policy #	**3.5.0**	Standard Title:	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**02/08/2018**	Reviewed:	**02/08/2018**

1. Purpose or Objective

The purpose of this standard is to establish a policy that provides radio connectivity throughout the ISICS system while minimizing roaming and excess system loading.

2. Technical Background

Capabilities

On the ISICS platform, it is possible to allow all radios and talkgroups to operate and "roam" throughout the system. It is also possible to restrict radios and/or talkgroups from operating on particular sites and sub-systems. It is also possible for users to leave one or more radios selected to an interoperability talkgroup on a long-term basis solely for the purpose of monitoring. This is commonly referred to as "parking on the talkgroup" and will unnecessarily consume system capacity.

For a radio to access a radio frequency (RF) site, it is an "AND" relationship between the Radio User Site Access Profile and the Talkgroup Site Access Profile. Typically, agencies set their radio access to all sites and manage the access through the Talkgroup Access Profiles.

Constraints

Sites and subsystems can only support a specific number of concurrent, active talkgroups. It is possible that a large number of "roaming" or other talkgroups with busy traffic could overload a site or sub-system. Similarly, users switching to an interoperability talkgroup during an emergency incident they are not assigned solely to monitor the incident will also unnecessarily consume system capacity.

The site access rules are implemented from the Core. If the site loses connectivity with the Core, the rules are suspended until connectivity is restored.

The system has a limit of 500 Talkgroup Site Access Profiles. With the number of agencies using the system, profile quantities should be minimal but still meet the need.

The system is capable of "Requested Site" where a talkgroup's traffic is pushed to a site regardless of the radio affiliations at the site. This consumes channel capability and should be minimally used and require special authorization.

3. Operational Context

System functionality must be maintained by ensuring that only talkgroups and users with a legitimate business need on a site or subsystem are allowed access.

4. Recommended Protocol / Standard

Approved statewide talkgroups would be allowed access to all sites and subsystems.

If an agency has a tactical or a main operability talkgroup that does not require statewide access, it shall be limited by the area needed for that talkgroup.

Regional talkgroups will be allowed on all sites and subsystems within the region, as well as sites and subsystems directly adjacent to the region.

Statewide Roaming-Only Talkgroups

Special roaming-only talkgroups could be used statewide by agencies leaving their primary response/service area. These talkgroups would be used only for communicating while roaming outside their standard coverage footprint.

Other than for special circumstances, standard operational and tactical radio traffic would not be allowed on these talkgroups. These talkgroups would not be permitted to be patched. Examples could be EMS or jail roam talkgroups.

Statewide Tactical Talkgroups

Special tactical talkgroups could be used statewide by agencies that require operations outside their home area. Other than for special circumstances, these talkgroups shall not be patched. (Examples would be regional drug task force or statewide SWAT team talkgroups.)

To prevent overloading of sites and subsystems from distant, unrelated incidents, it is recommended that users not channel-select region wide and statewide interoperability talkgroups to monitor activities they are not assigned to. This recommendation does not restrict the scanning of regional and statewide talkgroups while radios are channel-selected on their local talkgroups.

5. Recommended Procedure

Statewide Access

Statewide talkgroups shall be approved by the Iowa Statewide Interoperable Communications System Board (ISICSB) Operations and Technology Committees and be allowed on all ISICS sites and systems.

In an emergency, a subsystem administrator, Communications Unit Leader (COML) or Communications Unit Technician (COMT) may request the System Administrator or designee to temporarily allow a talkgroup statewide access. The System Administrator or designee will notify and obtain concurrence from one of the following individuals, in the order indicated, prior to implementing the emergency access: Statewide Interoperability Coordinator (SWIC), or ISICSB Chair. If the SWIC cannot be contacted, the System Administrator may honor the request and notify the SWIC as soon as possible. The temporary access may be granted for up to 14 days.

Adjacent Site Access

Talkgroups would be allowed on sites and subsystems that are within and directly adjacent to the talkgroup owner's agency response / service area.

The agency responsible for these talkgroups shall ensure that all radios programmed with the talkgroup have site preferences programmed to minimize traffic on the adjacent sites with talkgroup access. The agency responsible for these talkgroups will notify the appropriate, adjacent site's system owner before adding the talkgroup to the adjacent site.

The agency responsible for the talkgroups will work with appropriate, adjacent site's system owner to correct issues with excessive traffic to the adjacent site. If the adjacent site's system owner has issues that are not resolved, they should notify the ISICSB.

Requested Site Access

This capability of the system should be used as minimally as possible, with the minimum number of talkgroups and the minimum number of sites.

Agencies may use the Requested Site function on sites with permission from local owners and the ISICSB.

If site loading becomes an issue, any requested traffic at the site will have to be reviewed and possibly removed, or additional channel capacity can be added to the site. For the purpose of channel loading discussions, ownership is recognized by the agencies that have provided that channel capacity.

Radio User Initiated System Loading

In the event that radio system user(s) "parking on a talkgroup" or switching to an interoperability talkgroup during an incident they are not assigned to is causing unnecessary or excessive loading

conditions on a site or subsystem, a subsystem administrator or the System Administrator may immediately choose to shed load by contacting the radio user(s) violating this practice and request them to move off of the selected talkgroup.

If the user causing unnecessary or excessive loading cannot be reached by telephone or by calling them on the selected talkgroup, or if they are unwilling to move from the talkgroup, the subsystem administrator or System Administrator may contact the local subsystem administrator having security rights for the radio causing the issue and may request the radio be Dynamically Regrouped or Selectively Inhibited to remove the traffic load from the subsystem. A radio that is Dynamically Regrouped shall only be regrouped to the user's main dispatch talkgroup or other primary talkgroup. Dynamic Regrouping and Selectively Inhibiting a radio without the user's consent due to a violation of this standard should only be done as a last resort.

6. Management

If system loading becomes an issue at any site, it shall be dealt with at the local level. If the issue cannot be resolved at the local level, it will be brought forth to the Operations and Technology Committees. If the situation still remains unresolved after these steps, it shall then be brought to the ISICSB.

The System Administrator will provide periodic system usage and loading reports to the Subsystem Administrators and the ISICSB so system traffic patterns can be reviewed and corrections made if required.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Radio Site Access Permission – Subsystem Roaming**		Date Created:		**03-27-2018**	
Standard Policy #	**3.6.0**	Section Title**:**	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**04/12/2018**	Reviewed:	**04/12/18**

1. Purpose or Objective

The network infrastructure and subscriber units are configured to permit managed access to sites throughout various parts of the system. This managed site access provides the ability for users to achieve wide area coverage where necessary for mission-critical operations, enhanced in-building portable coverage, and a degree of system level backup in the event of certain types of major network failures. Roaming for non-essential operations is subject to being restricted, in order to maintain an acceptable grade of service for mission-critical operations.

2. Technical Background

Infrastructure programming settings that control site access for talkgroups / multigroups

There are settings in the system infrastructure to control the "Site Access Denial Type" parameter, which controls how site access is handled for radio users of the system. Radio users and talkgroups have independent access lists programmed into the system infrastructure. These lists control which sites the radio and/or the talkgroup can access. The level of access depends on the "Site Access Denial Type" setting. Options for this setting are:

> Individual Only: The radio is rejected if the individual radio user ID does not have access to the system.
>
> Talkgroup Only: The radio is rejected if the current, selected talkgroup ID does not have access to the site, regardless of radio user site access settings.
>
> Both: The radio is rejected only if BOTH the talkgroup ID AND the Radio User ID do not have access to the system.

Either: The radio is rejected if EITHER the talkgroup ID OR the Radio User ID do not have access to the site.

Infrastructure programming settings that control site access for Interconnect / Private Call

The site access privileges for private and interconnect calls are based on the site access settings for the radio user and not based on the system "Site Access Denial Type" settings. They are independent of talkgroup site access settings.

Radio programming settings that control site access

The subscriber radios contain "Site Preference" selections for radio programming. Radios can be programmed with multiple unique personalities, which will allow unique Site Preference Selections for each talkgroup in the radio.

Least Preferred: The site will be avoided unless it is the only usable site for operation.

No Preference: The site is given no preference. If the site is not listed here, the radio automatically assigns it no preference.

*Preferred: The site will be used over all non-preferred sites with similar signal strength.

*Always Preferred: The site will be used over all non-preferred sites with similar signal strength, even if the site loses communication with the Zone Controller and enters site trunking.

*Note: Always Preferred and Preferred are operationally identical if the radio sites have communication with the system and are operating in wide area mode.

Constraints
Using the "Both" site access denial setting to facilitate unique, individual needs will allow those individuals full access to all their talkgroups at sites they have "Radio User" permission for.

Using the "Either" site access denial setting to facilitate unique individual needs may block those individuals from site access, even in emergency conditions.

3. Operational Context

Normally, only regional and statewide interoperability talkgroups will be permitted access at ALL sites.

Talkgroups would generally be permitted access at all those sites necessary to support the "normal day-to-day" business operations of the users of that talkgroup.

If it is necessary that a talkgroup have redundancy protection in the event of a site failure, the attempt shall be made to use an adjacent or overlapping non-owned site for the talkgroup's

protection. Factors determining the best protection site include coverage of the site or function of the talkgroups per site.

Custom talkgroup site access configuration profiles can be created for consistency with this standard.

