



**Report to the Iowa Legislature on the Status of the
Iowa Statewide Interoperable Communications System Board (ISICSB)
Calendar Year 2017**



Table of Contents

I. Overview 3

II. Key Definitions and Acronyms 4

III. Membership 6

IV. Communications Interoperability Efforts..... 7

V. ISICS Deployment 20

VI. Attachments for 2017 23

I. Overview

During the first session of the 82nd General Assembly, the Iowa Legislature established Iowa Statewide Interoperability Communications System Board (ISICSB). 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

II. 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
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
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 RF Subsystem 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
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

III. Membership

December 2017 ISICSB Members

Local Representatives

<u>Name</u>	<u>Position</u>	<u>City/Locale</u>
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.
Deb Krebill	Fire Department (Career)	Marion F.D.
Denise Pavlik	Communication Center Manager	Scott County
Andy Buffington	Communication Center Manager	Winnebago Co.
Robert Rotter	County Sheriff	Iowa County
Michael Kasper	County Sheriff	Linn County
Kelly Groskurth	Member-at-Large	City Clerk, Treynor
Larry Smith	Emergency Management	Keokuk County
Linda Frederiksen	Emergency Medical Services	Scott County

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 Wolfradt	Chief Information Officer
Jeffrey Sundholm	Department of Transportation

Legislative Ex-Officio Members

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

IV. Communications Interoperability Efforts

The ISICSB holds monthly public meetings, on the second Thursday of the month. The ISICSB posts information on a web site at www.isicsb.iowa.gov.

During 2017, ISICSB addressed legislative mandates, as contained in Iowa Code 80.29, as follows:

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

From its inception in 2007 through 2017, ISICSB relies on Federal Interoperability Grants and State appropriations to support Board activities.

- In State Fiscal Year (SFY) 2017, \$154,661 in state funding was appropriated to ISICSB. This was cut to \$115,661 for SFY2018.
- Each Board and committee member has a full-time professional position and performs Board duties on volunteer and part-time basis.
- As part of a national interoperability initiative, circa 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.
 - Craig Allen has been Iowa's SWIC from April 2014 through June 2017.
 - Chris Maiers started as full-time SWIC in May 2017.
 - The SWIC position is one of two employees of this Board.
 - In 2010 the Board hired their first SWIC.
 - 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 only FirstNet broadband duties.
 - Until 2014, SWIC salary was paid for by Federal Interoperability grants.
 - Starting in Federal Fiscal Year (FFY) 2015 and continuing through FFY 2016, 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),
 - 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 Nationwide Public Safety Broadband Network (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 and in August 2013 was awarded funds for a three (3) year period with the restriction that this grant can only be used for broadband planning activities, and not a SWIC's overall interoperability duties. In Iowa this grant partially supports the SWIC's salary. Therefore, it is essential that annualized 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 2017, SLIGP 2.0 was announced as a means to continue to fund public safety broadband initiatives across the nation. Iowa has applied for this grant. If awarded, the funds would continue to support ISICSB efforts to expand broadband interoperability in Iowa in addition to funding the SWIC's activities.
- 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.
- 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 (SMEs) round 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.
 - NPSBN directed each state to identify a state point of contact (SPOC) for NPSBN interactions. 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.
- On November 17, 2017, Governor Reynolds reappointed Thomas Lampe as SPOC for Iowa.

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 2018, 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.

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

The ISICSB and 911 Council coordinated their activities and scheduled meetings on the same dates and at the same locations.

During 2017 SWIC Allen and SWIC Maiers and 911 Program Manager Blake DeRouchey began meeting weekly to ensure alignment of objectives and coordination of efforts between ISICSB and 911 Council.

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.

- ISICSB management 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.
 - Board 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, and

- 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 channel interference created by other states in interoperability channels and ISICSB Technology Committee worked collaboratively with several local communities to identify solutions and implement resolution to the communication problems.
- Clearly, interoperability is still an issue in Iowa preventing coordinating communications much of the time in the incidents examined.
- Iowa's statewide communication platform called the Iowa Statewide Interoperable Communications System (ISICS) awarded for construction in 2015 and scheduled to be fully operational in 2018 will go a long way in solving Iowa's public safety interoperability challenges.
- Absent a completed statewide interoperable system like ISICS, it is very difficult to solve communication issues that counties and cities have in Iowa. The Board will continue to explore viable options and additional initiatives to improve interoperability in the coming year.

During 2017, ISICSB conducted a series of regional training workshops designed to improve interoperability, focusing on delivery of the Department of Homeland Security's (DHS) Communications Leader (COML) and Communications Technician (COMT) courses.

- Communications Technician (COMT) at Camp Dodge in Johnston on July 31, 2017 to August 4, 2017
- Incident Tactical Dispatch (INTD) at Oran Pape Building in Des Moines on November 13, 2017 to 16, 2017

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.

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 Allen and SWIC Maiers have voted on several P25 standards that facilitate and expand interoperability on radio networks such as ISICS. ISICSB Chair Thomas Lampe is also a member 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.

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, more channels are expected to be added to supplement the new ISICS suite of talk groups.

The ISICSB developed and published 'quick' one page templates and instructions for ease of use and programming channels into radio equipment.

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. 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 common frequency and statewide system.

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.

- ***Policy statements passed in 2014:***
 - ***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 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 posing 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 \$1.6 Million federal grant to plan future build-out of the Nationwide Public Safety Broadband Network (NPSBN) in Iowa. NPSBN is being undertaken by a new federal agency, FirstNet. NPSBN will be a national public safety grade, wireless broadband network. This grant is 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 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.

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, ISICSB's appropriation was reduced to \$115,661 to conduct State of Iowa interoperability matters not covered by federal grants.

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 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 funding (local match), 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 enters the final year of SLIGP Grants for the rollout of FirstNet, a nationwide broadband network. ISICSB has applied for 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 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.

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

In August, 2013, the Board, on behalf of Iowa, received a federal broadband planning grant, known as the State and Local Implementation Grant Program (SLIGP), in the amount of \$1.67 Million for a three (3) year planning period to specifically focus on planning for the build-out in Iowa of the Nationwide Public Safety Broadband Network (NPSBN), a high-speed wireless broadband network specifically for public safety. This broadband network will supplement and compliment any and all public safety land-mobile radio systems. This grant can also be used to fund 50% of the SWIC's position, with the restriction that that 50% has to be entirely devoted to the broadband planning initiative of the NPSBN. This grant expires March 1, 2018.

Potential legislative items noted in Section 5 would address funding streams for interoperability in Iowa by supporting ISICSB and via grants that local agencies could use to expand interoperability.

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. That effort was recalled and a new RFP process was initiated.

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. Equipment was delivered to Iowa in January 2016. ISICS is scheduled to be completed within 30 months from contract signing. ISICSB members believe by working with state 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 occur.

- ISICSB has continued to expand 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.
- Regarding expanding use of the ISICS Platform, below is a list of agencies that have completed the process to use ISICS as of December 2017. 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.
 - 185th Iowa Air National Guard
 - Adair Guthrie EMA
 - Buena Vista County
 - Carlisle Fire Department
 - Carroll County
 - Chickasaw County
 - Dallas County
 - Delaware Township
 - Des Moines Police Department
 - Grundy County
 - Harrison County
 - Humboldt County
 - Iowa Department of Natural Resources
 - Jasper County
 - Kossuth County
 - Linn County Sheriff's Office
 - Mahaska County
 - Marion County Sheriff
 - Mercy Ambulance Des Moines
 - Metro Incident Command Radio Network (MICRN)
 - Mills County
 - Northern Warren Fire
 - Shelby County
 - Unity Point Des Moines
 - US Army Corp of Engineers, Lake Red Rock
 - Virginia Township Fire Rescue
 - Warren County
 - Westcom
 - Wright County

- See map of current ISICS buildout as of December 2017 (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 Sub-Committee to address Iowa's portion of planning and technology issues of this coming national network.

- This subcommittee was Co-Chaired by ICN Executive Director Ric Lombard and State of Iowa CIO Robert von Wolffrad. Members included SWIC Allen, SWIC Maiers, state and local subject matter experts (SMEs), Department of Management, E911 Council Chair, Connect Iowa, and representatives of police, fire and EMA.

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 (WISE) 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 has expanded to two additional schools, Norwalk and Martensdale. Overall feedback from the program was positive. The WISE Pilot report is now available for review and is included in this document packet.

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) Office of Emergency Communications (OEC). These Technical Assistance (TA) grants can be presented throughout the state. The ISICSB has acquired several national DHS/OEC interoperability tools for these efforts, such as:

- 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 is assisting with the planning for the next National Guard communications training events scheduled for 2018.
- ISICSB Training Committee in collaboration with DHS/OEC are actively planning more communication training opportunities scheduled for calendar year 2018. This follows COMT and Incident Tactical Dispatch classes in calendar year 2017.
- 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 recovery 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 to be built in the near future 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 that would provide additional funding sources through 2020.

The educational opportunities do not just include local subject matter experts (SME). This includes the Inter RF Subsystem Interface (ISSI) Summit that was held in March of 2017 in which SMEs from TIA/TR-8, the Federal Partnership for Interoperable Communications

(FPIC)¹ and vendors attended on invited travel by ISICSB. This summit provided extremely valuable information regarding the complexities, required time, expenses and pitfalls associated with an ISSI connection between two LRM 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*.

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 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 administrator, 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.

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 within the next three years.

SWIC Maiers and former SWIC Allen have also attended numerous county 911 meetings, and several county board meetings, to discuss interoperable communications and answer questions regarding ISICS and FirstNet. In addition, both former SWIC Allen and 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.

¹ 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 Safety Telecommunications Council (NPSTC) and a collaborative partner with SAFECOM and NCSWIC. (taken from <https://www.dhs.gov/safecom/fpic/>)

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

Part 7 covers the collaboration and issuance of a statewide multi-state agency RFP for a land-mobile radio (LMR) system.

Board Management and the SWIC did presentations at several events in 2017. The goal of the presentations was to update stakeholders on the ISICS Platform and share 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 incentivize expansion of the ISICS Platform to support regional efforts and bring to fruition the implementation of a statewide integrated public safety interoperable communications 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.

ISICSB members and SWICs 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.

ISICSB Technology Committee and FirstNet Broadband subcommittee hosted 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.

ISICSB Operations Committee is currently maintaining a Public/Private subcommittee to bridge concerns of private businesses providing communication resources to Iowa public safety community.

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.

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 Office of Emergency Communications (OEC) that meets regularly to investigate and solve problems pertaining to interoperability.

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 56 states and 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 just completed. 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.

V. 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 scheduled for July 2018.

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 expected to be complete in March of 2018 and construction is slated to be completed by May 2018. The status of the construction as of

December 15, 2017 is shown in Figure 1 (larger map in Attachment 2). Sites listed as Completed are expected to start radiating in early 2018. Sites denoted with an R are still in regulatory phases which determined whether or not this site can be used based on federal regulations. The lines connecting the sites represent the microwave backhaul paths that connect all the tower sites to the individual cores.

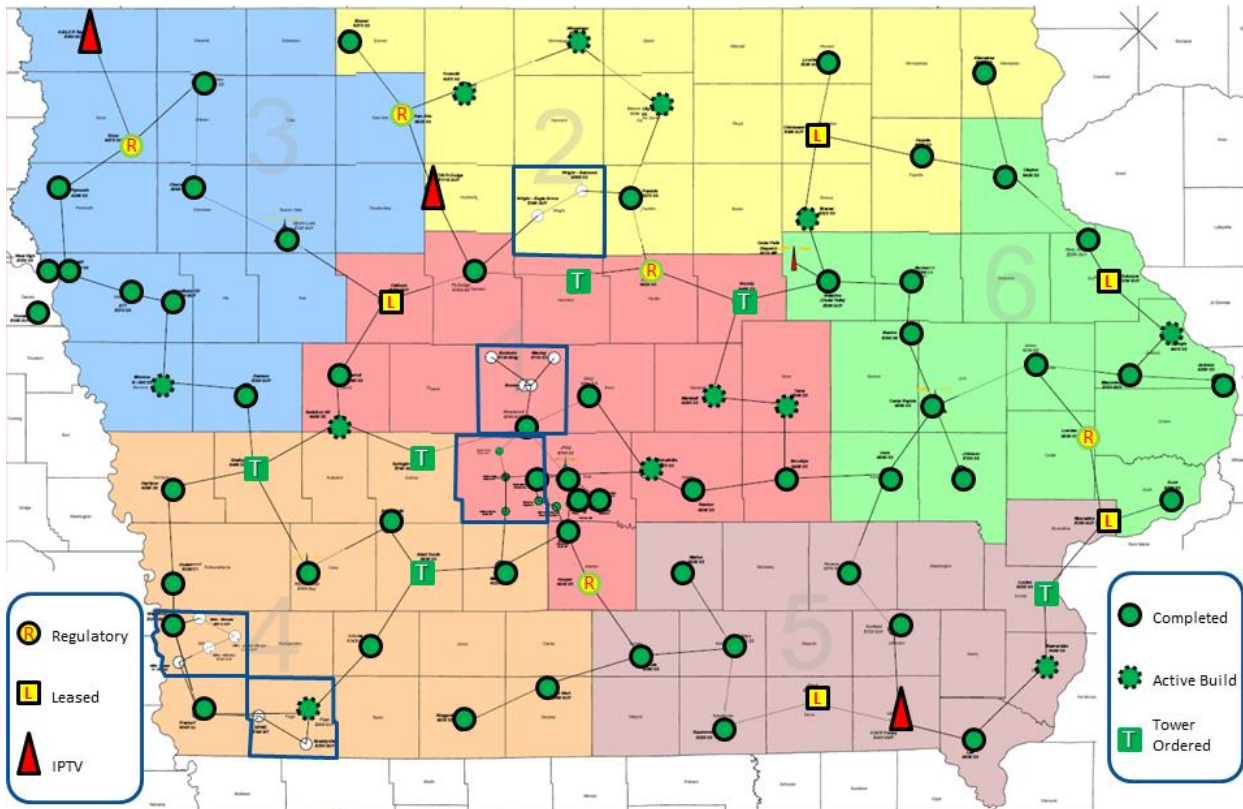


Figure 1. Current status of the ISICS Platform buildout. Blue-outlined counties represent those that have signed on to the system and have added or are adding infrastructure for their own local operations.