Dispatchers would be able to use the regional and statewide interoperability talkgroups or other "common," "roaming," or "pool" talkgroups as described in Infrastructure Configurations (below) for patching to their local area talkgroup to facilitate temporary wide area access.

4. Recommended Protocol/ Standard

Subscriber Unit Configuration

In subscriber radio programming, the radio would normally be enabled for all sites of the system, and the operational site access would be managed at the system level.

The Subsystem Administrator will program the radio's site preference tables to maintain roaming at an acceptable level, while minimizing impact to other sites.

Radios with no site preference tables, or with all sites set to the default "No Preference," will generally not be allowed on the system, because they will indiscriminately roam among all sites where the selected talkgroup is allowed.

Infrastructure Configuration

Radio user profiles would generally not have special site access permissions granted. Site access for wide area operations will primarily be managed at the talkgroup level. Subsystem Administrator's may accomplish this by designating site access throughout the system to a limited number of special wide are talkgroups. These special talkgroups would not be main dispatch or tactical talkgroups with high volumes of radio traffic but may be regional and statewide interoperability talkgroups or Wide Area, "roaming," "common," or "pool" talkgroups. The "Site Access Denial Type" for the system is at a site if both the talkgroup privileges are denied at the site. The use of "Critical User" and Critical Site" in the system is generally discouraged and must be authorized by the Iowa Statewide Interoperable Communications System Board (ISICSB).

5. Recommended Procedure

The defined standard would implemented and maintained by the appropriate System and Subsystem Administrator(s).

6. Management

The System and Subsystem Administrator is responsible for oversight and ensuring that the standard is followed.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Scanning**		Date Created:		**03-27-2018**	
Standard Policy #	**3.7.0**	Section Title**:**	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**4/12/2018**	Reviewed:	**4/12/2018**

1. Purpose or Objective

The purpose of this standard is to identify operational procedures and responsible authorities governing scanning activities.

2. Technical Background

Capabilities

The network infrastructure and subscriber units may be configured to permit managed user scanning of talkgroups. Scanning is a user option, and users need to be trained that including a talkgroup in a non-priority scan list will not necessarily result in them hearing traffic on that talkgroup. The talkgroup must also be "active" at the site where the user is affiliated. Talkgroups are activated if there is at least one user affiliated at the site that has the talkgroup of interest as their selected channel.

Constraints

N/A

3. Operational Context

A talkgroup owner may pre-approve monitoring privileges. Any unauthorized transmission on non-owned talkgroups in violation of this policy may result in immediate subscriber unit de-authorization and removal of the talkgroup from the radio prior to reauthorization on the network.

The network infrastructure and subscriber units will need to be configured so users can have wide area coverage and still maintain an acceptable level of service for all users. The use of "Critical User" and "Critical Site" in the system for the purpose of non-priority scanning is not

permitted unless permission by Iowa Statewide Interoperable Communications System Board (ISICSB) is granted, and scanning between different sites will be accomplished by the use of "requested sites." Local enhancements are exempt.

4. Recommended Protocol/ Standard

Talkgroup owners and Subsystem Administrators may approve limited scanning/monitoring privileges. Before scanning/monitoring of owned talkgroups, permission must be granted.

As cited in ISICS (Pending) Standard, Use of Shared Talkgroups, permission must come from:

- The Subsystem Administrators of the sites that are being requested for the talkgroup
- The jurisdiction / agency who is the "owner" of the requested talkgroup

Mutual aid, special roaming, and other shared talkgroups may be scanned at any time; however, "requested site" determinations will be made by the Subsystem Administrators of the affected sites.

5. Recommended Procedure

Scanning Configuration

If trunked scanning is desired, it is recommended that the local Subsystem Administrator set the radio site preferences to facilitate the scanning needs of the user, as well as coordinate with other Subsystem Administrators that may be impacted by changes in site talkgroup load.

It is further recommended that scanning be disabled when the user switches their radio to a conventional (non-trunked) channel, such as a Scene of Action (SOA) channel. However, if mixed-mode scanning (both trunked talkgroups and conventional channel members) is required by some users, it is also recommended that this scan type only be available when the radio is selected to a conventional channel. Mixed-mode scan may not provide priority revert depending on radio model, and the user may miss necessary traffic on the selected channel.

Scanning of Non-Home Site Talkgroups

It is possible to monitor a non-home talkgroup by configuring the system to request the non-home talkgroup appear on your primary/home system or "always preferred site(s)." However, doing so will consume a repeater channel on your primary/home system or "always preferred site(s)" and will carry the requested non-home talkgroups priority setting with it. Also, a call on the requested non-home talkgroup will not be delayed (busy queued) if the home system or "always preferred site(s)" does not have a channel available. While this "requested site" is the recommended approach, it must be carefully controlled, monitored, and evaluated, as it could exhaust system resources. It must be approved by the affected administering agency. Talkgroup permission forms can be found on the ISICSB website.

6. Management

The site owner and Subsystem Administrator will be the responsible authority for scanning issues. If an issue is unable to be resolved at the local level, it can be brought to the ISICSB.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Emergency Button**		Date Created:		**03-27-2018**	
Standard Policy #	**3.8.0**	Section Title**:**	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**4/12/2018**	Reviewed:	**4/12/2018**

1. Purpose or Objective

The purpose of this standard is to address Emergency Button usage on subscriber equipment. There will be a large variety of users on the radio system with various Emergency Button needs. The various ways the Emergency Button can be configured allow for flexibility of use; however, it is important to design the system in such a way that when an Emergency Button is pushed, it is responded to quickly and appropriately.

2. Technical Background

Capabilities

The Emergency Button feature, if programmed into radios, will allow a user to send an emergency notification by pressing a button on the radio. The notifications will audibly and visually alert all dispatch console positions displaying the talkgroup that receives emergency notification. Other radios that have the talkgroup selected will also receive the emergency notification and display the radio ID or alias of the radio generating the emergency.

Emergency calls are automatically assigned the highest priority available and would be first available from the queue if the system is in a busy situation. Subscribers' radios can optionally be configured to automatically key the Push-to-Talk (PTT) for a programmed period of time if the Emergency Button is pressed.

Constraints

Emergency Button usage must be directed to a predefined talkgroup in the radio programming, and the talkgroup that is selected for this must be approved by the Subsystem Administrator. Pressing the Emergency Button does not provide a central radio monitoring point with emergency location information.

3. Operational Context

An agency may use the Emergency Button function if they so elect; however, the process to receive an emergency notification needs to be documented and include resolution for the items listed under Section 4 of this standard.

4. Recommended Protocol/ Standard

Use of the Emergency Button as an emergency signaling option should be available to any agency on the radio system, subject to certain conditions and provisions.

- Agencies are not required to use this capability of the radio system.
- No agency will be permitted to enable their emergency signal on a talkgroup designated as "Emergency Button Restricted."
- All agencies implementing the Emergency Button must have a plan in place to respond to Emergency Button activation.
- All Emergency Button response plans must include, at a minimum:
    - A central radio monitoring point that can identify which radio user pushed the button and what the proper agency response should be.
    - A central monitoring point must be available during any/all hours that personnel are using the radio system.
    - A policy for use of the Emergency Button by radio users.
    - A response plan to assist the radio user in need.
    - In the event the central radio monitoring point is not the same agency as the radio user, an agreement on policy, monitoring, use, and response must be in place among the agencies.

5. Recommended Procedure

N/A

6. Management

Agencies wishing to use the Emergency Button function must coordinate with agency resources that will be receiving the emergency calls. The receiving agencies must have an appropriate plan in place, documenting the process that they will use to handle the emergency notification.

Emergency Button usage must be directed to a predefined talkgroup in the radio programming and the talkgroup that is selected must be approved by the Subsystem Administrator.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Configuration and Allocation**		Date Created:		**5-08-2018**	
Standard Policy #	**3.9.0**	**Standard Title:**	**Multigroup / Announcement**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**06-12-2018**	Reviewed:	06-12-2018

1. Purpose or Objective

The purpose of this procedure is to set forth requirements for multigroups or agency-groups that are directly shared among agencies and for talkgroups *within* the multigroups that are shared between agencies. This documentation will further provide the using agencies information on the intent, purpose, operation, and behavior of the individual multigroup.

Multigroup communications have a large impact on the talkgroups that are contained within the multigroup, especially if the affected talkgroups are shared among separate agencies.

2. Technical Background

Capabilities

A multigroup contains talkgroups within it. Its purpose is to provide a way to make announcements to a number of talkgroups at the same time; therefore, it is also referred to as an "Announcement Group."

A multigroup looks and behaves, for the most part, like a talkgroup. It can be programmed into console positions or subscriber radios and is activated the same as a talkgroup, by selecting a multigroup and transmitting.

After a multigroup call ends, there is a short period of "hang time" when a radio user can reply to the entire multigroup, even though the radio user has a single talkgroup selected within the multigroup.

Constraints

A talkgroup does not have to belong to a multigroup. If the talkgroup is in a multigroup, the talkgroup can only belong to **one** multigroup.

If a subscriber selects the multigroup mode on the radio, the radio can monitor talkgroup activity for all of the talkgroups associated with the selected multigroup **only** if the monitored talkgroup has an affiliated member in the same zone as the monitoring subscriber.

Talkgroups within a multigroup may be engaged in an active call at the time a multigroup call is initiated. The multigroups can be individually programmed to handle this in different ways:

- The talkgroup calls can be interrupted, and then the multigroup call begins. This is called "Ruthless Preemption," and anyone whose "push-to-talk" (PTT) is still active for the talkgroup calls will be unaware their call has been interrupted.
- The multigroup call can be set up to wait until all of the contained talkgroup calls are complete before the multigroup call is initiated; however, this may cause delays in initiating the multigroup call.

Delays may also be caused by talkgroup calls initiated before the multigroup call is allowed to start.

3. Operational Context

The multigroup function is an available, user option feature of the system.

4. Recommended Protocol / Standard

If an agency does not "own" the talkgroup it wishes to place within a multigroup, the agency must first obtain the permission of the owning agency.

Agencies must share multigroup information while fleetmaps are being planned and programmed into the system and subscriber radios. In addition to operational planning, this information is necessary to ensure that users are aware of the multigroup resource.

If an agency shares the multigroup or the associated talkgroups contained within a multigroup with other agencies, the owning agency shall be responsible for informing the sharing agency of the operational properties and guidelines for use of the multigroup. In the event the central radio monitoring point is not the same agency as the radio user, an agreement on policy, monitoring, use, and response, must be in place among the agencies.

- Information must be shared about the purpose and guidelines for use of the multigroup and interrupt mode, if active talkgroup calls will be terminated (ruthless preemption), if the multigroup will wait until the talkgroup calls conclude, and any other operational information as needed.
- Multigroups may only be used for owned or shared talkgroups. Multigroups may not be used with regional interoperability resources (i.e., talkgroups/channels) as detailed in Section 3, "Interoperability Standards."

5. Recommended Procedure

Recommended procedures will be handled by the individual agencies as part of their fleetmap process.

6. Management

The System Administrators of the shared multigroup resource shall be responsible for managing their multigroups must be approved by the Subsystem Administrator.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Talkgroup and Radio User Priority**		Date Created:		**05-08-2018**	
Standard Policy #	**3.10.0**	**Standard Title:**	**Configuration and Allocation**		Status	**Completed**
Approval Authority:	**ISICSB**		Adopted:	**06-12-2018**	Reviewed:	**06-12-2018**

1. Purpose or Objective

The purpose of this standard is to establish varying priority levels for talkgroups. This will ensure the most critical talkgroups on the system are granted a channel as quickly as possible when the system is experiencing busy conditions.

2. Technical Background

Capabilities

The system priorities can be managed at the user level and at the talkgroup level.

Constraints

All User Priorities will be set to 10. As radio users change talkgroups, their effective priority will be set by the talkgroup they are on.

3. Operational Context

Priority levels in the system will be managed at the talkgroup level. The goal is to distribute priorities across the system's talkgroups in a way that maximizes the ability for critical groups to communicate and minimizes the number of talkgroups with high priority. All User Priorities will be set to the lowest priority level, which is 10. As radio users change talkgroups, their effective priority will be set by the talkgroup that they are on.

4. Recommended Protocol/ Standard

The appropriate System Administrator shall assign talkgroup priority levels, not exceeding the level defined by the criteria below. All talkgroup priorities are subject to the review and audit provisions that are specified in State Standards Section 1, Management of System.

Priority 1
[Definition: Emergency]
Priority 1 will be used only for Emergency Alert calls, i.e., calls where the emergency button is pressed will be given Priority 1 status.

Priority 2
[Definition: Extraordinary/Temporary, Console Tactical Upgrade for Priority 3]
Priority 2 will be used for temporary reprioritization (via System Manager Terminal) of a lower priority talkgroup for critical operations, i.e., presidential motorcade, major incident command, etc. From a dispatch console position, a Priority 3 talkgroup can be upgraded to priority 2 by a dispatcher switching the "access priority" icon in the talkgroup window from "normal" to "tactical." In addition, Priority 2 will be assigned to dedicated "EMERGENCY ALARM" talkgroups for agencies that do not use the Emergency Alert (Emergency Button) function.

Priority 3
[Definition: Shared Talkgroups normally dealing with Mutual Aid]
Priority 3 will be used for public safety mission-critical announcement groups (multi-groups), network wide and local system wide mutual aid interoperability talkgroups, i.e., regional tactical talkgroups, STAC's.

Priority 4
[Definition: Console Tactical Upgrade for Priority 5]
A priority 5 talkgroup can be upgraded to priority 4 by a dispatcher switching the "access priority" icon in the talkgroup window from "normal" to "tactical."

Priority 5
[Definition: Talkgroups dealing with the Safety and Protection of Life and Property]
Priority 5 will be used for talkgroups that have an impact on the delivery of services involving the safety and protection of life and property. Priority 5 talkgroups may also include those talkgroups used by personnel involved in high-risk and mission-critical field operations, i.e., law enforcement, fire, and EMS mains.

Priority 6
[Definition: Temporary Console Tactical Upgrade for Non-Mission Critical]
A priority 7 talkgroup can be upgraded to priority 6 by a dispatcher switching the "access priority" icon in the talkgroup window from "normal" to "tactical."

Priority 7
[Definition: Non-Mission Critical]
Priority 7 will be used for all other "secondary", "administrative", "nonessential", or "non-mission critical" talkgroups used by subscriber agencies, both public safety and general government, i.e., public works.

Priority 8
[Definition: Temporary Console Tactical Upgrade for Non-Mission Critical]
A priority 9 talkgroup can be upgraded to priority 8 by a dispatcher switching the "access priority" icon in the talkgroup window from "normal" to "tactical."

Priority 9
(Definition: Non-Mission-Critical Low Priority Secondary Talkgroups)
Priority 9 will be used at the System Administrator's discretion for non-mission-critical low priority talkgroups. Training activities and educational facilities typically use this priority for training and educational purposes, as specified in their respective user agreement.

Priority 10
[Definition: Private and Interconnect Calls]
Priority 10 will be used for telephone interconnect calls or private calls, as defined by direct point-to-point, radio-to-radio communications that are not carried out within a talkgroup. This priority will also be used for talkgroups that are established for system testing.

5. Recommended Procedure

The Statewide System Administrator and Subsystem Administrators shall follow the outlined priority levels when creating or modifying talkgroups in ISICS.

6. Management

The Statewide System Administrator is responsible for supervision and management of this procedure.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Talkgroup Site Access and Roaming**		Date Created:		**05-08-2018**	
Standard Policy #	**3.11.0**	**Section Title:**	**Configuration and Allocation**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	7/12/18

1. Purpose or Objective

This standard establishes a policy for system and subscriber unit programming to provide ISICS users with wide area access, as needed, while minimizing roaming and preventing unnecessary system loading.

2. Technical Background

Capabilities

The ISICS platform and subscriber radios may be programmed to allow a talkgroup or radio to affiliate with all ISICS repeater sites and to roam between them or to restrict a talkgroup or radio from specific repeater sites.

Constraints

Each ISICS repeater site has a limited number of channels able to provide talk paths available to carry radio transmissions. If care is not taken to program talkgroups and radios to be allowed only on certain sites or prefer certain sites, radio traffic could unnecessarily overburden a site preventing some radio messages from being sent.

With respect to operable talkgroup site access, this standard only applies to state-owned tower sites. Local Sub-System Administrators who desire operable talkgroup access to other local sub-systems need to complete a Memorandum of Agreement between Sub-System Administrators/Owners.

Interoperable talkgroups shall be allowed access to local Sub-Systems.

3. Operational Context

Radio users may not have control over where their public safety responsibilities take them nor do they have the ability to control to which repeater sites their radios affiliate. Site affiliation permission must be proactively managed by sound system and radio programming guidelines. Not all scenarios can be defined by standard so system administrators should communally develop and share best practices.

4. Recommended Protocol/ Standard

Site Access Profiles define talkgroup access to ISICS repeater sites. They serve as the preferred tool for managing repeater site access. The following Site Access Profiles are established:

- In-County/Geopolitical Subdivision Operations: Includes all sites within a county or geopolitical subdivision and may include sites outside of the physical boundaries of the county or geopolitical subdivision but engineered to serve the county or geopolitical subdivision.
- Border (aka Adjacent Site): Includes all sites included in the In-County/Geopolitical Subdivision Operations profile plus one ring of adjacent repeater sites encircling the In-County/Geopolitical Subdivision Operations profile.
- Regional Sites: Includes all sites within a Homeland Security Region plus one ring of sites encircling the Regional Sites profile.
- Statewide Sites: Includes all ISICS sites.
- Custom Sites: Certain entities with atypical geographic boundaries may require a custom Site Access Profile. These profiles must be approved by the impacted site's owner and the Operations Committee.
- Requested Site: profiles will always broadcast specified radio traffic regardless of site affiliation with the repeater site. Example: A rural county relies on another county's repeater sites for coverage in a border area and car-to-car traffic (utilizing an In-County Operations profile) is not carried through that neighboring county's repeater. Requested Site profiles must be approved and documented by the neighboring site's owner and the Operations Committee.

Deviations from these Site Access Profiles must be approved in writing by the site owner(s). Ownership is defined as who owns the physical site and who purchased RF channels found on that site. In the case of state-owned sites, Operations Committee will review the deviation and recommend action to ISICSB for final approval.

The following Site Preference procedures are established to define individual radio access to ISICS repeater sites.

- Generally, talkgroup personalities should not have special site access permissions as site access should primarily be managed by talkgroup properties as established in the system.
- Generally, talkgroup personalities should be set to prefer the home infrastructure of the radio owner over that of non-home infrastructure.
- Generally, talkgroups with wide area access (e.g. statewide) should be set not to prefer one repeater site over another.