Optimization of the ISICS Platform and acceptance testing is scheduled to begin in Spring of 2018 and conclude in Summer of 2018. 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 2017 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 policies 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 along with counties of Dallas, Woodbury, Boone, Humboldt, Mills, Page and Wright have also chosen to use ISICS 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.

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).

A Level 3 User brings all the features of Level 1 and Level 2, but adds in direct connection to the ISICS core computer 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.

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. Counties that have opted to use ISICS as Level 4 Users are outlined in dark blue in Figure 1.

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 will be sent to all public safety answering points (PSAP) in January that outline preparatory steps that can be taken for ISICS access. This will allow for long-term planning strategies that local entities can use for their interoperable communications plans. 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.

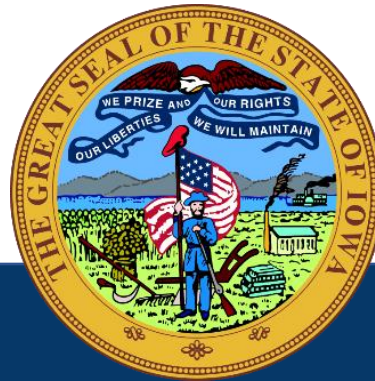
VI. Attachments for 2017

1. **2017 SCIP**
2. **Map of ISICS Network**
3. **List of agencies and counties that have joined ISICS for interoperability and/or operability.**
4. **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)**
5. **Standards adopted 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**
6. **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**

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,

A handwritten signature in blue ink, appearing to read 'Chris Maiers'.

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.

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.



Figure 1: Enhanced SCIP



TABLE OF CONTENTS

INTRODUCTION.....	1
Guiding Approach / Principles.....	1
Iowa Enhanced SCIP Overview.....	2
OVERVIEW OF STRATEGIC GOALS & OBJECTIVES.....	3
GOVERNANCE & COORDINATION.....	4
TECHNOLOGY & OPERATIONS.....	5
FUNDING & SUSTAINMENT	7
ISICSB COMMITTEE MISSION STATEMENTS AND SCIP GOALS & OBJECTIVES	8
IMPLEMENTATION PLAN.....	13
APPENDIX A: List of Acronyms.....	14
APPENDIX B: SWOT Analysis	15
APPENDIX C: ISICSB Committee SCIP Goal Implementation & Measurement.....	17
APPENDIX D: Code of Iowa	25

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 Plan¹.

The Interoperability Continuum² 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

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.

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.

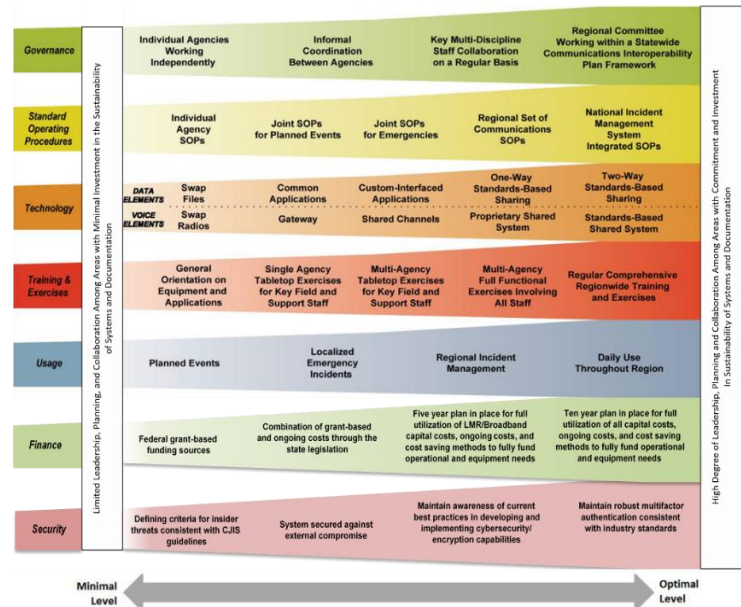


Figure 2: Iowa Interoperability Continuum

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.

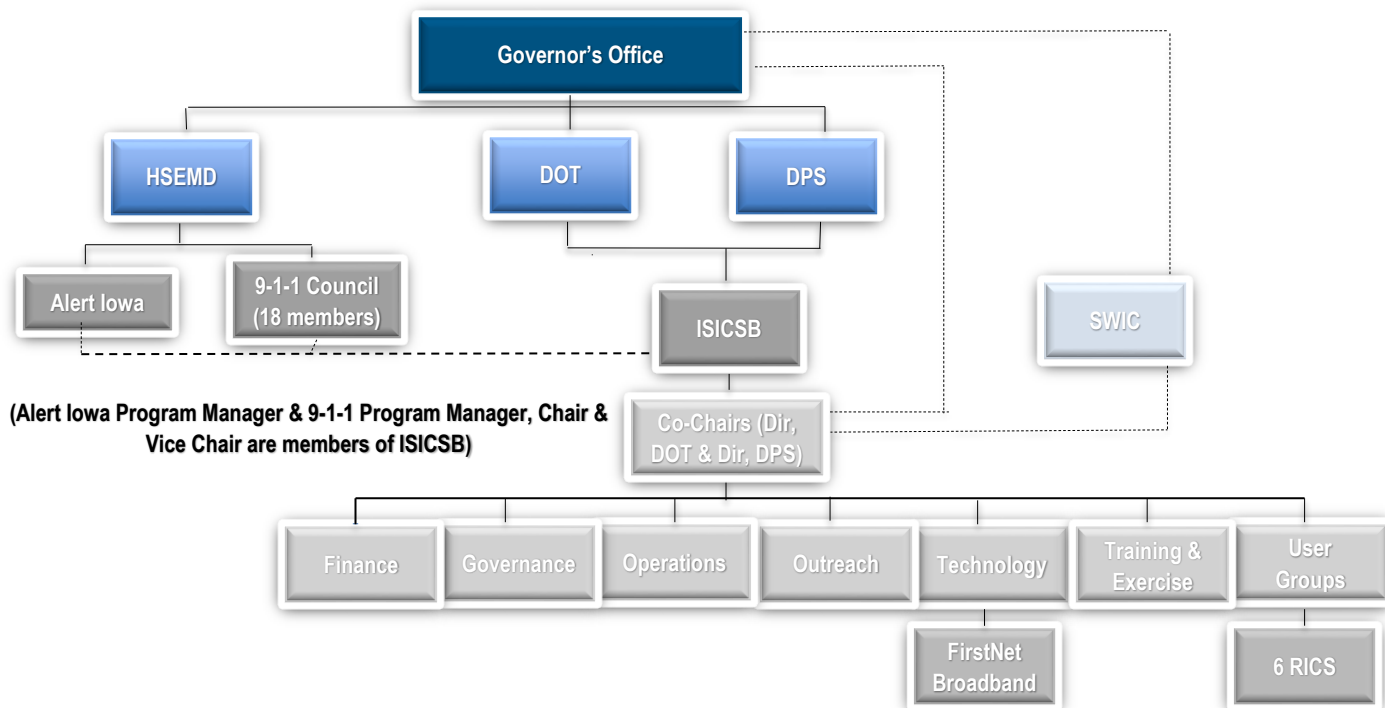


Figure 3: Governance Organization Chart

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 DOT³.

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			
			
<p>Mission Statement: The Finance Committee identifies potential funding streams and coordinates existing funds for interoperable communications priorities.</p>			
Goal #	Goals	Objectives	Benefits
1.	<i>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</i>	<ul style="list-style-type: none"> Develop annual fiscal processes which meets GAAP/GAAS requirements for ISICS Project 	<ul style="list-style-type: none"> 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.	<i>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</i>	<ul style="list-style-type: none"> Develop annual fiscal processes which meets GAAP/GAAS requirements for statewide data network 	<ul style="list-style-type: none"> 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.	<i>Develop appropriate process and procedures for administering all financial assets consistent with national best practices in accounting and auditing</i>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Establishes known processes and procedures for budgeting, accounting, inventorying and auditing all financial assets of ISICSB whether state or grant funds

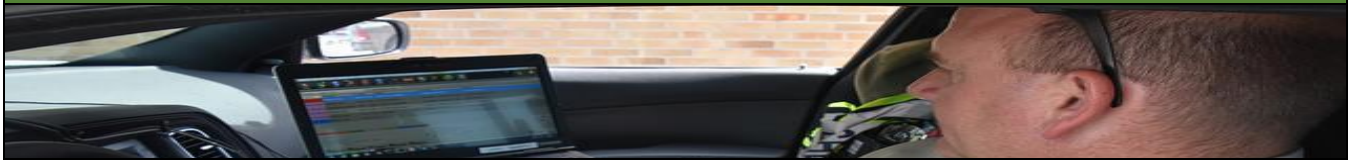
Governance Committee



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.	<i>Develop appropriate governance through creation of policy and procedure statements for enhancement, deployment and operation of ISICS</i>	<ul style="list-style-type: none"> • Develop policies as requested • Disseminate policies as needed 	<ul style="list-style-type: none"> • Promotes a shared understanding of governance involving the statewide system
5.	<i>Develop appropriate governance through creation of policy and procedure statements for enhancement, deployment and operation of a statewide broadband network</i>	<ul style="list-style-type: none"> • Develop policies as requested • Disseminate policies as needed 	<ul style="list-style-type: none"> • Promotes a shared understanding of governance involving statewide broadband network
6.	<i>Establish a process to administer grant funds or communications assets</i>	<ul style="list-style-type: none"> • Develop policies as requested • Disseminate policies as needed 	<ul style="list-style-type: none"> • 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.	<i>At the end of five years 95% of all dispatch centers have access to ISICS</i>	<ul style="list-style-type: none"> • Identify dispatch centers that need access • Establish operational policies for ISICS access • Deliver recommendation/documentation to ISICSB 	<ul style="list-style-type: none"> • Advances interoperability statewide by connecting dispatch centers to ISICS
8.	<i>To review the ISICS draft policies and make recommendations to Standards Working Group</i>	<ul style="list-style-type: none"> • Review and document recommendations to the Standards Working Group representative 	<ul style="list-style-type: none"> • Creates an opportunity to update ISICS policies
9.	<i>Align and update legacy plans, including system failures</i>	<ul style="list-style-type: none"> • Identify, review and update existing communications plans and include a system failure plan • Deliver recommendation/ documentation to ISICSB 	<ul style="list-style-type: none"> • Creates an opportunity to address issues with existing communications plans

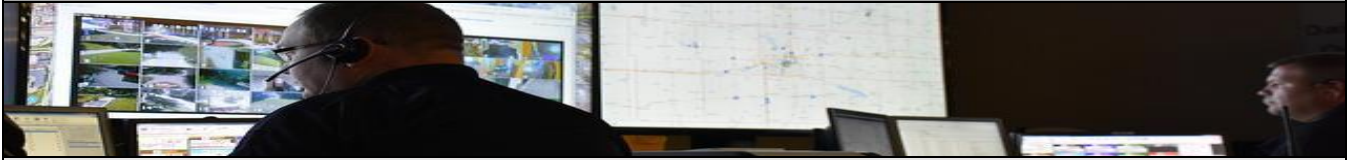
Outreach Committee

 <p style="font-size: 24px; font-weight: bold; margin: 0;">ISICSB</p> <p style="margin: 0;">Iowa Statewide Interoperable Communications System Board</p>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  10,000+ subscribers </div> <div style="text-align: center;">  95% statewide coverage </div> <div style="text-align: center;">  84+ towers throughout Iowa </div> <div style="text-align: center;">  \$0 users fees </div> </div> <p style="font-weight: bold; margin: 5px 0;">The ISICS Platform</p> <p style="font-size: 10px; margin: 0;">Iowa Statewide Interoperable Communications System</p>
---	---

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.	<i>To develop and deliver outreach materials for use in making decisions to become a user of ISICS (by final system acceptance) by June 2018</i>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Promotes awareness of benefits of becoming an ISICS user
11.	<i>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.</i>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Promotes awareness of benefits of becoming a broadband network user
12.	<i>Develop a plan for utilizing social media relative to ISICSB activities and interoperability issues</i>	<ul style="list-style-type: none"> Adoption of social media plan In five years, the ISICSB website or the SWIC becomes the primary and central point for information 	<ul style="list-style-type: none"> Allows for a wide audience to be reached with information pertaining to interoperability.
13.	<i>Approach and educate elected officials</i>	<ul style="list-style-type: none"> Develop a training plan Engage association partners 	<ul style="list-style-type: none"> 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.	<i>To lead technological solutions for voice interoperability</i>	<ul style="list-style-type: none"> To develop standards for ISICS communications equipment Create minimum standards for ISICS interoperable communications equipment 	<ul style="list-style-type: none"> Supports interoperability involving voice across communications equipment
15.	<i>To lead technological solutions for data interoperability</i>	<ul style="list-style-type: none"> Create minimum standards for interoperable communications equipment Make recommendation to ISICSB to adopt standards 	<ul style="list-style-type: none"> Supports interoperability involving data across communications equipment
16.	<i>Investigate voice and data convergence and differentiating the needs of public safety</i>	<ul style="list-style-type: none"> Investigate technology Choose best course of action Make recommendations 	<ul style="list-style-type: none"> 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.	<i>Develop and provide standard core training for interoperable communications across the various state regions</i>	<ul style="list-style-type: none"> Establish guidelines defining standard core training Embed communications training within existing state training institutions 	<ul style="list-style-type: none"> Promotes consistent training across state regions
18.	<i>Expand the statewide core group of trainers who would be able to teach necessary COMU positions classes and increase COMU awareness</i>	<ul style="list-style-type: none"> Create a COMU awareness outreach program for dissemination through the Outreach Committee Seek Train-the-Trainer classes 	<ul style="list-style-type: none"> Increases the number of trainers to promote more training and organization of statewide COMU program
19.	<i>Develop a cost analysis of training to augment future budgetary planning</i>	<ul style="list-style-type: none"> Obtain training funding 	<ul style="list-style-type: none"> 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.	<i>Develop processes and vet the application process for access to the ISICS interoperable communications platform within state or grant resources.</i>	<ul style="list-style-type: none"> • Add efficiencies to application process • Determine resource needs for an objective evaluation of Level 3 and 4 resource users 	<ul style="list-style-type: none"> • Decreases application process time relative to number of applications per user level • Encourages increased number of users
21.	<i>Develop processes for guidance on broadband data interoperable communications platform within state or grant resources.</i>	<ul style="list-style-type: none"> • Identify and deploy process to assist in the application for broadband access 	<ul style="list-style-type: none"> • Decreases application process time relative to number of applications per user level • Encourages increased number of users
22.	<i>Strengthen all RICs</i>	<ul style="list-style-type: none"> • Travel to every county to conduct outreach to all stakeholders • Listen and accept feedback • Identify meeting frequency and appropriate tasks 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 ISICS 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Most counties use Alert Iowa-- Statewide system for alerts and warnings, incorporates reverse 911, integrates IPAWS • Outdoor and indoor warning systems • Paging systems
Weaknesses	<ul style="list-style-type: none"> • Diversity of radio frequency use • Tactical Interoperability Communications Plan (TICP) not current • Funding • Outreach and education on ISICS • 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 	<ul style="list-style-type: none"> • Stakeholders have limited broadband technical knowledge • Reliance on commercial carriers for information • No dedicated funding stream 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Multiple points of contact for alerts and warnings • Lack of standards

<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Opportunities</p>	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Expanding ICSIC Adopting FirstNet Development of applications Sharing information with all stakeholders and decision makers 	<ul style="list-style-type: none"> Leveraging voting seat on Telecommunications Industry Association (TIA) Create grant funding method to push grants to locals 	<ul style="list-style-type: none"> Some counties still have the opportunity to join Alert Iowa Addressing Alerts & Warnings in the SCIP
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Threats</p>	<ul style="list-style-type: none"> 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			
<p>Mission Statement: The Finance Committee identifies potential funding streams and coordinates existing funds for interoperable communications priorities.</p>			
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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Develop annual fiscal processes which meet GAAP/GAAS requirements for ISICS Project 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Develop annual fiscal processes which meet GAAP/GAAS requirements for statewide data network 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Review ISICSB policies within 60 days 	<ul style="list-style-type: none"> Develop policies as requested Disseminate policies as needed 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Review ISICSB policies within 60 days 	<ul style="list-style-type: none"> Develop policies as requested Disseminate policies as needed 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Process is adopted by ISICSB 	<ul style="list-style-type: none"> Develop policies as requested Disseminate policies as needed 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> The number of dispatch centers connected to ISICS 	<ul style="list-style-type: none"> Identify dispatch centers that need access Establish operational policies for ISICS access Deliver recommendation/documentation to ISICSB 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Throughput. The number the ISICSB received from the committee vs the number delivered 	<ul style="list-style-type: none"> Review and document recommendations to the Standards Working Group representative 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Completion of plan 	<ul style="list-style-type: none"> Identify, review and update existing communications plans and include a system failure plan Deliver recommendation/documentation to ISICSB 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Outreach materials developed for ISICS, then distributed and posted on the website, reviewed and updated by the end of the state fiscal year 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Outreach materials developed for broadband then distributed and posted on the website, reviewed and updated by the end of the calendar year 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Adoption of social media plan In five years, the ISICSB website or the SWIC becomes the primary and central point for information 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • Training program development complete • Number of engagement/participants involved in training program 	<ul style="list-style-type: none"> • Develop a training plan • Engage association partners 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> Publish state specific findings 	<ul style="list-style-type: none"> To develop standards for ISICS communications equipment Create minimum standards for ISICS interoperable communications equipment 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Publish state specific findings 	<ul style="list-style-type: none"> Create minimum standards for interoperable communications equipment Make recommendation to ISICSB to adopt standards 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Publish staff studies on findings 	<ul style="list-style-type: none"> Investigate technology Choose best course of action Make recommendations 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • Development of training materials • Number of people trained 	<ul style="list-style-type: none"> • Establish guidelines defining standard core training • Embed communications training within existing state training institutions 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Increase number of trainers so that at least two COML classes can be scheduled per year • Number of people trained • 	<ul style="list-style-type: none"> • Create a COMU awareness outreach program for dissemination through the Outreach Committee • Seek Train-the-Trainer classes • 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Delivery of a cost analysis document 	<ul style="list-style-type: none"> • Obtain training funding 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Increasing the number of people on the credentialing list 	<ul style="list-style-type: none"> • Increased opportunities to complete position task book • Increase regional training opportunities 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Add efficiencies to application process • Determine resource needs for an objective evaluation of Level 3 and 4 resource users 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Process developed • Number of users assisted, applied for and approved 	<ul style="list-style-type: none"> • Identify and deploy process to assist in the application for broadband access 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Increase in RIC user attendance, participation, and investment 	<ul style="list-style-type: none"> • Travel to every county to conduct outreach to all stakeholders • Listen and accept feedback • Identify meeting frequency and appropriate tasks 	<ul style="list-style-type: none"> • 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

DEPARTMENT OF PUBLIC SAFETY, §80.28

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

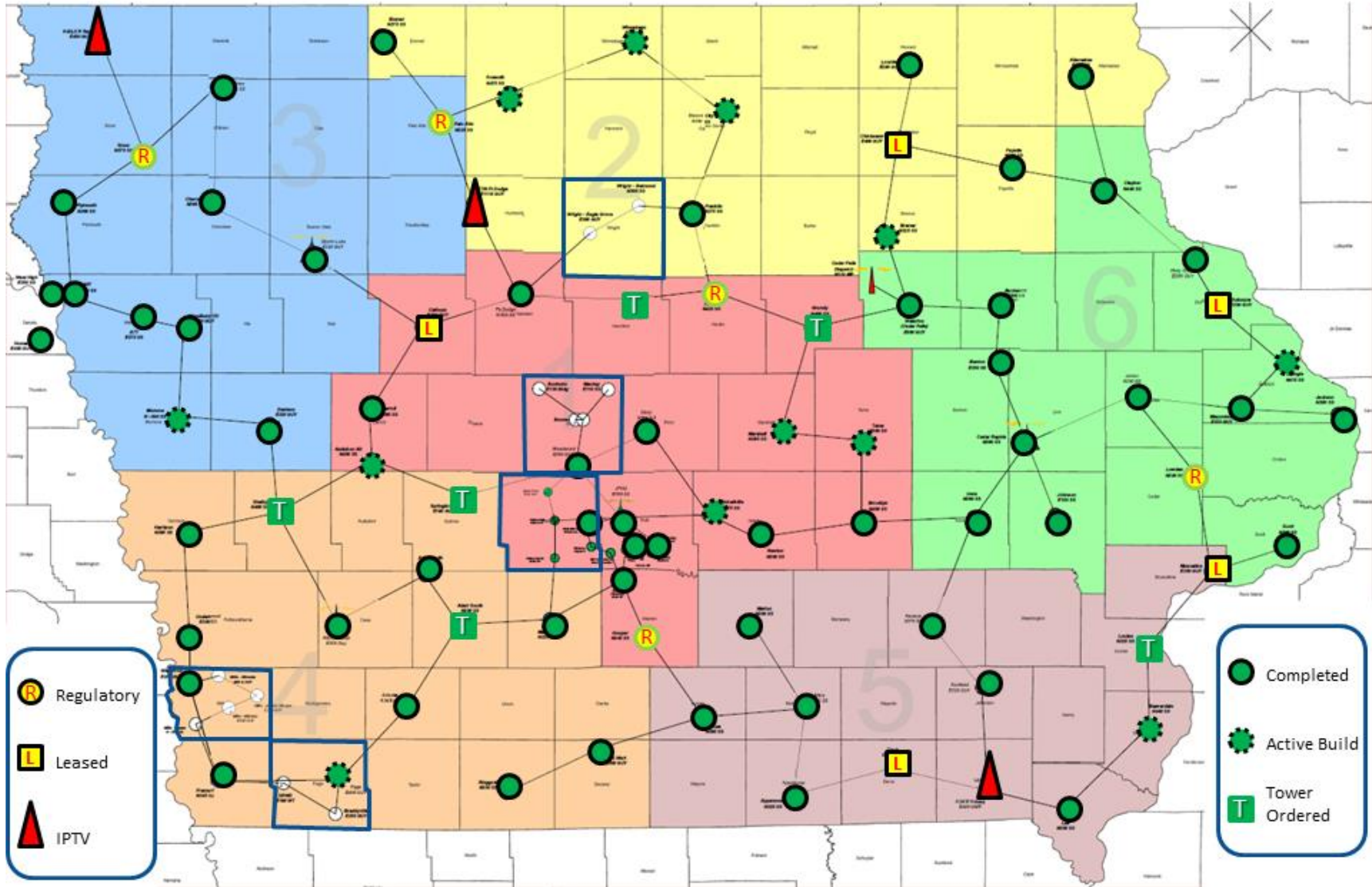
purpose. The departments shall enter into an agreement to provide administrative assistance and support to the board.

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. Blue-outlined counties represent those that have signed on to the system and have added or are adding infrastructure for their own local operations.

Attachment 3: List of agencies and counties that have joined ISICS for interoperability and/or operability.

- 185th Iowa Air National Guard
- Adair Guthrie EMA
- Buena Vista County
- Carlisle Fire Department
- Carroll County
- Chickasaw County
- Dallas County
- Delaware Township
- Des Moines Police Department
- Grundy County
- Harrison County
- Humboldt County
- Iowa Department of Natural Resources
- Jasper County
- Kossuth County
- Linn County Sheriff's Office
- Mahaska County
- Marion County Sheriff
- Mercy Ambulance Des Moines
- Metro Incident Command Radio Network (MICRN)
- Mills County
- Northern Warren Fire
- Shelby County
- Unity Point Des Moines
- US Army Corp of Engineers, Lake Red Rock
- Virginia Township Fire Rescue
- Warren County
- Westcom
- Wright County

Attachment 4: 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)***



PUBLIC NOTICE

Policy Release Number: 2012-05 (aka ISICSMC12-B) revised

State of Iowa

Date of Proposal ISICSB Meeting: December 8, 2016
Dates Posted for Public Comment: December 8, 2016 to
Date Adopted by ISICSB:
Public Comment:

Minimum Interoperable Radio Channels & Nomenclature

Effective Date: Jan. 1, 2018

All Public Safety Radios Shall be programmed to include the channels as listed in the attached ICS217A form (as applicable to your frequency band and as channel capacity allows) by the effective date of January 1, 2018.

This Iowa Statewide minimum interoperability channel plan will improve multi-agency interoperability for communication by Land Mobile Radio (LMR) systems at times of a major incident and/or need.

The following radio channel names have been changed as of January 1, 2014:

- State Fire Aid/Fire Mutual Aid (154.2800 MHz) - Now called VFIRE21
- Law Aid/Mutual Aid Law (155.4750 MHz) - Now called VLAW31
- State EMS/EMS Mutual Aid (155.3400 MHz) - Now called VMED28

In order to maintain consistency with current capabilities, agencies may wish to continue use of these frequencies, using the updated names. All Channels listed in the attached ICS217A document will follow CTCSS, DCS, NAC, CSQ designations as set forth by the most recent publication of The Department of Homeland Security's NIFOG handbook. See www.dhs.gov/national-interoperability-field-operations-guide-nifog

Additional information can be found from the Iowa Statewide Interoperable Communications Systems Board (ISICSB) at www.isicsb.iowa.gov.



Policy Statement

State of Iowa

Policy Release Number: 2017 – 07

Date of Proposal ISICSB: Meeting: July 13, 2017
Dates Posted for Public Comment: July 12, 2017
Date Adopted by ISICSB: Meeting
Public Comment: None

Policy Statement supporting the National Emergency Number Association (NENA) i3 Standard for Next Generation 9-1-1 (NG9-1-1).

WHEREAS: The Iowa Statewide Interoperable Communications System Board (ISICSB) is established in Code of Iowa sections 80.28 and 80.29. ISICSB is charged to develop, implement and oversee policy, operations, and fiscal components of communications interoperability efforts at the state and local levels, and to coordinate similar efforts at the federal level, with the objective of overseeing operation of statewide integrated public safety systems, and establish, monitor, and maintain appropriate policies and protocols, expand, maintain and fund stakeholder education, public education, and official education programs to demonstrate value of short-term communications interoperability solutions, and;

WHEREAS: ISICSB investigates data and video interoperability systems and standards such as the i3 Standard that support public safety and service, and;

WHEREAS: ISICSB is tasked with establishing, monitoring and maintaining policies and protocols that ensure interoperable communications function properly by following best practices and standards set forth by associations such as NENA, and;

WHEREAS: ISICSB supports the expansion of regional efforts to promote implementation of the statewide integrated public safety communications interoperability system that includes standards like the i3 Standard, and;

WHEREAS: ISICSB views NG9-1-1 and the State of Iowa 911 Communications Council as a vital partner and stakeholder in developing a shared communications system that is capable across platforms, and;

WHEREAS: ISICSB supports and encourages nationally recognized organizations to continue providing standardization of public safety equipment, systems, networks, platforms, and services like the NENA i3 Standard for NG9-1-1 which supports various data and video interoperability systems, and; Now therefore;

IT IS ISICSB POLICY: That the Iowa Statewide Interoperable Communications System Board (ISICSB) hereby endorses the i3 Standard as the architecture for interoperable NG9-1-1 systems; encourages immediate adoption and implementation of NG9-1-1 and encourages national associations to advance the deployment of i3-based NG9-1-1 systems and services in a coordinated and effective manner.

Attachment 5: Standards adopted 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***



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

Standard Name:	Subscriber Security		Date Created:	March 3, 2017	
Standard Policy #	1.1.0	Section Title: Governance	Interoperability Guidelines	Status	Completed
Approval Authority:	ISICSB		Adopted:	06/08/2017	Reviewed: 06/08/2017

1. Purpose or Objective

The objective of this standard is to provide the proper guidance for “Radio System Keys” in order to ensure radio subscriber security is protected. By utilizing “Radio System Keys,” the radios are able to be programed with the appropriate security options. To properly account for and represent the various system key capabilities available by different manufactures, each capability will be discussed in its own section.