Deviations from these Site Preferences must be approved in writing by the impacted site owner(s). Ownership is defined as who owns the physical site and who purchase RF channels found on that site. In the case of state-owned sites, Operations Committee will review the deviation and recommend action to ISICSB for final approval.

The following is a Prohibited Action:

- Selecting a talkgroup (by choosing it as the transmit channel on a radio) for which one has no reasonable need to monitor (as defined by the impacted system administrator) is known as "parking on a talkgroup" and is prohibited. This does not prohibit one from including a talkgroup in a scan list while the radio is legitimately affiliated to another talkgroup.

Exceptions to any item in this standard should be decided on a case-by-case basis by either the Operations Committee or the Technology Committee and are subject to the ISICSB approval.

Emergency exceptions to this standard or emergency resolutions of site access issues may be temporarily authorized by agreement between a Subsystem Administrator and the Chair of ISICSB or the Chair of the Operations Committee (if the ISICSB Vice Chair is not available). Temporary authorization may exist until the next meeting of the Operations Committee or sixty days, no longer.

5. Recommended Procedure

Subsystem Administrators are responsible for ensuring that radios and infrastructure under their control comply with this standard.

6. Management

The Statewide System Administrator is expected to manage and enforce this standard. Conflicts should be handled through the Compliance and Conflict Resolution processes

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Computer Aided Dispatch and Air Traffic Information Access Connectivity**		Date Created:		**03-27-2018**	
Standard Policy #	**3.12.0**	Section Title**:**	**Configuration and Allocation**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**10/11/18**	Reviewed:	**10/11/18**

1. Purpose or Objective

The purpose of this standard is to establish policy and procedures for systems requiring connectivity to ISICS, such as:

- Computer Aided Dispatch (CAD) systems
- Logging systems requiring Air Traffic Information Access (ATIA)
- Reporting and monitoring systems requiring ATIA

2. Technical Background

Capabilities

There are two CAD connection methods available by this standard. Each method has unique capabilities and levels of impact to the system:

- ATIA (Air Traffic Information Access)
- API (Application Programming Interface)

ATIA (Air Traffic Information Access)

Installation: The individual ISICS ATIA interfaces are at the zones, and multiple zones can be combined to a system level interface, depending on the vendor capabilities. A single installation is used to support all entities.

Impact: The impact and level on control is read-only of data contained in the ATIA stream. There is no control, access, or edit capability of system resources through the ATIA interface.

Typical uses: CAD, system usage reports, live system monitoring, data for audio logging.

Architecture: The ATIA interfaces can be licensed and enabled on each zone of the ISICS system; the individual zone ATIA interfaces will be individually firewalled to protect the ISICS system.

The ATIA feeds then pass on to a system level data collection repository and access point.

Individual agency connections to the repository will be individually firewalled to protect the repository and agencies from each other.

The individual network extensions for the ATIA information are considered extensions of ISICS and are subject to the standards defined for the ISICS platform.

API (Application Programming Interface)

Installation: At the Dispatch location and is used to support the needs of the local dispatch operation.

Impact: Control of local console functions – calls, paging Alias Database Management, etc.

Typical uses: Computer Aided Dispatch (CAD)

Architecture: Installation is at the local dispatch center

Constraints

Direct connections to ISICS add an inherent risk to the system. The risk is minimized as much as possible by the steps within this standard, while still making the connection capabilities available.

Servers in the ISICS platform support entire zones rather than individual dispatch agencies, and the servers have the subscriber alias replication to them from the Zone "ZDS" database. The agency connection plan must reference the impact to those servers.

3. Operational Context

The interface subsystem will be owned and managed by the individual agency.

4. Standardized Policy

The requesting agency will be responsible for determining which of the two connection methods meet their needs:

- ATIA (Air Traffic Information Access)
- API (Application Programming Interface)

The requesting agency will be responsible for providing a plan that shows their design and/or connection requirements.

The individual agency will be responsible for the financial costs of their connection to the system.

5. Recommended Procedure

Requests and/or plans for CAD connections to the ISICS system are reviewed by the Statewide System Administrator for recommendation to the Operation Committee.

The agency plan will include written, technical advisements from Motorola and the CAD product vendor, indicating system impact and potential issues to the system.

Interfaces to the system must be either:

- Non-Internet Protocol (IP), such as command and control RS232 links or equivalent.
- Isolated networks with equivalent standards on security and network isolation.

If the agency interface generates a failure impact for ISICS, the agency will be notified by the Statewide System Administrator that their interface will be taken offline until the problem is resolved.

Due to the tight integration of the API interface with the system, it should be expected that the individual agency will have Motorola technical staff involved in the API connection design.

6. Management

This standard is governed by the Iowa Statewide Interoperable Communications System Board (ISICSB).

Individual connection requests will be reviewed by the Statewide System Administrator for recommendation to the Operations Committee.

The interfaced subsystem will be owned and managed by the individual agency.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Status Message Transmission**		Date Created:		**06-07-2018**	
Standard Policy #	**3.13.0**	**Section Title:**	**Configuration and Allocation**		Status	**Approved**
Approval Authority:	**ISICSB**		Adopted:	**11-08-2018**	Reviewed:	**11-08-2018**

1. Purpose or Objective

The purpose of this standard is to specify that status messaging is an available feature of the system.

2. Technical Background

- **Capabilities**

The status message feature does not consume system Radio Frequency (RF) resources; the information is sent to the system by using the control channel of the RF subsystem.

There is not an appreciable limit to the number of sets of status sets that may be programmed into the system; this does not become a factor in planning the usage of the resource.

Mobile radios may have an optional Direct Entry Keyboard (DEK) that can be purchased, which allows for one-touch status messaging. Without this, messages are selected and sent by using the menus within the radios.

Status messaging can be interfaced with Computer Aided Dispatch (CAD) systems.

- **Constraints**

To use this feature, the Radio Control Manager (RCM) application provided by the ISICS Platform vendor must be purchased, licensed, and installed on the console operator positions that are going to be receiving the status messages.

3. Operational Context

This is an available feature of the system. The Subsystem Administrators shall be responsible for configuring and managing this feature for their respective users.

4. Recommended Protocol/ Standard

N/A

5. Recommended Procedure

N/A

6. Management

The local Subsystem Administrators in coordination with the System Administrator shall be responsible for configuring and managing this feature for their respective users.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Outage Responsibility**		Date Created:		**4-17-2018**	
Standard Policy #	**4.1.0**	**Standard Title:**	**Maintenance**		Status	**Approved**
Approval Authority:	**ISICSB**		Adopted:	**05-10-2018**	Reviewed:	**05-10-2018**

1. Purpose or Objective

The purpose of this standard is to define the system outage responsibilities.

2. Technical Background

Capabilities

The System Administrators have the responsibility for identifying an outage situation and determining the course of action for resolution.

Constraints

There are too many unknowns to define an actual recovery time period for an outage; parameters may easily be beyond the control of the system support staff.

3. Operational Context

System Administrator, Subsystem Administrators or designee are responsible for the portions of the system they oversee status for both planned and unplanned (emergency outages) will be updated as available on the StatusBoard.

4. Recommended Protocol / Standard

This process is initiated when there is a notification of system impairment.

If an owner's system supports other subscribing agencies, that owner shall be responsible for monitoring the system on a 24-hour basis, whether by on-site personnel or an automated electronic monitoring and notification process.

If the system impairment does not impact other subscribing agencies of the system, the resolution process will be at the discretion of the responsible agency.

5. Recommended Procedure

Upon notification of an equipment outage, the Subsystem Administrator is responsible for the impaired portion of the system will be expected to:

- Determine the impact of the impairment to the operation of the system. A minor failure is something that either does not affect, or minimally affects, user functionality. A major failure is something that seriously affects or risks user functionality of the system.
- Determine if there are internal or external factors that may alter the priority of a system impairment, such as weather, subscriber loading, unique public safety activities, impending events, etc.
- Determine if manual intervention is required. A serious failure would require initiating repair processes regardless of the time of day, and a minor failure may wait until business hours before repair. The determination is at the Subsystem Administrator's discretion and would be based on internal system functionality and external subscriber needs.
- Determine if additional external resources are required.
- Make an entry in the system log detailing the impairment.
- Use the notification process as defined in notification-related standards.

If requested by any of the Subsystem Administrators, the details of recovery process may be reviewed by Statewide System Administrators for possible improvements to outage recovery processes.

6. Management

The individual System Administrator, Subsystem Administrators or designee are responsible for managing system and subsystem outages.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Agency Maintenance**		Date Created:		**11-03-2017**	
Standard Policy #	**4.2.0**	**Section Title:**	**Maintenance**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	7/12/18

1. Purpose or Objective

The purpose of this standard is to define the maintenance responsibilities and roles of the ISICS system and sub-system administrators. The maintenance levels for the ISICS system and subsystems must be set to a standard to protect the overall functionality and integrity of the system for all users. A proper maintenance standard will also protect the warranties of the system and subsystems.

2. Technical Background

Capabilities

Standards in maintenance protect the integrity of the system and protect the warranties of the sites and equipment. Coordinated maintenance is simplified by having one set of maintenance standards, especially at shared sites.

Constraints

Improper maintenance not only poses a risk to the operational functionality of the ISICS system and subsystems, but it could also risk equipment warranties and potentially cause confusion at shared sites.