2. Technical Background

▪ **Capabilities**

The Iowa Statewide Interoperable Communications System Board (ISICSB) wants to ensure that the highest level of security is incorporated into the Iowa Statewide Interoperable Communications System (ISICS) in order to protect the integrity of its users and ISICS as a whole. Both System and Advance System Keys assist in accomplishing this task. Advanced System Keys allow for the following protections: restricting who is given access to program the radios and restricting radio and talkgroup IDs. Advanced system keys allow the user to determine how long the key will be operable. Advanced System Keys offer an extra layer of security for users as these keys are unable to be replicated.

Security options also vary by the radio brand the system user selects to access ISICS. For example, the radio might include an option to password protect the radio. This will allow the agency to prevent any modifications to be made to the radio settings without inputting the password.

- **Constraints**

The Advanced System Key is determined by the vendor radio, and is configurable to allow enhanced security. The radio user will need to provide a configurable system key (child key, daughter key, slave key, distribution key, etc.) to be configured by the ISICS System Administrator (System Administrator) or the System Administrator's Designee (Administrator Designee) who is selected from a list of individuals approved by ISICSB.

All ISICS users will have to sign for and will incur all the costs and liabilities associated with each key; absolving ISICSB and its representatives of any liabilities and/or costs associated with its use or impact from use of the key.

3. Operational Context

As mentioned earlier, the Advanced System Key is being utilized to increase security in the programming of the radios as well as protecting the integrity of ISICS. Please refer to Sections four and five of this standard for greater information regarding the management of the keys.

4. Recommended Protocol/ Standard

Do not program a radio you are not responsible for without written consent. Please note, if a key is programmed and distributed as "software and hardware," then the keys will be logged and tracked. The System Administrator will track all keys. The information will be stored on state secure servers internal to State of Iowa.

- **System Key Administration**

There will be one Master System Key per vendor in the possession of the System Administrator. The System Administrator will develop all system keys (child key, daughter key, slave key, distribution key, etc.) with proper provisioning for user specific requirements to allow subscriber programming. ISICSB reserves the right to amend this policy at their sole discretion in order to increase the security and protect the integrity of the system.

All keys generated by the System Administrator will have an expiration date set, which will assist in increasing security and tracking the keys distributed to system users. ISICSB reserves the right to revoke the ability to possess a key if the agency's possession affects the integrity and/or security of ISICS.

• **Liability for the Misuse of the System Keys**

Each agency must designate a governmental employee as representative and a governmental employee as alternate who will be responsible for obtaining and securing the system key(s). While not mandated, ISICS encourages agency users to create their own agency policy to ensure compliance. Both representatives will be required to sign for the key(s) and will agree to the following:

1. The agency representative and agency alternate absolve ISICSB and ISICS representatives of all liability involving the loss or misuse of the system key(s) they signed for and took possession of for their agency.
2. The agency representative and agency alternate will be personally and professionally liable for the misuse and/or loss of system keys while in their possession. The agency representative will not be liable for the loss or misuse of a system key while in the possession of the agency alternate or vice versus unless the agency user's policy assigns such liability. If this is the case, then ISICSB will follow the most stringent policy in determining liability and the ability for individual users to have future access to the system.
3. All system users are mandatory reporters of misuse of ISICS. Failure to do so could result in the individual and/or agency who has knowledge of the misuse being permanently removed from the system. The agency representative and agency alternate agree to provide this requirement to all agency users.
4. If the misuse and/or loss of a system key is discovered by the agency representative and/or agency alternate, then the violation must be reported orally to the System Administrator within 48 hours of obtaining this knowledge. This will allow for a cursory investigation by the individual agency user to ensure the information is accurate. ISICSB stresses the importance of reporting the misuse or loss of a system key if the agency cannot determine the credibility of the information received as a failure to report could result in the loss of the key or access to ISICS. The oral notification must be followed up with a written explanation to be submitted to the System Administrator within 48 hours of providing the oral notification. The System Administrator will forward the information to the Standards Coordinator within 24 hours of receiving the written notice. To protect the integrity and the security of the system, access to the system keys will be immediately suspended until the issue is resolved.

Please review the standard “Response to Non-Compliance” for additional information.

5. The misuse and/or loss of a system key could result in the agency representative’s and agency alternate’s access to ISICS being permanently revoked.

5. Recommended Procedure for System Keys

The ISICS System Administrator and his or her designee (System Designee) will be the keepers of the Master Advanced System Keys. The System Administrator and System Designee will distribute the provided key back to the entity for subscriber programming. The entities who receive the keys are responsible for documenting all keys that have been programmed. This information will be placed into a tracking spreadsheet. The System Administrator may contact the person responsible for the keys for auditing purposes.

- **Radios that are Capable of the Advanced System Keyfeature**

Agencies will need to purchase a key reader and key buttons. The agency will be responsible to bring the blank key buttons to the System Administrator or System Designee to be programmed.

Key Expiration Dates

- System Partners: Two Years
- Trusted Technician: Three Years

System Partners and trusted technicians must consent to the following:

- (1) Yearly Iowa Department of Public Safety Background checks, and
- (2) Misuse of their position could result in access to ISICS being revoked.

Examples include but are not limited to the following: violation of one of the standards, his or her actions directly causes a failure to the system, accessing group and/or systems within ISICS he or she was not granted access, or failing to properly program in anyway a radio, other device which causes any misuse, degradation or loss of use of access of any user.

Programmed Key Range Usage

To ensure programed key are not misused, a range limit will be set for each ID based on the range the agency will need to conduct business. If a greater use is demonstrated, then the range will be able to be modified by reprogramming the key.

Time restrictions are mandatory restrictions by ISICSB.

Assumptions: In drafting this standard, the Standards Working Group assumes there will be individuals qualified to serve as the ISICS System Administrator (System Administrator) and the System Administrator’s Designee (Administrator Designee), and these individuals will be able to successfully carry out their required duties.

Liabilities: The manner in which the standard is drafted, keeps a majority of the liability with the individual agency users and the individuals employed by ISICS to carry out the required duties. All liability cannot be discharged from the system as there are legal doctrines recognized by Iowa Code, such as the doctrine of respondent superior.

Cost: The cost of the standard is unknown. Some costs could include filling the position of ISICS System Administrator (System Administrator) and System Administrator’s Designee (search, background checks, possible salary, etc.).



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

Standard Name:	Variance and Waivers		Date Created:		11-29-16	
Standard Policy #	2.1.0	Section Title: Governance	Management of System		Status	Completed
Approval Authority:	ISICSB		Adopted:	08/10/2017	Reviewed:	08/10/2017

1. Purpose or Objective

0

The objective of this standard is to provide the guidelines for granting a temporary or permanent *variance* and/or *waiver* to the established standards, protocols and procedures to a user of the Iowa Statewide Interoperable Communications System (ISICS). These terms as they relate to the ISICS are defined as follows:

- **Variance**-The approved deviation from the established and mandated ISICS standards, protocols and procedures in which the deviation would not jeopardize the integrity of the system and/or cause an undue burden on other users.
- **Waiver**-An approved release from the mandate to adhere to a specific ISICS standard, protocol, and procedure. The waiver will only be granted if the waiver does not jeopardize the integrity of the system and/or cause an undue burden on other users.

2. Technical Background

- **Capabilities**
- **Constraints**

3. Operational Context

While the Iowa Statewide Interoperable Communications System Board (ISICSB) and Standards Coordinator acknowledge there are times when a standard, procedure and/or protocol may create an undue burden on a user or may not be able to be successfully complied with, the number one priority is to ensure the integrity of ISICS is upheld so all users are able to enjoy the benefits of the system. If granting a variance or waiver would jeopardize this overall goal, then it will not be granted.

4. Recommended Protocol/ Standard

All requests for a variance or waiver must be provided in writing to the ISICS Standards Coordinator. All oral requests will be viewed as an inquiry and a request for guidance and not a formal request for a variance or waiver.

5. Recommended Procedure

The agency requesting approval for a variance and/or waiver must submit its request in writing to the Standards Coordinator. The request must contain the components below. Any incomplete requests will be denied. If more than one variance or waiver is being requested, then the required elements must be completed for every variance and/or waiver being requested.

Required Elements

- (1) Provide a detailed description of the variance and/or waiver being requested.
- (2) Provide detailed justification for the variance and/or waiver. If the standard, protocol and/or procedure in which the variance or waiver being requested causes the agency harm or has negative consequences on the agency, then this must be described in detail.
- (3) Detailed account of how, if at all, granting the variance or waiver will affect other users on the system.

Process of Review

Upon receiving the request for a variance and/or waiver, the Standards Coordinator will review the request to ensure all required elements are present. If elements are missing, then the request will be denied and returned to the user. If all elements are present, then the application will be forwarded to the appropriate experts in the subject matter as identified by the Standards Coordinator.

Elements Considered when Approving or Denying a Request for Variance or Waiver

- (1) Technical Component
 - a. Current Impact
 - b. Future Impact
- (2) Impact to the Operational Components
 - a. Already Established Systems
 - b. Future Systems
- (3) The Agency's Conformance with other Standards, Protocols, and Procedures
- (4) Current and Future Cost to the ISICS and other Users if a Variance or Waiver is Granted
- (5) Alternatives to Granting the Variance or Waiver

The ISICSB will have an open comment period for all affected users. Each affected user will be provided notice of any potential negative impacts if the variance or waiver is granted. The impacted agency will be given 30 days to provide a written response.

In emergency situations, a temporary variance or waiver may be approved. Oral and written notice must be provided to affected agencies.

Full approval of the variance and/or waiver will be provided in writing to affected parties and posted electronically for all other users to review.

6. Management

The ISICSB and the Standards Coordinator are responsible for reviewing and granting or denying variances and waivers to requesting agencies.

Assumptions: The Standards Working Group assumes a Standards Coordinator will be appointed, and the individual will strictly adhere to this standard. The Standards Coordinator will utilize the expertise of subject matter experts in making the best recommendation to the ISICSB and to protect the integrity of the system. In making his or her recommendation, it is assumed the Standards Coordinator will act as a disinterested person.

Liability: The Standards Working Group acknowledges normal liabilities as they relate to the employer-employee relationship as recognized by the Iowa Code. Additionally, liability may arise if a variance or waiver is granted and harm is caused to another user of the system and thereby affecting the overall integrity of the system.

Cost: Exact costs to the ISICSB are unknown at this point, but potential costs could include the services of the Standards Coordinator and other experts who assist in the process.



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

Standard Name:	Maintenance of Alias List		Date Created:	11-29-16	
Standard Policy #	2.2.0	Section Title: Governance	Management of System	Status	Completed
Approval Authority:	ISICSB		Adopted:	08/10/2017	Reviewed: 08/10/2017

1. Purpose or Objective

The objective of this standard is to provide guidance on how to resolve disputes involving radio user names, talkgroup and/or agency acronyms.

The appointed *Technical System Administrator* will be responsible for maintaining the login user aliases, talkgroups and agency acronyms. The information will be stored on the Iowa Statewide Interoperable Communications System (ISICS) secure database.

2. Technical Background

• **Capabilities**

Before approval of aliases, talkgroups and/or agency acronyms for usage on the ISICS, the Technical System Administrator must refer to the table of approved user alias, talkgroups and agency acronyms.

• **Constraints**

The *Technical System Administrator* is responsible for regularly keeping the table up-to-date to ensure aliases, talkgroups or agency acronyms are not duplicated. The table must be stored on the ISICS secure database.

3. Operational Context

N/A

4. Recommended Protocol/ Standard

N/A

5. Recommended Procedure

The Technical System Administrator will manage the table, and notify the Standards Coordinator of any conflicts which are unable to be resolved amongst agencies. The Standards Coordinator will review the conflict and provide a recommendation to the Iowa Statewide Interoperable Communications System Board (ISICSB) within 14 days. The ISICSB will provide a resolution to the conflict within 30 days.

6. Management

The Technical System Administrator will regularly maintain and update the table and distribute any changes to users on a monthly basis, if needed, such as via e-mail.

Assumptions: The Standards Working Group assumes a Technical System Administrator will be appointed and will strictly adhere to the standard, and promptly notify ISICSB when a conflict is discovered.

Liabilities: The Standards Working Group acknowledges normal liabilities as they relate to the employer-employee relationship as recognized by the Iowa Code.

Cost: Exact costs the ISICSB are unknown at this point, but potential costs could include the services of the Technical System Administrator and the technology needed to maintain and upkeep the ISICS secure database in which all the information is housed.



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

Standard Name:	System Login Naming Maintenance		Date Created:	11-29-16	
Standard Policy #	2.3.0	Section Title: Governance	Management of System	Status	Completed
Approval Authority:	ISICSB		Adopted:	08/10/2017	Reviewed: 08/10/2017

1. Purpose or Objective

The objective of this standard is to provide users with notice on how *Core Support Users'* login accounts will be managed. Core Support Users' include system administrators, technical support staff and ISICS Managers. The Core Support User login accounts will be managed by the System Administrator.

2. Technical Background

• **Capabilities**

Login accounts are not assigned to individuals, but rather by their position or the specific task they are authorized to complete. Therefore, one Core Support User may be assigned multiple login accounts based on their access rights as determined by technical and security experts and approved by the Systems Administrator.

• **Constraints**

Login user IDs will be unique and will not be duplicated anywhere in the system. All user IDs will be assigned.

3. Operational Context

In addition to being assigned login IDs for specific access rights. Every individual will be assigned an individual login ID. The assigned login IDs will use a standards format to ensure uniformity.

4. Recommended Protocol/ Standard

The specific procedures governing the actual operations and duties of Core Support Users are defined elsewhere in the standards, protocols and procedures.

5. Recommended Procedure

User IDs will be developed using guidelines established by technical experts to ensure all user IDs follow a standard format and no user ID is duplicated.

6. Management

The Iowa Statewide Interoperable Communications System Board (ISICSB) and the Standards Coordinator are responsible for updating this procedure. Technical experts appointed by the ISICSB are responsible for the creation and management of the accounts.

Assumptions: The Standards Working Group assumes the ISICSB, Standards Coordinator and technical experts will strictly adhere to standard.

Liabilities: The Standards Working Group acknowledges normal liabilities as they relate to the employer-employee relationship as recognized by the Iowa Code.

Cost: Exact costs to the ISICSB are unknown at this point, but potential costs could include the services of the Systems Administrator, Standards Coordinator and technical experts, and the maintenance of the Iowa Statewide Interoperable Communications System (ISICS) in which the Core Support User login accounts will be housed.

Attachment 6: 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*

COMMUNICATIONS RESOURCE AVAILABILITY WORKSHEET				Frequency Band		Description			
				VHF, UHF, 7/800		Iowa Interoperability Channels			
Channel Configuration	Channel Name	Eligible Users	Receive Frequency	Receive Squelch	Transmit Frequency	Transmit Squelch	Mode (A, D or M)	Remarks	
Simplex/Direct	VCALL10	For FCC Part 90 licensees, the non-Federal National Interoperability Channels VCALL10-VTAC14, UCALL40-UTAC43, and 8CALL90-8TAC94 are covered by a "blanket authorization" from the FCC - "Public safety licensees ... can operate mobile units on these interoperability channels without an individual license." See FCC 00-348, released 10/10/2000, paragraph 90.	155.7525 N	156.7	155.7525	156.7	A	Effective 01/01/2014	
Simplex/Direct	VTAC11		151.1375 N	156.7	151.1375	156.7	A	Effective 01/01/2014	
Simplex/Direct	VTAC12		154.4525 N	156.7	154.4525	156.7	A	Effective 01/01/2014	
Simplex/Direct	VTAC13		158.7375 N	156.7	158.7375	156.7	A	Effective 01/01/2014	
Simplex/Direct	VTAC14		159.4725 N	156.7	159.4725	156.7	A	Effective 01/01/2014	
Duplex/Repeater	UCALL40		453.2125 N	156.7	458.2125	156.7	A	Effective 01/01/2014	
Simplex/Direct	UCALL40D		453.2125 N	156.7	453.2125	156.7	A	Effective 01/01/2014	
Duplex/Repeater	UTAC41		453.4625 N	156.7	458.4625	156.7	A	Effective 01/01/2014	
Simplex/Direct	UTAC41D		453.4625 N	156.7	453.4625	156.7	A	Effective 01/01/2014	
Duplex/Repeater	UTAC42		453.7125 N	156.7	458.7125	156.7	A	Effective 01/01/2014	
Simplex/Direct	UTAC42D		453.7125 N	156.7	453.7125	156.7	A	Effective 01/01/2014	
Duplex/Repeater	UTAC43		453.8625 N	156.7	458.8625	156.7	A	Effective 01/01/2014	
Simplex/Direct	UTAC43D		453.8625 N	156.7	453.8625	156.7	A	Effective 01/01/2014	
Duplex/Repeater	7CALL50		769.24375 N	\$F7E	799.24375 N	\$293	D	Effective 01/01/2014	
Simplex/Direct	7CALL50D		769.24375 N	\$F7E	769.24375 N	\$293	D	Effective 01/01/2014	
Duplex/Repeater	7TAC51		769.14375 N	\$F7E	799.14375 N	\$293	D	Effective 01/01/2014	
Simplex/Direct	7TAC51D		769.14375 N	\$F7E	769.14375 N	\$293	D	Effective 01/01/2014	
Duplex/Repeater	7TAC52		769.64375 N	\$F7E	799.64375 N	\$293	D	Effective 01/01/2014	
Simplex/Direct	7TAC52D		769.64375 N	\$F7E	769.64375 N	\$293	D	Effective 01/01/2014	
Duplex/Repeater	7TAC53		770.14375 N	\$F7E	800.14375 N	\$293	D	Effective 01/01/2014	
Simplex/Direct	7TAC53D		770.14375 N	\$F7E	770.14375 N	\$293	D	Effective 01/01/2014	
Duplex/Repeater	7TAC54		770.64375 N	\$F7E	800.64375 N	\$293	D	Effective 01/01/2014	
Simplex/Direct	7TAC54D		770.64375 N	\$F7E	770.64375 N	\$293	D	Effective 01/01/2014	
Duplex/Repeater	7TAC55		769.74375 N	\$F7E	799.74375 N	\$293	D	Effective 01/01/2014	
Simplex/Direct	7TAC55D		769.74375 N	\$F7E	769.74375 N	\$293	D	Effective 01/01/2014	
Duplex/Repeater	8CALL90	For FCC Part 90 licensees, the non-Federal National Interoperability Channels VCALL10-VTAC14, UCALL40-UTAC43, and 8CALL90-8TAC94 are covered by a "blanket authorization" from the FCC - "Public safety licensees ... can operate mobile units on these interoperability channels without an individual license." See FCC 00-348, released 10/10/2000, paragraph 90.	851.0125 W	156.7	806.0125	156.7	A	Effective 01/01/2014	
Simplex/Direct	8CALL90D		851.0125 W	156.7	851.0125	156.7	A	Effective 01/01/2014	
Duplex/Repeater	8TAC91		851.5125 W	156.7	806.5125	156.7	A	Effective 01/01/2014	
Simplex/Direct	8TAC91D		851.5125 W	156.7	851.5125	156.7	A	Effective 01/01/2014	
Duplex/Repeater	8TAC92		852.0125 W	156.7	807.0125	156.7	A	Effective 01/01/2014	
Simplex/Direct	8TAC92D		852.0125 W	156.7	852.0125	156.7	A	Effective 01/01/2014	
Duplex/Repeater	8TAC93		852.5125 W	156.7	807.5125	156.7	A	Effective 01/01/2014	
Simplex/Direct	8TAC93D		852.5125 W	156.7	852.5125	156.7	A	Effective 01/01/2014	
Duplex/Repeater	8TAC94		853.0125 W	156.7	808.0125	156.7	A	Effective 01/01/2014	
Simplex/Direct	8TAC94D		853.0125 W	156.7	853.0125	156.7	A	Effective 01/01/2014	
Direct	VFIRE21	WARNING: These frequencies are NOT covered by the blanket authorization for nationwide interoperability channels.	154.2800 N	156.7	154.2800	156.7	A	Effective 01/01/2014	
Direct	VLAW31		155.4750 N	156.7	155.4750	156.7	A	Effective 01/01/2014	
Direct	VMED28		155.3400 N	156.7	155.3400	156.7	A	Effective 01/01/2014	
Direct	Point to Point	Communications Centers	155.3700 N	DCS 271	155.3700	DCS 271	A	Effective 05/01/2016	
ICS Form 217A	These channels are recommended by the Iowa State Interoperable Communications System Board.				http://isicb.iowa.gov		3/17/2016		



Iowa Communications Network | Iowa Department of Public Safety
Iowa Statewide Interoperable Communications System Board

Wi-Fi Internet for School Emergencies

Pilot Program Study



Lieutenant Thomas Lampe, Bureau Chief—Interoperability-Communications Bureau
Iowa Department of Public Safety
July 31, 2017

Table of Contents

Acknowledgements.....	i
Executive Summary.....	i
I. Introduction.....	1
School Security Needs.....	1
Law Enforcement Mobile Data Needs.....	2
Need for Updated and Coordinated School Emergency Response.....	2
Iowa’s Available Resources.....	3
II. Cost Analysis.....	4
Vendor Costs and Quotes.....	4
Utilization of Existing Infrastructure.....	5
III. Vendor Performance.....	6
Pre-Deployment Testing.....	6
Product Comparisons.....	6
Recommendations.....	6
IV. Funding Needs Options.....	8
Grants.....	8
Cost Benefit.....	8
WISE Pilot cost reduction model examples.....	9
V. Findings.....	11
VI. School Official Comments.....	13
VII. Public Safety Comments.....	14
VIII. Capabilities That Will Come With the Expansion of WISE.....	15
Example Scenario Active Shooter: Current vs Desired State.....	15
IX. Conclusion.....	17
X. References.....	18
XI. Addendums/Appendices.....	19
Appendix A: Statement of Work.....	19
Appendix B: Vendor Quotes.....	20
Appendix C: Instructions to join networks.....	42

Acknowledgements

A pilot study such as Wi-Fi Internet for School Emergencies (WISE) is an ambitious program that would not have been possible without the hard work and dedication of the following individuals: Helen Troyanovich, Ric Lombard, Shawn Wagner, Jeremy Howard, Scott Pappan, Trooper Chuck McNally, Trooper Rodney Larson, Trooper Luke Valenta, Trooper Joseph Long, Sergeant David Halverson, Trooper Jared Rude, Trooper Aaron Taylor, Trooper Matthew Struecker, Trooper Cody Frank and Chris Maiers. The author would also like to thank Iowa Department of Public Safety (DPS) Commissioner Roxann Ryan, Trooper Nathan Rippey, Anthony Jenkins, Assistant Director Gerard Meyers, Sergeant Kevin Farver, Captain Randy Olmstead, Paul Stuber Ryan Mulhall and Marc Evans.

The time commitment from employees of the Iowa Communications Network (ICN), DPS and Iowa State Patrol (ISP) is graciously recognized.

ICN and DPS express thanks and gratitude to Norwalk High School, Martensdale-St. Mary's and Marshalltown High School for their willingness to participate in this program.

The authors of the WISE pilot also want to extend a sincere thanks to Aruba, Cisco and Fortinet for their employees' time and generous donation of equipment for this program.

For a video of the WISE program, click on the link below:

<https://www.youtube.com/watch?v=ACQdmICuqas>

Wi-Fi Internet for School Emergencies (W.I.S.E.) Pilot – Final Report

Executive Summary

The Wi-Fi Internet for School Emergencies (WISE) program was commissioned in 2016 by Governor Terry Branstad as a means to help secure school grounds and build safer communities across Iowa; provide public safety with secure, reliable and efficient broadband connections via existing Iowa Communications Network (ICN) fiber optic networks; increase the presence of public safety entities on school campuses as a deterrent to help prevent a tragedy such as those seen at Littleton, Colorado and Sandy Hook, Connecticut.

The installation of a secured Wi-Fi connection on school grounds brings several advantages for schools and emergency responders and cost-savings for the State of Iowa. The Wi-Fi network could also be used to upload dash camera video recorded during a shift from a state or local law enforcement officer (LEO) or to stream live video from a patrol car on scene. Schools Participating in WISE have a dedicated Wi-Fi network for first responders that could be used in the event of an emergency to access any cameras on campus via VPN in order to assess the situation and send video from the dash camera back to dispatch.

The presence of cameras and LEOs on school campuses has been found to be a deterrent to violence. In addition, the cost-savings noted by the Iowa State Patrol (ISP) could apply to other law enforcement agencies across Iowa with respect to time, mobile bandwidth usage and wear and tear on vehicles. For the ISP, the cost-savings amounted to the equivalent of twelve vehicle replacements per year and time savings that netted the equivalent of 13.7 extra full time employees (FTEs) on patrol per year.

No dollar value can be attached to preventing violence. However, given the above findings and many benefits stated above, DPS recommends schools in Iowa attempt to implement this technology to achieve the many benefits WISE provides. The deployment of this technology statewide is expected to increase officer efficiency when uploading dash camera video, increase deterrence at schools when LEOs will be on campus more frequently and improve relationships with schools, police and parents.

I. Introduction

School Security Needs

Since the beginning of the [Safe School Initiative](#) in 1999, school officials, law enforcement agencies, and subject matter experts, worked collaboratively toward developing an increasingly secure, safe, and healthy educational environment for children attending school. Iowa School Safety Resources have been developed and designed via multi-agency collaboration and made available at the following links:

HLSEM link: http://homelandsecurity.iowa.gov/programs/school_safety.html

DOE link: <https://www.educateiowa.gov/pk-12/school-facilities/safety-and-accessibility/emergency-operations-planning>

The Final Report and Findings of the Safe Schools Initiative (Vossekuil, Fein, Reddy, Borum, and Modzeleski 2002) published by the U.S. Secret Service and Department of Education found:

1. Incidents of targeted violence at school are rarely sudden, impulsive acts.
2. Prior to most incidents, other people knew about the attacker's idea and/or plan to attack.
3. Most attackers did not threaten their targets directly prior to advancing the attack.
4. There is no accurate or useful "profile" of students who engage in targeted school violence.
5. Most attackers engaged in some behavior, prior to the incident that caused concern or indicated a need for help.
6. Most attackers were known to have difficulty coping with significant losses or personal failures. Many had considered or attempted suicide.
7. Many attackers felt bullied, persecuted, or injured by others prior to the attack.
8. Most attackers had access to and had used weapons prior to the attack.
9. In many cases, other students were involved in some capacity.
10. Despite prompt law enforcement responses, most shooting incidents were stopped by means other than law enforcement intervention.

The [Indicators of School Crime & Safety 2016](#) (Musu-Gillette, Zhang, Wang, Zhang, and Oudekerk 2017) reports that, while safety measures are visibly improving, pockets of violence at schools are either steady or trending upward. In Iowa the number of reported incidents of students bringing a firearm to school grounds has remained relatively constant since the 2010-2011 school year with two to three incidences per year. This report also stated that in Iowa 11.2% of teachers were threatened with violence and 7.6% were physically attacked.

The Morbidity and Mortality Weekly Report published on June 10, 2016 by the Centers for Disease Control and Prevention (Kann, et al. 2016) found that while the national incident rate of school-aged children carrying a weapon (e.g., gun, knife or club) has fallen since 1991, it has held relatively steady since 2013. In 2015 16.2% of students reported carrying a weapon, and 5.3% had carried a firearm. Of those students surveyed, 4.1% reported carrying a weapon on school grounds, and 6.0% of students have been threatened or injured with a weapon.

Kann, et al. (2016) also reported that nationally 15.5% of students were electronically bullied, 20.2% were bullied on school grounds, 7.8% of students nationwide had been in a physical confrontation, 29.9% reported feeling sad or hopeless for two or more consecutive weeks, 17.7% seriously considered suicide, 14.6% actually drafted a suicide plan and 8.6% attempted suicide at least one time.

A 2008 U.S. Secret Service and Department of Education Study (Pollack, W.S., W. Modzeleski, and G. Rooney 2008) found variability in the likelihood that information that students learn regarding a peer's plan for a violent attack gets relayed to a trusted adult. This variability may be attributable to school culture.

Locally during the 2014-2015 school year, Iowa schools had to remove a student from school for a day or more 12,533 times (a rate of 1 for every 2,480 students). Of those, 277 (2.2%) involved alcohol, 1,945 (15.5%) involved illicit drug use, 9,546 (76.2%) resulted from a violent incident and 765 (6.1%) were due to possession of a weapon (Musu-Gillette, Zhang, Wang, Zhang, and Oudekerk 2017).