3. Operational Context

Each site and each piece of equipment shall be considered "owned" by one of the appropriate owners of the system or sub-system. The individual owners will then be responsible for the maintenance of the sites and equipment they own. Agreements between the owners and/or maintenance contractors are at each agency's discretion, but the owner is ultimately responsible for their portion of the system.

Maintenance of the system and subsystems falls under one of two categories:

- Day-to-day routine: For general day-to-day maintenance activities
- Emergency and urgent repairs: Serious system and subsystem impairment which may cause an unacceptable loss of service to the users of the system

4. Recommended Protocol/ Standard

N/A

5. Recommended Procedure

Any broad maintenance issues that affect multiple owner agencies should be discussed and resolved among System and Sub-System Administrators.

For day-to-day maintenance, individual agencies or contractors will maintain equipment they are responsible for.

For emergency and urgent repairs, the owning agency may request and expect reasonable cooperation in support resources (i.e., support staff and/or parts) from other System Administrators to restore equipment or the system to normal operation.

Repair of any equipment not owned by an agency requires notification and consent of the responsible System and/or Sub-System Administrator of the owning agency.

System and/or Subsystem Administrators/Owners or their contracted service providers will be responsible for:

- Providing primary and alternate contact information for local ISICS support
- Notifying the responsible agency of equipment and location issues that require attention.
- Notification of impacting maintenance that will be taking place.
- Managing the inventory of the equipment that they are responsible for, as defined by their internal department inventory processes.
- Making sure equipment at shared sites is clearly labeled to indicate agency ownership.
- Managing the equipment maintenance logs.
- Posting Federal Aviation Administration (FAA) and Federal Communications Commission (FCC) licenses or reference to the location of the licenses at the sites.
- Posting service technician information at the sites.
- Keeping routine equipment maintenance logs at the sites.

The Statewide System Administrator will be responsible for maintaining a system event log.

- All maintenance work being scheduled that may affect the system and/or subsystem's performance shall be preceded by reasonable notification to the other Local System Administrators.
- The Sub-System Administrators shall ensure that all technicians assigned to work on system equipment have successfully completed appropriate training on that equipment. The Statewide System Administrator may review training records as needed. Training requirements are referenced in the training section of the standards manual.

- Following a preventive maintenance plan, as defined in the Preventative Maintenance section of the standards manual.
- Each Sub-System Administrator will maintain a list of qualifications and contact information of their technical staff.
- Each System and Sub-System Administrator will maintain a list of the system and subsystem spare parts / equipment they have available. This provides other System and other Sub-System Administrators the option to request use of this spare equipment. The borrowing agency is responsible for returning the original spare parts / equipment, or, at the lending agency's discretion, the successfully tested replacement component.
- Any infrastructure hardware and software upgrades or changes that may have an impact on the system will need reasonable discussion and approval by the Statewide System Administrator.

The Sub-System Administrator for the impaired system and subsystem will determine how critical an equipment failure is operationally, determine the appropriate action, and escalate or de-escalate the repair process as needed. For example, a single failed channel on a main simulcast cell would not be a critical failure, but a simulcast cell failure would be

6. Management

The Sub-System Administrators are responsible for managing maintenance of the equipment and sites they are responsible for, as well as managing emergency repair situations.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Preventative Maintenance**		Date Created:		**11-03-2017**	
Standard Policy #	**4.3.0**	**Section Title:**	**Maintenance**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	7/12/18

1. Purpose or Objective

The ISICS system is owned and managed by multiple servicing entities, so a failure of any portion may easily impact users beyond the failed portion of the system. For example, failure of a backup power system at certain sites during a power loss may have a serious impact on the rest of the system. The maintenance levels for the ISICS system and subsystems must be set to a required standard to protect the functionality of the system overall for users of the system. A proper maintenance standard will also protect the warranties of the system and subsystems.

2. Technical Background

Capabilities

Standards in preventative maintenance protect the integrity of the system and protect the warranties of the sites and equipment. Coordinated maintenance is simplified by having one set of maintenance standards, especially at shared sites.

Constraints

Improper preventative maintenance not only poses a risk to the operational functionality of the ISICS system and subsystems, but it could also risk equipment warranties and cause confusion at shared sites.

3. Operational Context

Each site and each piece of equipment shall be considered “owned” by one of the appropriate owners of the system or sub-system. The individual owners would then be responsible for the maintenance of the sites and equipment they own. Agreements between the owners and/or

maintenance contractors are at each agency's discretion, but the owner is ultimately responsible for their portion of the system.

4. Recommended Protocol/ Standard

Sub-System Administrators/Owners or their contracted service providers shall be responsible for:

- Monitoring the performance of their subsystem equipment using the monitoring and reporting tools that are part of the subsystem. If issues do arise, it shall be the agency's responsibility to resolve the problem directly or bring the issue to the Statewide System Administrator if a broader resolution is needed.
- Ensuring that Federal Communications Commission (FCC) and Federal Aviation Administration (FAA) Rules and Regulations are followed.
- Ensuring that spare modules, boards, and field replaceable units for the agency's equipment are properly inventoried and maintained.
- Immediate notification of the appropriate System and/or Sub-System Administrator when there is a preventative maintenance issue that may impact other portions of the system.
- Ensuring that battery maintenance and replacement plans will be in place.
- Managing/keeping contracts current for maintenance service and support.

Periodic site inspections will be performed to find or prevent problems. Site inspections include:

- Power system testing and maintenance
- Shelter inspection
- Tower inspection
- Equipment inspection

5. Recommended Procedure

Preventative maintenance shall be performed. Appendix E is provided as a guideline for the development of a maintenance program.

6. Management

The System and Sub-System Administrators are responsible for managing the maintenance of the equipment and sites they are responsible for.

1. Purpose or Objective

The purpose of this Appendix is to provide a guide for the development of preventive maintenance programs for participants of the ISICS System.

PREVENTIVE MAINTENANCE CHECKLIST			
Agency Location:			
	Due Date	Completed Date	Completed By (Name & Agency)
Compound			
Driveway-Gate-Fence			
Function of locks			
Function of gate			
Driveway accessibility			
Signage intact			
Inspect fence-line: holes, loose barb wire			
Site			
Snow cleared			
Grass mowed and weeds chopped, treated and controlled			
Trash cleaned up			
Tower (visual inspection)			
Guy wires			
Antennas intact			
General appearance			
Feedlines Secure			
Tower lights functioning			
Paint Condition			
Fuel Tank (LPG or Diesel)			
Visual Inspection			
Fuel Line Condition / Regulator(s) operational			
Fuel Level			
Building			
Vandalism			
Building Condition			
Foundation Inspection (Building, Tower, Pads)			

APPENDIX E – PREVENTIVE MAINTENANCE CHECKLIST

Outside light working-intact			
Grounding wires intact			
Signage intact			
Clean intake air vents			
Intake vents – Louvers Adjusted / Operating Properly			
Entry doors and locks functioning			
Generator (Outside)			
Oil Level			
Coolant Level / Test			
Battery Fluid Level			
Battery Voltage			
Block Heater operational			
General Appearance – check for leaks			
Maintenance Comments current			
Inside Building			
Generator (Inside)			
Oil Level			
Coolant Level / Test			
Battery Fluid Level			
Battery Voltage			
Block Heater operational			
General Appearance – check for leaks			
Maintenance Comments current			
Automatic Transfer Switch			
General appearance of Transfer Switch (open door inspection)			
Generator Test (Load/No Load) {Close ATS Door First!}			
Fill out Log sheet			
Transmitter Area			
Temperature			
Smell – electrical / burnt			
Feedline Entry Panel Inspection			

APPENDIX E – PREVENTIVE MAINTENANCE CHECKLIST

Pressure gauge for antenna lines			
Update site log			
Battery rack for corrosion			
AC surge protectors green or black			
HVAC filters			
HVAC – Operational Test - Cooling			
HVAC – Operational Test - Heating			
Alarm system test			
Power Supplies / Batteries			
UPS Operational / Test			
Clean / Dust Building & Equipment			
Site Log Files			
Tech Data Sheets			
FCC Licenses Current			
FAA Logs Current			
RF Equip Logs Current			
Annual Maintenance			
Tightness of coax jumpers			
Sweep antenna lines			
Grounding system – conductance test			
EME Log Verification			
Fire Extinguisher			
Eye Wash Stations			
Safety Supplies Restocking			

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Record Keeping Requirements**		Date Created:		**11-08-2017**	
Standard Policy #	**4.4.0**	**Section Title:**	**Maintenance**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	7/12/18

1. Purpose or Objective

The purpose of this standard is to define the record keeping requirements of the ISICS system.

2. Technical Background

Capabilities

Proper record keeping will facilitate the maintenance and support of the system.

Constraints

System records are subject to audits.

3. Operational Context

The following records shall be maintained by the agencies responsible for supporting the system. They shall also be kept readily available for support staff responsible for managing and maintaining the system and subsystem:

- System standards manual
- System documentation & technical procedure manuals
- Current system and equipment as built documentation, as defined in State Standard 4.6.0
- Agency specific policy and procedure manuals
- Equipment manuals
- Contact information, as defined in State Standard 4.4.0
- Preventative maintenance logs, as defined in State Standard 4.2.0
- A common system event log containing issues, status, resolution, and involved equipment
- FCC required station logs and FAA required tower light logs

- System fleetmap configuration

The specifics of the documentation kept by supporting agencies are at the individual agency's discretion.