When those factors are coupled with emergency response for inclement weather events, fire hazards, local hazardous materials scenarios for critical infrastructure sectors (e.g. manufacturing, agriculture, and transportation); the need for public safety agencies to partner with school officials to develop innovative and cost-effective ways to enhance security for schools has never been greater.

Development of infrastructure such as security cameras within schools have been shown to decrease the probability of a confrontation within the school building (National Crime Prevention Council 2011). Students are more likely to intervene in fights if they have knowledge of cameras in the facility.

Law Enforcement Mobile Data Needs

Recently a need has developed with the advent and expansion of recording devices associated with law enforcement. During a typical shift, a law enforcement officer (LEO) would be required to upload the video from his or her dashboard and body camera (if equipped) to a central records management center for retention. The LEO can return to the local office for a direct download or upload it via an Internet connection. Driving to the agency office can require substantial time and equipment investment when wear and tear on vehicles and fuel consumption are considered. This is time in which LEO may not be able to patrol. Uploading video can also be network intensive depending on the number of files and their size and require robust speed and security.

Need for Updated and Coordinated School Emergency Response

Responding to an emergency in a school building (e.g. active shooter, fire or medical emergency) brings planning challenges due to potential unknown locations of attackers, fires or how many students and staff need medical attention. When an emergency occurs, mobile broadband networks have been crippled in the past with the sudden increase in users at the site. In addition, the cellular signal may not be able to provide adequate coverage inside of the school buildings. The launch of FirstNet will help alleviate some of those concerns, but the in-building coverage concerns at schools will likely remain. In addition, while current average mobile broadband speeds of 15-20 Mbs download and 6-12 Mbs upload are adequate for downloading and uploading video under normal conditions, a stark increase in users at a site may slow speeds further especially in a rural community with less network capacity.

WISE options may limit the costs associated with FirstNet in Iowa. Some agencies may choose to equip every squad car or emergency response vehicle with FirstNet capable devices, and some agencies may limit data packages, which could preclude LEOs from uploading their dash and body camera video in the field via a mobile broadband network like FirstNet, due to increased costs associated with uploading five or more gigabytes (GB) of data with each shift.

In addition, not every school in Iowa has a closed circuit camera network. Including a basic camera system in school as part of the WISE program may be beneficial to furthering school security given that cameras have been shown to act as a deterrent to violence. The cameras could also be accessed by law enforcement via VPN in the event of an emergency.

Iowa's Available Resources

Iowa is in the unique position nationally in that it has an existing fiber optic network connection to approximately 300 high schools across the state. Given this unique position, *How could state's existing assets be leveraged to improve operational security to our schools and expand broadband access for first responders in the most cost-effective way?* This was the impetus for the “Wi-Fi Internet for School Emergencies”, or *WISE Pilot* initiative. A Department of Public Safety (DPS) led project, the WISE Pilot utilizes existing fiber broadband infrastructure (Figure 1)¹, managed by Iowa Communications

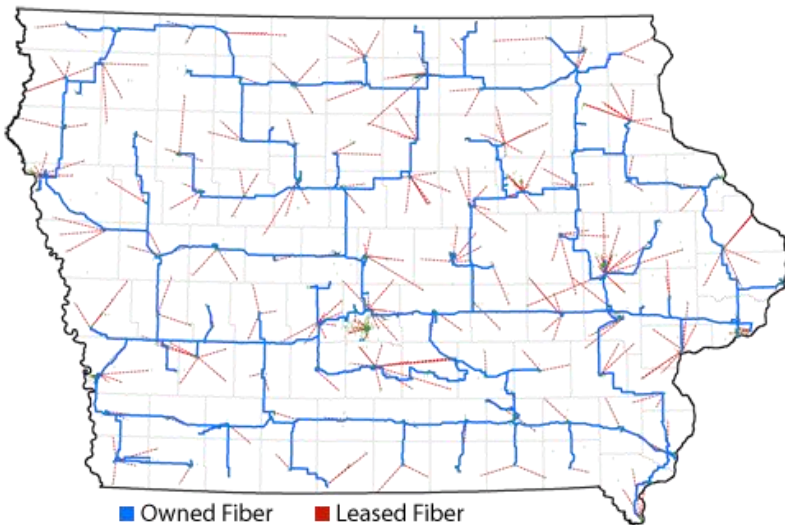


Figure 1. Map of the ICN fiber optic network.

Network (ICN), which is already in place at many Iowa schools. Three wireless access point (AP) equipment vendors agreed to participate in this one year pilot project, and dedicated equipment and resources through Scope of Work agreements to Iowa Communications Network, to assist ICN and DPS in developing dedicated, secure, private wireless internet access for public safety at three high school locations in Iowa—Marshalltown High School, Martensdale-St. Mary's High School and Norwalk High School ([Appendix A](#)).

This dedicated wireless broadband access, with speeds as high as 100 Megabits per second (Mbps) per site for uploads and downloads, is available to authorized state, regional, county, and local public safety agency personnel, both operationally (daily) and during an event (emergency). It ties into a dedicated ICN circuit that is not part of the school's general Internet connection. During operational use, LEOs could stop by the school to upload their daily video. The deterrent of law enforcement presence on campus became clear within days of roll out. Although the WISE Pilot network was not put to the test with an actual catastrophic event during the trial period, the bandwidth speed withstood high capacity video uploads. A YouTube video highlighting the WISE Pilot can also be found at <https://www.youtube.com/watch?v=ACQdmICuqas>.

¹ Map available at <https://icn.iowa.gov/about-icn/agency-information-icn-story>.

II. Cost Analysis

Vendor Costs and Quotes

The three school sites needed to add infrastructure for the WISE program. Three vendors donated AP equipment to make the WISE Pilot possible. Each vendor was given an identical quote scenario from which to provide an estimate cost sheet to include in this report. Please note the estimates below are non-binding and may include general list or book pricing, and do not reflect state contract rates, if applicable. See [Appendix B](#) for cost sheets for outdoor only and indoor/outdoor coverage.

Scenario 1: Price range for cloud management with minimal equipment expenditures up to on-site server management at Norwalk High School, outdoor coverage and a three-year license term:

- Aruba: \$3,182.00 - \$7,522.00
- Cisco: \$6,438.00 - \$8,438.00
- Fortinet: N/A

If these costs in *Scenario 1* are extrapolated for the other 300 schools around Iowa with ICN access, the total cost to deploy the WISE program statewide would be:

- Aruba: \$954,600 - \$2,256,600
- Cisco: \$1,931,400 - \$2,531,400
- Fortinet: N/A

While the outdoor APs would provide some indoor coverage, the network at the school could be expanded to include indoor access. However, robust indoor coverage would substantially increase the cost of the program. The question remains whether indoor coverage would be needed in most schools. The second scenario below illustrates the costs associated with indoor coverage added to schools.

Scenario 2: Norwalk High School, complete indoor/outdoor coverage, 65 APs, three-year license term:

- Aruba: \$60,400
- Cisco: \$127,665
- Fortinet²: \$48,130 - \$52,802

If these cost in *Scenario 2* are extrapolated out for the other 300 schools around Iowa with ICN access, the total cost to deploy the WISE program statewide would be:

- Aruba: \$18,120,000
- Cisco: \$38,299,500
- Fortinet²: \$12,939,000 - \$15,840,600

These cost estimates are based solely on the single quote from Norwalk High School. They do not reflect and bulk discounts that would be granted based on a significantly larger purchase. The statewide estimates do not account for size and layout of schools across Iowa.

² Range of price is given due to Fortinet offering two configurations.

Utilization of Existing Infrastructure

The schools already have access to the ICN and service contracts. That would eliminate any potential for additional monthly data access fees associated with this type of broadband service. Any impact on a system such as the ICN is expected to be minimal.

Some schools already have an existing network of cameras. Tying the existing camera video server to the school's network for streaming over WISE and a VPN connection would bring a one-time cost for set-up which is not included in this report. After that, there would be no additional on-going costs associated with operating the cameras that schools are not already funding.

III. Vendor Performance

Pre-Deployment Testing

During the process of receiving price quotes from vendors, computer modeling of Wi-Fi signals were performed to gain an understanding of how wireless AP placement would affect coverage (Figure 2). These models proved beneficial in assessing the needs of each school.

Product Comparisons

The supplied equipment by three vendors was assessed by making notes of the setup process including configuration and resolved and unresolved issues.

It was found that Cisco equipment was very simple to setup and configure. Problems surfaced regarding 802.1x authentication outside the intended domain users were assigned to. Overall system performance was good, but the authentication issues were never resolved. The Cisco system support proved to be adequate.

The Aruba equipment was diverse and secure. It was moderately simple to setup. 802.1x authentication was easily configured and tested successfully. Aruba was the only equipment that was able to undergo a user load test. Performance was good, and there are no outstanding issues with this system and support was excellent.

Fortinet offered a secure system that was moderately easy to set up. 802.1x authentication was not tested on the product. Performance was good despite a lack of certificate authentication testing. The prices were also very competitive.

Recommendations

The Aruba system was found to be the most effective solution when installation, performance and support were investigated. The Aruba platform is also what the ICN uses for their networking needs.

Newer field laptops with 802.11ac or 802.11n Wi-Fi adapters are preferred given the faster performance capabilities. However, users must ensure that all wireless network card drivers are up-to-date to ensure performance levels are adequate. It should also be verified that wireless cards were not configured to prefer 5 GHz rather than 2.4 GHz. The correct channel width and speed settings should also be verified.

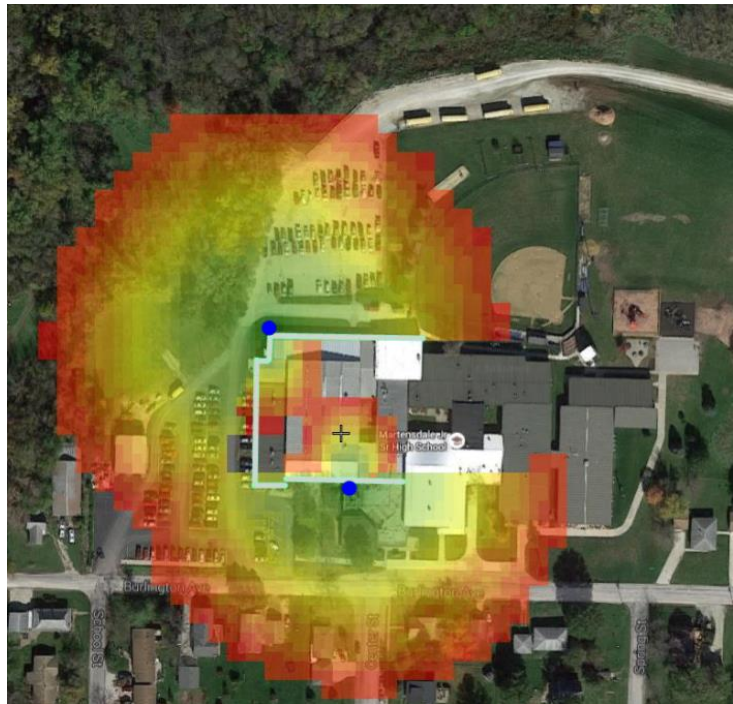


Figure 2. Sample of wireless network coverage modeling at Martensdale-St Mary's Junior and Senior High School.

It was also found that in order to fully utilize the speeds associated with the ICN, wireless cards in field computer equipment should be dual-band. This allows access to the faster 5 GHz Wi-Fi connections for video uploads and data transfers where possible.

IV. Funding Needs Options

Grants

Grants for school safety through integration of technology, although harder to obtain recently, are still available through both government and private entities. Available grant funding depends on timing and other factors, such as urban or rural locations, economic markers such as free or reduced cost lunch recipients, or size and area of coverage selected. Grant funding generally covers one-time costs for initial installation of networks, but seldom cover recurring costs necessary for software licensing and hardware maintenance, configuration changes, and 24x7x365 support required for critical infrastructure sector networks.

The on-going costs would focus on maintenance and administration of the installed wireless APs. Those included cloud management, identity authentication and general maintenance of equipment. Those costs varied with each vendor and ranged from a few hundred dollars for the outdoor only solutions to over \$25,000 for indoor and outdoor coverage.

Cost Benefit

For daily operations, the greatest cost benefit realized during WISE Pilot was reducing trooper drive time and mileage to upload vehicle mobile video units. Figure 3 is a map of Iowa displaying high schools with ICN Part III connections and their proximity to DPS District Offices. In actuality, the farther away the school is located from District Offices, the greater the benefit. Further, DPS field leaders could more readily recognize priority areas where WISE network APs could generate the highest cost savings when deployed efficiently following the WISE Pilot cost reduction model. This could add a level of deterrence to schools that may be farther away from a local District or Sheriff's Office.

This pilot study acknowledges that the concept of deterrence of violence on school grounds is beneficial but cannot be quantified via cost-savings. However, the lack of quantifiable savings with respect to deterrence should not outweigh the other benefits such as added capabilities of emergency response at schools and cost-savings noted by law enforcement agencies.

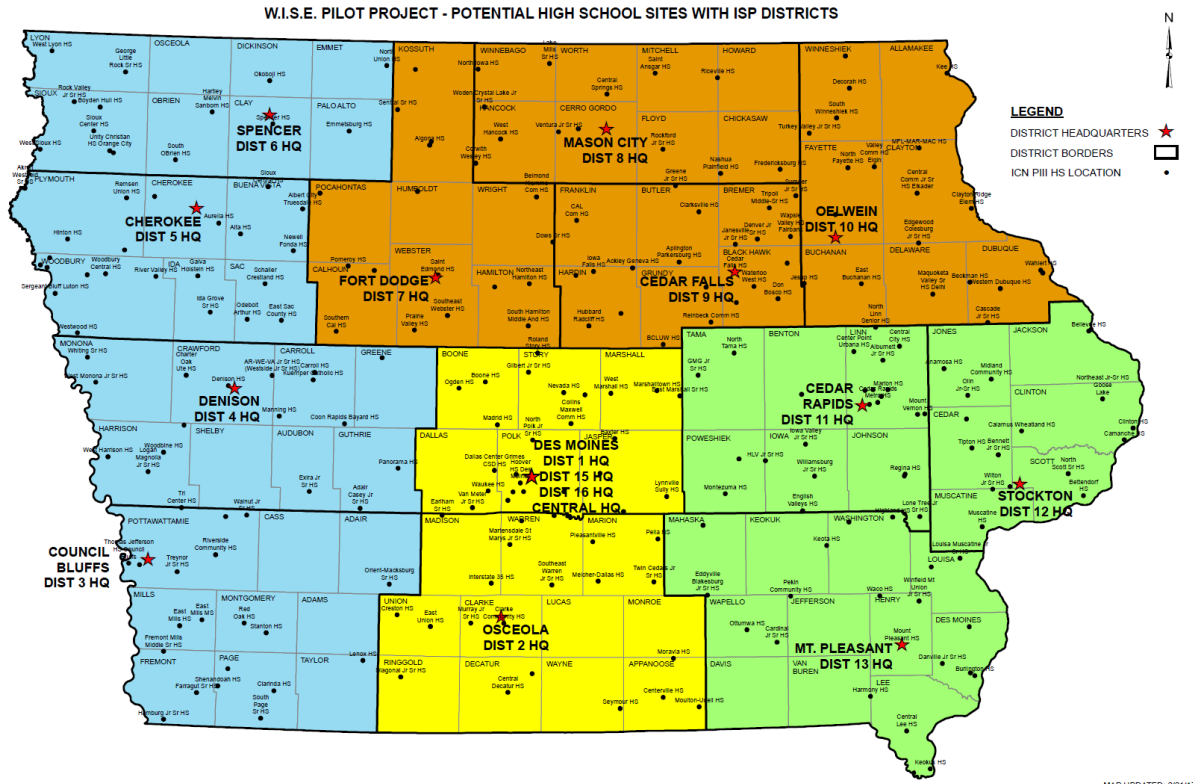


Figure 3. Map of ISP Posts and high schools with ICN Part III access that could serve as future WISE locations.

WISE Pilot cost reduction model examples

The WISE Pilot was able to quantify the miles saved per trip from trooper domicile to upload video for ISP district troopers. By utilizing a WISE Pilot AP (sign-in instructions are in [Appendix C](#)) to upload in-vehicle mobile video, the following savings in mileage per shift³, time and salary were noted in Table 1. A complete listing of the savings by each trooper is compiled in Table 2.

School	Number of Troopers	Total Daily Miles Saved ⁴	Total Daily Time Saved (hours) ⁵
Marshalltown	4	134.7	2.45
Martensdale-St. Mary's	3	51.9	0.94
Norwalk High School	4	58.1	1.06
Daily Totals	11	244.7	4.45

Table 1. Listing of WISE schools, use by troopers, mileage and time savings.

Given that these totals are only for a select group of troopers (eleven), this can be scaled to the entire force. Using the median salary of a trooper (\$28.66) as an estimate for cost savings, average daily cost savings for a single state trooper using a WISE site to upload their video is \$11.60 using the average daily

³ Only miles for a one-way trip from domicile to district office or school facility were counted.

⁴ Combined miles of troopers using the school site.

⁵ Assuming an average travel speed of 55 mph.

time savings of 0.40 hours each day. If this level of savings is applied to the approximately 270 troopers currently on patrol, the time savings scales up to potentially 109.23 hours of extra patrol time per day worked. Extrapolated out a full year (250 working days) nets a potential savings of 27,307.5 hours in reduced travel time that can be reallocated to patrolling the roads in Iowa. This is the equivalent of having an extra 13.7 FTEs patrolling. If a median salary of a trooper of \$59,602.40 is applied to those potential time savings as defined by FTEs, a net cost savings of \$816,552.90 is realized.

The average miles saved by a trooper each day in this study is 22.25 miles. Scaled up to the force of the patrol (approximately 270 troopers), a daily mileage savings of approximately 6,007.5 miles is realized. This approximates to 1,506,166.07 miles saved in a year assuming those 270 troopers are patrolling five days per week. If a 120,000 mile replacement interval on a trooper's vehicle is assumed, this savings results in twelve (12) fewer vehicle purchases each year. At a cost of approximately \$25,000 for each vehicle (Dodge Charger), that nets \$300,000 in savings for vehicles alone. This does not account for the time required to upgrade each vehicle for police work.

School Site	Miles to District Office	Miles to WISE School	Miles Saved
Marshalltown High School	48.6	2.0	46.6
Marshalltown High School	48.6	2.0	46.6
Marshalltown High School	39.0	15.6	23.4
Marshalltown High School	52.4	34.3	18.1
Martensdale-St. Mary's	26.1	2.7	23.4
Martensdale-St. Mary's	30.4	16.4	14.0
Martensdale-St. Mary's	49.7	35.2	14.5
Norwalk High School	26.1	6.1	20.0
Norwalk High School	30.4	24.9	5.5
Norwalk High School	49.7	37.1	12.6
Norwalk High School	26.1	6.1	20.0

Table 2. Listing of schools, miles to district office from a trooper's domicile, miles to school from a trooper's domicile and miles saved by the trooper using the school to upload data rather than commuting to the nearest district office.

This does not account for the savings that other police departments and sheriff's offices could also realize with the implementation of the WISE program. Local municipal police departments could utilize the faster upload times offered by the ICN as a means to increase patrol time and time efficiency during a shift. The sheriff's office would likely see savings both with time and mileage which leads to lower overhead costs associated with vehicle purchases and maintenance.

V. Findings

The WISE program has been found to mutually benefit both schools and public safety stakeholders. Having multiple LEOs appearing on a school campus every day also serves as a deterrent to violence. Having a network of cameras and a secure and reliable means of transmitting the data to public safety personnel onsite and remotely increases officer efficiency by reducing drive time and miles traveled. Public safety personnel can also quickly assess any situation that may be reported in order to gain perspective on the event scale and scope.

Trooper Valenta stated that several school districts and counties may have unique agreements for a law enforcement presence at schools. He compared Martensdale to Norwalk, “Martensdale is a contract town. So, the Sheriff’s Office is required by their contract to provide so much presence. So, a lot of times they’ll show presence in that town but they have to be there per the contract. If you had a WISE System in that town, they’d be able to fulfill their contract obligations while they’re still there uploading their videos so they wouldn’t have to make an extra trip to town or into their Sheriff’s Office if they didn’t need to.”

Using WISE to upload dash camera video from ISP troopers dramatically cuts down on needed drive time and miles on vehicles. It also provided a secure network for trooper computers to securely connect to the Internet to upload sensitive materials such as video and field reports.

Each individual school’s utilization of the WISE network to upload data varied with the number of Troopers stopping by to utilize the service. Each school saw a maximum of three users. During those months, the WISE Sites saw peak or near-peak usage (Table 3):

School	Month	Users	Data Transferred (GB)	Average Daily Use (GB)
Martensdale-St. Mary’s	February 2017	3	25.06	0.90
Martensdale-St. Mary’s	March 2017	3	18.43	0.59
Marshalltown High School	May 2017	3	31.24	1.01
Marshalltown High School	March 2017	2	43.96	1.42
Norwalk High School	May 2017	3	27.68	0.89
Norwalk High School	February 2017	2	9.26	0.33

Table 3. Listing of the schools, months with peak or near-peak usage and number of users for each WISE site.

Utilization of the WISE network for uploads of dash camera video is expected to increase as more troopers, LEOs and sheriff deputies find WISE sites as a convenient and time-efficient means of uploading video recorded during a shift.

Some initial firmware and software settings in computer consoles prevented full utilization of upload capabilities. These problems were addressed via firmware and driver updates and modified software settings. This added efficiency to data transfers that cut down on the amount of time troopers had to allot for uploads at the end of a shift. This allowed them to spend more time patrolling.

A sweet spot in signal coverage for schools was also found. The network needs to be configured in such a way so the signal only covers the building and adjoining parking lots so it does not spill into streets. This prevents an issue with ISP troopers’ computers from connecting to the network at an intersection and causing programs to hang due to a loss of connectivity when the trooper drives away from the school.

Some of those concerns can be addressed by properly using current Wi-Fi bands in 2.4 GHz and 5 GHz. The 2.4 GHz signal is great for applications that face obstructions such as indoor coverage. The 5 GHz signal allows for faster data transfers and does not propagate as far as 2.4 GHz due to attenuation. In this case, 5 GHz would be best-served for outdoor networks such as parking lots, and 2.4 GHz would work best indoors.

VI. School Official Comments

"Marshalltown high school is excited to continue its collaboration with the emergency responders in our county. Having the ICN infrastructure in our building and utilizing it to its greatest capacity is also a wonderful foresight for our state and for providing safety to the children in our school district," Jacquie Wyant, principal at Marshalltown High School, said. The reception at Marshalltown High School was positive overall, and she believes the program should be implemented statewide given that an emergency situation such as an active shooter could happen anywhere.

Principal Wyant stated, "It makes perfect sense to me to be a part of this program." No disruptions to a normal school day were noted while the WISE Program was being implemented and tested. Principal Wyant was also pleased with some unexpected benefits such as traffic slowing down by the school when a LEO was present. She also noted that students may be discouraged from skipping out of school if they saw a LEO present or knowing that a LEO may arrive at random times.

Principal Wyant also noted that the network performed well at Marshalltown High School. All students have a device such as a laptop or tablet that can access the school Wi-Fi. The general use school Wi-Fi network uses the same ICN connection as WISE. No performance lags were noted during times the network was used.

Tim Geyer, Norwalk High School Technology Director, affirmed that the WISE Pilot worked well and was not intrusive to normal school operations. There were no issues with the network being bogged down by user uploads as well.

Mr. Geyer noted the police presence on campus, "I see their cars in the parking lot every now and then, and that's a good thing." He added that the LEOs using the network seemed to love it.

Mr. Geyer offered a suggestion regarding AP placement. The suggestion focused on proper placement of the AP to ensure the LEO is visible. This would maximize the potential deterrence. He also noted that a separate ICN circuit may not be needed for all schools depending on their use.

VII. Public Safety Comments

Iowa State Patrol Trooper Luke Valenta⁶ offered feedback regarding several aspects of the program. He first noted the experience of being able to drive up to the school and download or upload data on site without leaving his squad car, “I can literally upload two hours of video in less time than it would actually take just to drive to the office.”

“With the computers having an air card, we can still upload from the car as normal. But with video, it's just such huge files that it would just take forever unless you're actually on a T-1 hard line or using a WISE System. So, the smaller forms are not as essential, as far as like they upload normally whether you're at the office or just driving around, but the larger files, like video files from the in-car camera, are what really make a big difference as far as you would either have to drive the office then remove it from the trunk unit and actually take it in physically to the office and hook it up to the computer. It's much simpler using the WISE System, you can just drive up to it go to the same screen on the program and never have to take it out of the trunk or anything, just hit the upload button in the program.”

Trooper Valenta also commented on the noted differences between using a public Wi-Fi network from a local business. Much of his feedback focused on the speed of the transfers.

“WISE is much faster in comparison, just because where I'm at, close to a large metropolitan area where it already has a good cell phone coverage, so the air card in the computer is already at a faster rate. Whereas a normal Wi-Fi, you really don't see any difference at all between using a Wi-Fi from a business or just with the air card in the computer where I'm at. But with that said, the WISE itself is much faster.

Trooper Valenta noted the improved performance of data transfers as stakeholders grew familiar with the program and how to create efficiencies in the network configuration.

“Initially when it first started, it was OK. I had quite a bit of video to upload and it took quite a bit of time but through the course of the testing they found some different things that they could tweak some different settings on the computer and updating some drivers. So, after they tweaked it a little bit it was much, much faster, it's actually faster than going to the office and use the hard line.”

⁶ Video of interview available at: https://www.youtube.com/watch?v=eC_86zEdyM8

VIII. Capabilities That Will Come With the Expansion of WISE

The added capabilities of WISE complement the current and future capabilities of communication systems that can be integrated together to achieve total interoperability within the State of Iowa such as the Iowa Statewide Interoperable Communication System (ISICS) and FirstNet. If the WISE program is adopted state-wide, large-scale planning can commence that would allow for emergency response plans and drills at schools that can address problems associated with various indoor events (e.g. basketball and volleyball games; musical, drama and theater productions), outdoor events (e.g. football games, baseball games and track and cross country meets) and day-to-day activities within the school. These drills and events could include newer technologies such as wireless body cameras, drones to fly over school to repeat signal into hard to reach areas on school grounds. These large-scale emergency response plans and drills at schools that can be integrated with ISICS and FirstNet to complete the triumvirate of public safety communications.

Once ISICS is fully deployed, schools could have a radio in the offices and/or select classrooms with an emergency button. If a situation unfolds, the staff could press the button and immediately reach all the near-by police, fire and medical personnel that are available. This would dramatically shorten response time.

In the event of an incident that would require a multiple department response such as an active shooter, the ability to rapidly disseminate information to first responders is very valuable. Having streaming video feeds allows for any incident response to be more efficiently coordinated by assessing:

1. Incident location
2. Incident evolution
3. Number and types of casualties
4. Any need for special weapons and tactics (SWAT) teams and where to send them
5. Specific number of fire and medical personnel needed
6. Live streaming from school or event center cameras to incident command

The deployment of a network such as WISE may also bring several unexpected benefits for stakeholders. These could include improved student conduct due to presence of cameras, increased situational awareness in the event of an incident response which may also increase parents' confidence in emergency response at schools and improved community relations with first responders. An improvement in motorists' compliance with posted speed limits and other traffic laws were also noted when a LEO was present.

Example Scenario Active Shooter: Current vs Desired State

Current State

Today in most schools if an active shooter entered the facility and opened fire, students or staff would have to call 9-1-1 and state the situation. The intensity of the incident would likely induce a panicked state in the caller(s), and information relayed would potentially be incomplete or incorrect. A large-scale police and paramedic response would ensue with very little understanding of how many shooters are present, the number of casualties and if the event is still unfolding. Increased cellular congestion would shut down the usability of the current cellular network in the area. Fragmentation among the various counties and municipalities would make interoperable communication via LMR difficult.

No full assessment of the situation would be available until a SWAT team is sent into the building with little knowledge of the layout or status of the event.

Emergency medical coordination would be impossible via cellular phone calls and possibly LMR communication without a statewide network for interoperable communication such as ISICS.