4. Recommended Protocol/ Standard

- N/A

5. Recommended Procedure

Materials identified under Operational Context shall be made available to support staff and anyone else who needs access to it. The individual Sub-System Administrators will ensure that document materials are current.

Sub-System Administrators will be responsible for running system performance reports relative to problems or issues that need resolution and save the reports until the issue is clearly resolved.

The Statewide System Administrator will be responsible for archiving and storing common information shared between Sub-System Administrators from a client workstation at Zone Controllers within the region. This information will be stored at both onsite and offsite locations.

6. Management

System Administrators and supporting agencies are responsible for managing the record keeping.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Contact Information Procedures**		Date Created:		**11-08-2017**	
Standard Policy #	**4.5.0**	**Section Title:**	**Maintenance**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**7/12/18**	Reviewed:	7/12/18

1. Purpose or Objective

The purpose of this standard is to define the procedure and process for maintaining contact information for internal and external staff responsible for the support of the ISICS system and distribution of the contact information in a secure fashion.

2. Technical Background

Capabilities

Having the contact information readily available to the system support staff will facilitate:

- General purpose day-to-day communications
- Source information for distribution lists
- Notification of the responsible agencies for equipment / location issues
- Contacting support staff in the event of a system failure / on-call duty
- Having a clear list of vendor support contacts
- Facilitating the information electronically / centrally eliminates duplication of effort

Constraints

The contact information must be kept up-to-date and be distributed to support staff that uses the ISICS system.

Contact information should not be released to the public or media so there is no compromise of support staff safety.

3. Operational Context

The Sub-System Administrators shall maintain support staff's current contact information within the ISICS network through client workstations.

The contact list shall contain information such as:

- Internal support staff, System and Sub-System Administrators, technicians, etc.
- External support staff, subcontractors, equipment providers, etc.
- Dispatch centers of the system
- Building security contact list

The Statewide System Administrator shall be responsible for the functionality of the contact information sharing resource and for performing backups and archives of the contact information.

The contact information shall also be kept available in hardcopy format for the System and Sub-System Administrators and Iowa Statewide Interoperable Communications System Board (ISICSB).

4. Recommended Protocol/ Standard

The usage of a central electronic resource that can be shared between the System and Sub-System Administrators shall be used to record the contact information. The details of this resource are at the discretion of the Statewide System Administrator.

5. Recommended Procedure

The Sub-System Administrators shall maintain current contact information of their support staff in a central electronic resource within the ISICS network at the closest zone controller. The resource will be accessible and printable to the System and Sub-system Administrators through the client workstations on the system.

The contact information to be saved will include such things as:

- Agency
- Functional role
- Work address
- Contact phone numbers (work, home, pager, cell) at the support person's discretion
- Email address
- Radio ID, if assigned

Any changes shall be sent to the Statewide System Administrator for updating the shared information. The Statewide System Administrator shall then send out notification about the updated contact list.

6. Management

The Statewide System Administrator shall be responsible for this process, and details are at the discretion of the Iowa Statewide Interoperable Communications System Board (ISICSB).

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**System Maintenance: Programming and Qualifications**		Date Created:		**06-19-2018**	
Standard Policy #	**4.6.0**	**Section Title:**	**Maintenance**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**8/9/18**	Reviewed	8/9/18

1. Purpose or Objective

The purpose of this standard is to establish minimum qualification requirements for system technical staff, both in-house and contracted. This will ensure that functionality and integrity is maintained by requiring system configuration, maintenance, and repair functions be performed by qualified personnel.

2. Technical Background

Capabilities

This standard protects the integrity of the system by ensuring training and background requirements of all personnel working on the system and by describing the authorized activities of a contract service provider who is to provide maintenance and programming services.

Constraints

Some sensitive and non-public system security information will be available to businesses and people operating outside of the ISICS platform. Standards and agreements are necessary to ensure the appropriateness of the businesses' activities and protect the integrity of the system. Programming information falls under non-public, confidential records according to Iowa Code 22.7(50).

3. Operational Context

System functionality and integrity must be maintained by ensuring that only qualified personnel perform system configuration, maintenance, and repair functions. Not all user agencies participating in the statewide system have technicians on staff to program and perform

configuration, maintenance, and repair on radios and other electronic infrastructure. Agencies may need to contract with one or more service providers for these services at agency's expense. The choice of service provider is at the discretion of the user agency, but the contract service provider must enter into an agreement with the user agency. The user agency must ensure the requirements of this standard are met prior to and are responsible for execution of the service.

4. Recommended Protocol/ Standard

ISICS Standard 2.10.0 (Training Technical Staff) details training requirements for performing maintenance on equipment.

System Owners' Internal Technical Staff

- Employed technical staff of owning agencies will follow the same or an equivalent internal process of ensuring absence of criminal history, as outlined below in the Contract Service Providers section. The minimum standard for criminal history checks will include but may not be limited to the Interstate Identification Index (III). Other screening and/or training may also be required. If Criminal Justice Information (CJI) protected data will be within viewable or audible range of any technical staff, appropriate screening and training must be completed.
- Employed technical staff of owning agencies will follow the same process of ensuring technical competency, as outline below in the Technical Staff Requirements (Internal and External) section.
- Sub-system administrators shall maintain a list of technical training completed by internal technical staff.
- Compliance with this standard will be subject to audit.

Contract Service Providers

User agencies may contract radio programming and system infrastructure work provided the following requirements are met:

- A service shop must prove it is a qualified service center eligible to conduct business in the State of Iowa.
- A service shop must provide an insurance certificate and may, prior to commencement of work, be asked to purchase a security bond by the user agency.
- When a user agency contracts with a contract service provider for the purpose of providing maintenance, repair, programming, and related service on electronic infrastructure to include dispatch consoles and/or radio subscriber equipment, the service provider must obtain and pay for all permits, licenses, and approvals necessary for programming and maintenance to fulfill the provisions.
- Due to the sensitive and non-public nature of the programming information, the contract service provider must provide written assurance to the System Administrator and if necessary Sub-system Administrator that it is authorized and has all necessary permits and licenses to conduct business in the State of Iowa. Unless specifically authorized by the System Administrator and user, in writing and on an individual radio-by-radio basis, the

contract service provider may not directly or indirectly permit any unauthorized third party to view, read, print, extract, copy, transmit, archive, edit, create, clone, transfer, release, tamper with, reverse engineer, or otherwise compromise key file, or any infrastructure configuration database file for any radio, console, or other infrastructure element on the system.

- The contract service shop must provide references as requested by user agencies. The System Administrator and/or the user agency may request to view the resume of any staff member of the contract service provider or to conduct background checks.
- The contracted technician must submit to a background check consistent with conditions outlined above in Section 4: *System Owners' Internal Technical Staff*. The contracting agency is responsible to ensure the background check has occurred.
- Contracting agencies shall use the contract service provider's technical staff in their certified areas of competency, as proven by vendor certification.
- The contract service provider shall maintain all training certifications for its personnel and provide copies of these certifications to System Administrators when requested.
- Contracting agencies may contract for services only for equipment they have jurisdiction over.
- Contracting agencies shall notify the appropriate Sub-System Administrator of any contract for services.

Technical Staff Requirements (Internal or External)

- The technical staff that is assigned to work on system and/or subsystem equipment shall successfully complete appropriate training on all equipment they are assigned to work on. This training will be completed prior to working on the equipment.
- The technician must have or possess satisfactory knowledge and experience in either the equipment being maintained or radio programming.
- Personnel who are not trained shall not perform configuration, maintenance, or repair work unless this work is performed under the direct supervision of trained and approved personnel.
- Technical staff shall stay up to date on current training and notify other sub-system administrators and the system administrator of any encountered problems and any resolutions.
- Technicians shall be familiar with applicable ISICS Standards.
- System and subsystem technical staff shall be familiar with site access procedures, equipment outage, and maintenance notification requirements of the ISICS Standards.
- Technical staff connecting to the radio network shall take reasonable efforts to maintain a clean computer that is free of malware and only used for work purposes. Technical staff shall follow all standards and best practices regarding security. Before they connect to the network, they shall work with the appropriate System Administrator to ensure they have the latest anti-malware protection on their computers, and the computers are free of malware.

5. Recommended Procedure

Agencies requiring contract services must enter into an agreement with the contractor providing service. The agreement will specify enforcement provision, including consequences of misuse and the release of non-public system security information consistent with Iowa Code 22.7(50).

6. Management

The Statewide System Administrator, the appropriate Subsystem Administrators, and the contracting agencies are responsible for managing and maintaining the agreement process.

The Statewide System Administrator will:

- Facilitate the development of and maintain the current version of the best practices for the internal and external technical staff.
- Maintain a list of the overview/best practices trainers for the internal and external technical staff.

Sub-System Administrators are responsible to ensure that:

- Minimum training requirements of in-house staff are met.
- Only qualified personnel perform system maintenance functions.
- System technicians are familiar with all applicable sections of the ISICS standards.

Contracting Agencies shall:

- Ensure that these system standards are adhered to when using contract services.
- Ensure that only qualified personnel perform system maintenance work.
- Notify the appropriate Sub-System Administrator when contracting for service.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Hospital Access**		Date Created:		**4-17-2018**	
Standard Policy #	**5.1.0**	**Standard Title:**	**System Access by Non-Governmental Organizations (NGO's)**		Status	**Approved**
Approval Authority:	**ISICSB**		Adopted:	**05-10-2018**	Reviewed:	**05-10-2018**

1. Purpose or Objective

The purpose of this standard is to establish a policy that provides for hospital security voice communications over the ISICS platform where such communications would benefit the emergency preparedness of the facility. This policy does not apply to Hospital/Emergency Medical Services (EMS) communications or Inter-hospital compact communications addressed elsewhere.

2. Policy Background

The Federal Department of Homeland Security (DHS) has identified hospitals as critical facilities in the event of a chemical and/or biological emergency. Two-way radio communications between persons inside the hospital and public safety personnel outside the building is a critical need when an emergency occurs. The Iowa Statewide Interoperable Communications System Board (ISICSB) is empowered to enter into system use agreements with eligible hospitals when such use is consistent with the protection of life and safety.

3. Operational Context

Hospital security personnel often work directly with public safety personnel who respond to fire and safety/security incidents at these facilities. Hospitals have the potential for some or all areas of the facility to be under quarantine at times to manage communicable disease outbreaks or other infectious disease processes. It is important that a solid means of communication exists for coordination of hospital personnel inside and public safety personnel outside the facility in such circumstances.

4. Recommended Protocol/ Standard

Licensed hospitals which operate an emergency department that is open to the general public 24 hours a day, seven days a week, may utilize the ISICS platform for communication with public safety personnel where such use is consistent with and supportive of the facility's Emergency Response Plan (ERP). Communications using the system shall be focused on protection of life and property, security, emergency situations, and emergency preparedness. Internal day-to-day communications for the purpose of operational, administrative support, or other non-emergency communication will not be allowed.

5. Recommended Procedure

Hospitals shall submit, for ISICSB approval, a plan which details the number and types of radios and number of talkgroups requested, how and by whom the talkgroups will be used, and how the use of the ISICS platform will interface with the hospital's Emergency Response Plan. Hospitals shall also include a copy of their Emergency Response Plan. Once approved, hospitals shall enter into a User Agreement with the ISICSB. Hospitals shall be responsible to coordinate use within their facility, as allowed by the User Agreement. Hospitals will agree to comply with the ISICSB State Standards and Standard Operating Procedures (SOPs) prior to use of the system. The User Agreement shall specify the maximum number of radios that may be owned by the hospital and activated on the system under this standard. The User Agreement shall also specify enforcement provisions, including consequences of misuse.

The talkgroups programmed in hospital radios under this policy shall be limited to those specified by the User Agreement: interoperability talkgroups authorized by the ISICS platform standards and/or public safety talkgroups that have been authorized by the respective agencies owning those talkgroups.

6. Management

An NGO participant seeking to access the ISICS platform shall follow the contracting entity guidelines illustrated in the flow chart found under State Standard, Regional Development and Responsible Entity.

Iowa Statewide Interoperable Communications System (ISICS)
Standards, Protocols, Procedures

Standard Name:	**Standards Compliance Process**		Date Created:		**06-19-2018**	
Standard Policy #	**7.1.0**	**Section Title:**	**Compliance & Conflict Resolution**		Status	**APPROVED**
Approval Authority:	**ISICSB**		Adopted:	**8/9/18**	Reviewed:	8/9/18

1. Purpose or Objective

The purpose of this standard is to describe the process by which users of ISICS will be evaluated to ensure compliance with the standards, policies, and procedures set forth by the Iowa Statewide Interoperable Communications System Board (ISICSB). Evaluations may be scheduled and/or non-scheduled.

2. Technical Background

Capabilities

Constraints

3. Operational Context

The ISICSB is charged with setting standards and determining protocols and procedures for the most efficient and effective operations between and among users of the ISICS platform.

The improper use of ISICS Platform resources can have minor to grave consequences. These standards, policies, and procedures have been set forth by teams consisting of radio users and managers to maximize service and to minimize potential negative consequences. Responsible management of this resource requires that compliance be evaluated.

4. Recommended Protocol/ Standard

The ISICSB Chair, System Administrator, the Operations Committee and the Technical Committee chairs, or Sub-System Administrators, may call for an evaluation in response to an event or incident that caused an outage or damage to or had the potential to cause an outage or

damage to users or resources of the ISICS Platform. Events and incidents may include evaluating outcomes that consistently show non-compliance.

5. Recommended Procedure

The results of the evaluation will be forwarded to the Standards Committee for review and possible counsel with the Governance Committee to determine which ISICS standard(s) the agency was in non-compliance.

The findings of this review will be forwarded to the ISICSB. With the available findings and evidence, the ISICSB shall review the case with appropriate entities and decide on an appropriate course of action for non-compliance.

6. Management

The ISICSB Chair, acting on behalf of the Iowa Statewide Interoperable Communications System Board, will manage this process.

Attachment 5: Documents published in 2018:

- **Technical Recommendation – ISICSB TR-2018-001** – *Programming Guide Technical Recommendation*
- **Technical Recommendation – ISICSB TR-2018-002** – *Multi-Key Equipped Subscriber Units*
- **White Paper –** Encryption Needs in Iowa

Technical Recommendation Regarding Programming Guide

ISICSB TR-2018-001

ISICSB Technology Committee

In 2017, the Iowa Statewide Interoperability Communication Systems Board (ISICSB) Technology Committee formulated a Subscriber Unit Programming Guide. This document could be used to store all pertinent technical information that approved ISICS users may need to reference to when entering information into subscribers units. The information contained in this document would include, but would not be limited to, items such as frequency information, WACN IDs, system IDs and subscriber IDs.

Much time was spent researching the ways to bring to life a document that does not overwhelm the user with technical details. Various issues arose including issues of confidentiality, necessity of adding references to Iowa Code within the document, additional hierarchy references that could be associated with the document, who has access to the document, administrative rules among others.

Discussions drifted towards creating policy that would address the aforementioned concerns and the Subscriber Unit Programming Guide. After more research, it was discovered that recent amendments to Iowa Code negated the need for a policy that the ISICSB could or would need to approve or adopt.

With the ISICSB User Group Committee (UGC) and Standards Subcommittee already setting forth polices and agreements for users of the system, it did not seem necessary to spend more time pursuing any further processes. The Technology Committee has concluded that the Subscriber Unit Programming Guide is ready for adoption by the ISICSB.

The proposed ISICS Subscriber Unit Programming Guide is at a point where the necessary technical information can be readily entered into the document and is ready for use by ISICS Approved users.

The ISICS Subscriber Unit Programming Guide would be considered a living document in order to address future technical changes, and other hierarchy changes that may exist beyond the reference to Iowa Code. Those changes would be made as the ISICS Board would deem necessary.

To that end, the ISICS Technology Committee is recommending to the ISICS Board that the Subscriber Programming Guide be adopted as an official confidential document under Iowa Code 22.7(50).

Technical Recommendation for Multi-Key Equipped Subscriber Units

ISICSB TR-2018-002

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.

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 where 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

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

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 DES variants for local operability.

Iowa Statewide Interoperable Communications System Board

Thomas T. Lampe, Chair
Jason Leonard, Vice-chair
Chris Maiers, SWIC

Dear P25 User Needs Subcommittee Chair,

The Iowa Statewide Interoperable Communications System Board (ISICSB) is tasked under Iowa Code 80.28 and 80.29 to ensure that interoperable capabilities among all public safety and public service entities in Iowa is as robust as technically and procedurally possible. With the completion of the new P25 Phase II Iowa Statewide Interoperable Communications System (ISICS) nearing, the Encryption Subcommittee (ESC) was commissioned to examine the need and technical requirements of deploying encrypted interoperable talkgroups on a statewide LMR system.

The ESC began meeting in August of 2017 and has steadily worked through various aspects of the deployment, management and operational implications of AES-256 encrypted interoperable talkgroups. The working sessions included meetings with technical experts from TR-8, the Federal Partnership for Interoperable Communications, and stakeholders at the local, state and federal level. The ESC discovered several technical obstacles that would hinder effective management of the various key material and update cycles.

Given those results, the ESC has drafted a white paper (enclosed) outlining the need for effectively managed encrypted interoperability in Iowa, technical and logistical limitations of the current communications landscape in Iowa and proposed solutions for the obstacles. The proposed solutions would enhance interoperability and benefit the entire P25 user base on a local, state and federal level.

This letter is submitted as an official request for consideration of the proposed solutions outlined below and in the included white paper. We encourage the UNS to consider these solutions to be forwarded to the Project 25 Steering Committee for consideration to be forwarded to the Telecommunications Industry Association (TIA) TR8 Chair for consideration and assignment to the appropriate subcommittees for possible action within the current suite of P25 standards relating to encryption.

1. Standardization and adoption of over-the-ethernet keying (OTEK) and over-the-Internet keying (OTIK) that would allow for the loading and updating of TEKs and KEKs, setting initial and modifying management periods, ability to interface with multiple key management devices and ability for a Master KMF to create and modify partitions on a crypto module;
2. Adoption of the Inter-KMF Interface to allow for agencies with disparate KMFs to securely share encryption material;
3. Standardization adoption of methods for subscriber radios to communicate with multiple KMFs. This includes the ability to define the home system KMF as the Master KMF and the others as secondary KMFs. This would also create a pathway for aliased SLNs to add flexibility in programming and partitioning of the crypto module.

These topics are introduced for discussion and we realize further work will be needed before a formal recommendation is considered for approval, but we believe these solutions would enhance the interoperable capabilities of numerous agencies whose personnel must utilize multiple P25 LMR systems.

If you have any questions, please direct them to our statewide interoperability coordinator, Chris Maiers, via email at maiers@dps.state.ia.us or via phone 515-201-7478.

Very respectfully,

Lieutenant Tom Lampe
Iowa Department of Public Safety
ISICSB Chair

Captain Jason Leonard
Waverly Police Department
ISICSB Vice Chair

Patrick Updike
Iowa Department of Corrections
ISICSB Technology Committee Chair

ENCRYPTION NEEDS IN IOWA

ISICSB
Iowa Statewide Interoperable
Communications System Board

Table of Contents

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[1] and is governed by the Iowa Statewide Interoperable Communications System Board (ISICSB).[2] 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.

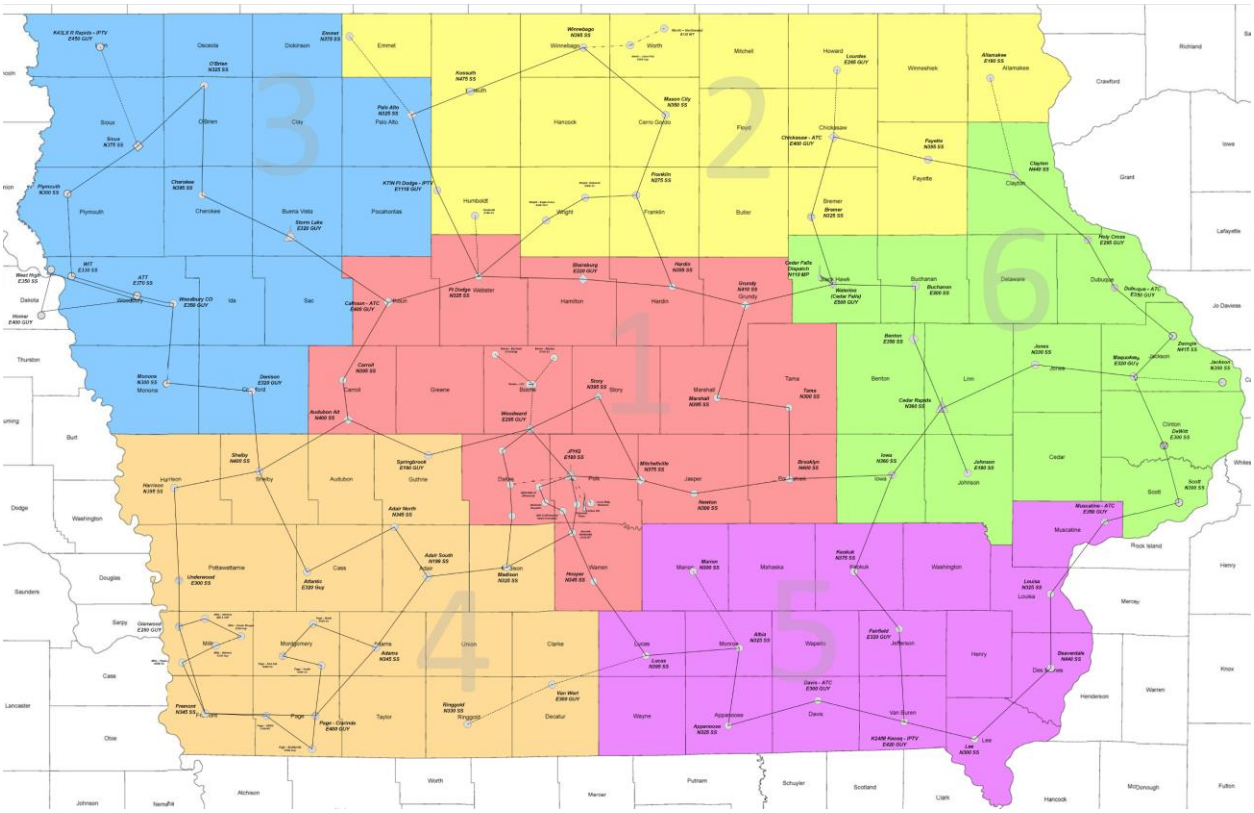


Figure 1. Layout of the ISICS Network with various Homeland Security Regions shaded.

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

[1] Iowa Code 29C.23.
[2] 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[3] that are tasked with enforcing laws in Iowa. In addition to law enforcement, 732 fire departments serve Iowa's 3,145,711 residents[4]. Of the fire departments, approximately 90% of the personnel are volunteer[5].

Iowa's population distribution has undergone an evolution over the past decade (Figure 2)[6]. 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.

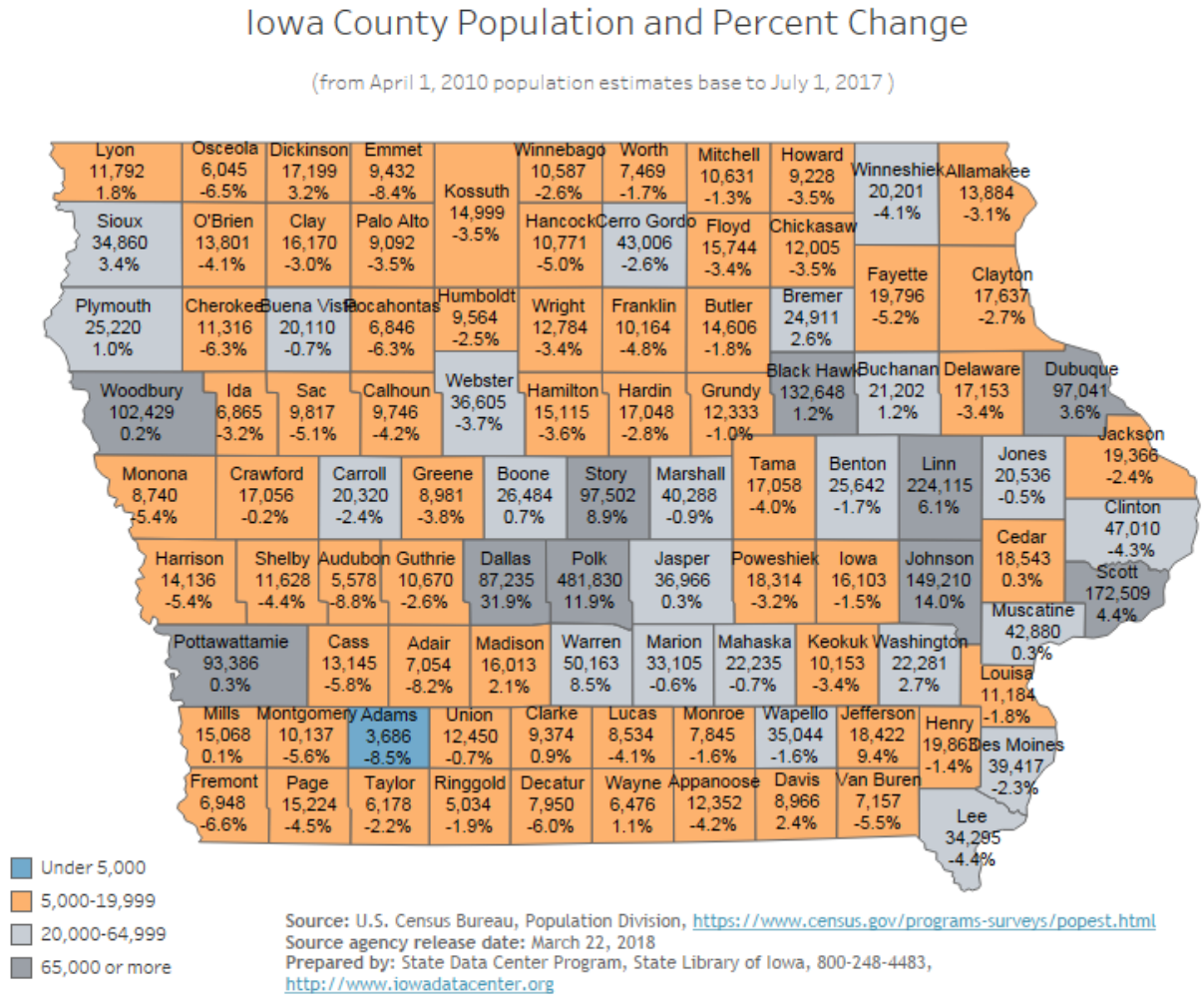


Figure 2. Iowa population and estimated population change map from April 1, 2010 to July 1, 2017.

[3] US Bureau of Justice Statistics' 2008 *Census of State and Local Law Enforcement Agencies*
[4] https://www.census.gov/quickfacts/fact/table/ia,US/PST045217
[5] https://apps.usfa.fema.gov/registry/summary#stateTotalsTable
[6] http://www.iowadatacenter.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[7].

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[8] through 2016[9], 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*[10] 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

[7] https://dom.iowa.gov/document/county-taxable-tif-valuations-class-ay2016fy2018
[8] http://www.dps.state.ia.us/commis/ucr/2010/iacrime_2010.shtml
[9] http://www.dps.state.ia.us/commis/ucr/2016/iacrime_2016.shtml
[10] https://isicsb.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[11] (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

[11] 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 crypo 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

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.

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 where 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

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

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 DES variants for local operability.