Desired State

In the desired state with the expansion of WISE if the same event unfolded at a school, the school office could press the emergency button on the radio to immediately alert a dispatch center, police, fire and medical personnel via ISICS. The dispatcher may be able to log in remotely via VPN to view any cameras connected to the WISE network to assess the situation such as the number and location of shooters and victims along with whether the event is still unfolding. If that capability did not exist at the dispatch center, a responding LEO could log into the WISE network and view the cameras through a VPN connection and notify the dispatcher of how the event is evolving. That information could be relayed via ISICS to every responding officer, deputy, trooper and paramedic.

Once on-scene police and paramedics could log into the WISE network to stream cameras to assess the situation. Proper coordination could take place to neutralize the shooter or shooters, assess the situation for safety of medical and fire personnel and coordinate a thorough emergency medical response.

Advanced calls could be placed to hospitals by paramedics on scene via ISICS or by using a FirstNet-enabled smart phone. Coordination of where victims are taken to for treatment could take place much earlier in the scenario which would save lives.

Police would be able to post updates from the field on various social media outlets to allow coordination with parents on where to pick up their kids via the WISE network at the school or FirstNet.

IX. Conclusion

The WISE Program has been shown to be a benefit for schools and public safety stakeholders in this initial test. The presence of law enforcement on campus at random times serves as a deterrent to violence. Other unexpected benefits were noticed including drivers obeying posted speed limits. It seems likely that students may also be less likely to skip out of school if a LEO is present on campus.

The WISE program is also a means to fully utilize the ICN. WISE provides a means to get more use out of a network schools are already paying to access.

The WISE network also benefited the law enforcement agencies who utilized it. They noted less travel time to their local office to upload video which saved mileage and wear and tear on squad vehicles. The time savings also allowed for more time on patrol. The network connections that were provided through WISE were faster than wireless broadband cards and secure, unlike public Wi-Fi networks. The bandwidth was also reliably available in the event of an emergency.

Given the benefits of this program, it is recommended that the WISE Pilot be expanded to every school with ICN access across Iowa.

X. References

Vossekuil, B, R.A. Fein, Ph.D., M. Reddy, Ph.D., R. Borm, Psy.D., W. Modzeleski. 2002. *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States*. Washington, D. C.: United States Secret Service and United States Department of Education.

Musu-Gillette, L, A. Zhang, K. Wang, J. Zhang, B.A. Oudekerk. 2017. *Indicators of School Crime and Safety: 2016*. Washington, D.C.: United States Department of Education and United States Department of Justice Programs.

Kann, L, T. McManus, W.A. Harris, et al. *Youth Risk Behavior Surveillance — United States, 2015*. *MMWR Surveill Summ* 2016;65(No. SS-6506).

Pollack, W.S., W. Modzeleski, G. Rooney. 2008. *Prior Knowledge of Potential School-Based Violence: Information Students Learn May Prevent a Targeted Attack*. Washington, D.C.: United States Secret Service and United States Department of Education.

National Crime Prevention Council. 2011. *Be Safe and Sound: A Case-Study Evaluation of the Program Based on Experiences of Nine Pennsylvania Schools*. Arlington, VA.

XI. Addendums/Appendices

Appendix A: Statement of Work

Project Name: Dept. of Public Safety wireless POC
Customer: Dept. of Public Safety
Contact Name: Jeremy Howard
Customer Address: 400 East 14th Street
Contact Phone: (515) 725-4081
Customer City, St, Zip: Des Moines, IA 50319
Contact Email: jeremy.howard@iowa.gov
Date: April 6, 2016

OVERVIEW

Time frame to begin the project is to be determined; thus, completion date is to be determined. Iowa Communications Network (ICN) is prepared to begin working on this project, and will make every reasonable effort to complete the work as defined in the Statement of Work (SOW) and provide the deliverables as defined in the Statement of Work.

This work is to be performed for Department of Public Safety (DPS) by Iowa Communications Network (ICN) for the installation of the Enterprise Solution. The services will be delivered on-site as applicable. Some or all work may be performed remotely.

All service is to be provided to DPS during normal business hours (8-5 Mon-Fri), unless otherwise noted. This installation will take place at a designated date and time.

Pre-installation Consulting and Planning

- Prior to commencing work an ICN engineer and/or Project Manager will contact School.
- ICN will review with the School the implementation activities to be performed.
- ICN will explain the roles and responsibilities of Schools personnel and agree on the corresponding project schedule.

Scope Of Work

ICN has constructed the configuration of a Wireless solution for DPS that meets three objectives Customer has of the wireless technology; ease of use for the end user, secure and optimal coverage. The application is to be used to greatly improve the time it takes for public safety officers to upload video content from the present process and tools available. With the wireless solution, the officer will be able to drive to any respective school location as designated, automatically and securely associate to the wireless network and upload video content in a greatly reduced period of time. ICN is working with DPS to perform a proof of concept (POC) to utilize wireless technology to substantiate the effectiveness of the vendors solution. The equipment for the POC includes a wireless controller, outdoor access points, and a virtualized wireless Management instance. The wireless controller will terminate all of the outdoor POC access points to serve specified wireless clients. The wireless controller will also be implemented to aid in managing, monitoring, alerting and troubleshooting of the wireless network.

Prerequisites:

- ICN will work with DPS and School to accurately capture a location to perform the wireless POC.
 - Provide Google earth images outlined with coverage requirements
- ICN will work with DPS and School to accurately capture all requirements to make the outdoor wireless solution secure, easy to use with fast data transmission reliability.

ICN Statement of Work:

Generated Tuesday, April 6 2016

- ICN will work with School and vendor onsite or remotely to implement, configure and test the wireless controller and wireless management tool.
- ICN will work with School and vendor to minimize disruption to daily school activities. All activities will be done and scheduled with the school unless otherwise agreed upon.
 - This wireless controller will be installed in the ICN room at the respective school unless otherwise agreed upon
 - Perform installation of the wireless controller and confirm connectivity
 - Perform installation of the wireless Management Platform and confirm connectivity
 - Configure AP's according to DPS requirements
 - Integrate POC controller and AP's into solution at school.
 - Test AP connectivity
 - ICN is providing roof top temporary mounting hardware for the wireless access points. These temporary mounts are non- invasive to the schools structure and will be placed and cabled according to schools approval.
 - ICN to perform an outdoor wireless survey of proposed location after the installation is complete (coverage optimization)
 - Configure up to (2) wireless clients for DPS to test
 - Wireless access point location and coverage will accompany this SOW.

Appendix B: Vendor Quotes

Outdoor Quotes

ICN / Single School Pricing Options for Outdoor Coverage Considerations

Pricing includes 2 outdoor APs and associated mounting hardware.
 Pricing does not include centralized controller.
 Pricing does not include AOS 8 Mobility Master.
 Pricing does not include ClearPass or Airwave for Network Access and monitoring.
 Pricing does not include any discounts.

Option 1 - Instant Only Deployment					
Line#	Part Number	Description	Unit Price	Quantity	Total
1.00	JX967A	Aruba AP-365 (US) Outdoor AP	\$1,295.00	2	\$2,590.00
1.01	H4XN9E	Aruba 1Y FC NBD Each AP 365 SVC [for JX967A]	\$57.00	2	\$342.00
1.02	JW053A	AP-270-MNT-V2 AP-270 Series Outdoor Pole/Wall Short Mount Kit	\$125.00	2	\$250.00
Quote Total					\$3,182.00

Notes: Does not provide PoE power source, school would need PoE switches
 Does not provide centralized management, each school would be managed separately

Option 2 - Instant / Central					
Line#	Part Number	Description	Unit Price	Quantity	Total
1.00	JX967A	Aruba AP-365 (US) Outdoor AP	\$1,295.00	2	\$2,590.00
1.01	JW053A	AP-270-MNT-V2 AP-270 Series Outdoor Pole/Wall Short Mount Kit	\$125.00	2	\$250.00
2.00	JY925AAE	Aruba Central DM 1 Token 1y Sub E-STU	\$100.00	2	\$600.00
Quote Total					\$3,440.00

Notes: Does not provide PoE power source, school would need PoE switches

Option 3 - 7005 Controller					
Line#	Part Number	Description	Unit Price	Quantity	Total
1.00	JX967A	Aruba AP-365 (US) Outdoor AP	\$1,295.00	2	\$2,590.00
1.01	JW053A	AP-270-MNT-V2 AP-270 Series Outdoor Pole/Wall Short Mount Kit	\$125.00	2	\$250.00
2.00	JW634A	Aruba 7005 (US) 4-port 10/100/1000BASE-T 16 AP and 1K Client Controller	\$1,495.00	1	\$1,495.00
2.01	H2ZT1E	Aruba 1Y FC NBD Exch 7005 Controller SVC [for JW634A]	\$231.00	1	\$693.00
2.02	JW471AAE	Aruba LIC-ENT Enterprise (LIC-AP LIC-PEF LIC-RFP and LIC-AW) License Bundle E-LTU	\$300.00	2	\$600.00
2.03	H2XW3E	Aruba 1Y FC 24x7 License Cn Bundle SVC [for JW471AAE]	\$46.00	2	\$276.00
Quote Total					\$5,904.00

Notes: Does not provide PoE power source, school would need PoE switches
 Provides onsite controller capable of SD-WAN connection back to core controller.
 Can be managed by AOS 8 Mobility Master

Option 4 - 7008 Controller					
Line#	Part Number	Description	Unit Price	Quantity	Total
1.00	JX967A	Aruba AP-365 (US) Outdoor AP	\$1,295.00	2	\$2,590.00
1.01	JW053A	AP-270-MNT-V2 AP-270 Series Outdoor Pole/Wall Short Mount Kit	\$125.00	2	\$250.00
2.00	JX928A	Aruba 7008 (US) 8p 100W PoE+ 10/100/1000BASE-T 16 AP and 1K Client Controller	\$2,595.00	1	\$2,595.00
2.01	H4VP9E	Aruba 1Y FC NBD Exch 7008 Bch Cntrl SVC [for JX928A]	\$402.00	1	\$1,206.00
2.02	JW124A	PC-AC-NA North America AC Power Cord	\$5.00	1	\$5.00
2.03	JW471AAE	Aruba LIC-ENT Enterprise (LIC-AP LIC-PEF LIC-RFP and LIC-AW) License Bundle E-LTU	\$300.00	2	\$600.00
2.04	H2XW3E	Aruba 1Y FC 24x7 License Cn Bundle SVC [for JW471AAE]	\$46.00	2	\$276.00
Quote Total					\$7,522.00

Notes: Provides POE sufficient to cover both external APs

Provides onsite controller capable of SD-WAN connection back to core controller.

Can be managed by AOS 8 Mobility Master

Price Estimate



Joshua Harrington
 Cisco Systems, Inc.
 1089 Jordan Creek Parkway, Suite 210
 WEST DES MOINES, IOWA-50266
 UNITED STATES
 Ph no: +1 408 894 7867

Cisco Systems, Inc.
 1089 Jordan Creek
 Parkway, Suite 210
 WEST DES MOINES, IOWA-
 UNITED STATES
 Ph no: +1 408 894 7867

Price Estimate for planning and information purposes only and is not a binding offer from Cisco.

Date : 18-Jul-2017

Estimate ID: BR73550877AU
 Deal ID: NA

All Prices Shown in USD

Line Number	Part Number	Description	Service Duration (Months)	Lead Time	Unit List Price	Qty	Unit Net Price	Disc(%)	Extended Net Price
1.0	MR74-HW	Meraki MR74 Cloud Managed AP	---	7	1,399.00	1	1,399.00	0.00	1,399.00
2.0	MR84-HW	Meraki MR84 Cloud Managed AP	---	3	2,399.00	1	2,399.00	0.00	2,399.00
3.0	LIC-ENT-1YR	Meraki MR Enterprise License 1YR	---	3	150.00	1	150.00	0.00	150.00
4.0	LIC-ENT-3YR	Meraki MR Enterprise License 3YR (First Year On Us)	---	3	300.00	1	300.00	0.00	300.00
SubTotal									4,248.00
5.0	MX65-HW	Meraki MX65 Cloud Managed Security Appliance	---	3	945.00	1	945.00	0.00	945.00
6.0	LIC-MX65-SEC-1YR	Meraki MX65 Adv Security License 1YR	---	3	650.00	1	650.00	0.00	650.00
7.0	LIC-MX65-SEC-3YR	Meraki MX65 Adv Security License 3YR (First Year On Us)	---	3	1,300.00	1	1,300.00	0.00	1,300.00
SubTotal									2,895.00
8.0	MS220-8-HW	Meraki MS220-8 Cloud Managed 8 Port GigE Switch	---	3	985.00	1	985.00	0.00	985.00
9.0	LIC-MS220-8-1YR	Meraki MS220-8 Enterprise License 1YR	---	3	55.00	1	55.00	0.00	55.00
10.0	LIC-MS220-8-3YR	Meraki MS220-8 Enterprise License 3YR (First Year On Us)	---	3	110.00	1	110.00	0.00	110.00
SubTotal									1,150.00

Valid through
 FOB Point: None
 Note:

Product Total 8,293.00
Service Total : 0.00
Subscription Total 0.00
Total Price: 8,293.00

Signed: _____
 Joshua Harrington

This Price Estimate does not constitute an offer by Cisco to sell products, but is instead an invitation to issue a purchase order to Cisco until the valid date specified in this Price Estimate. Such a purchase order will be subject to Cisco standard procedures, terms and conditions for the acceptance of purchase orders. This order may be subject to sales tax, VAT, duty and freight charges even if not noted on this estimate.

1201 North Avenue, Norwalk, IA Aruba Wireless POC Project

Overview:

DataVizion will be performing an outdoor Aruba wireless Proof of Concept(POC) which will be used for the Department of Public Safety (DPS) at the location of 1201 North Avenue, Norwalk, IA. DPS is looking for a wireless solution that will allow ease of use, reliable and a secure transfer method to offload data from their vehicle to DPS servers. For the POC, we will be utilizing (1) Aruba 7010 Mobility Controller, (2) AP-275's and (2) AP-275 mounts. DataVizion will be providing Iowa Communications Networks (ICN) with full support for the duration of the POC.



1201 North Avenue, Norwalk, IA Aruba Wireless POC Project

Below is an overview of the two proposed AP locations. All locations are defined individually throughout this report for more in depth information.



Main Server Room Bullet Point Information:

- Main Server room is located at the RED TAC
- 7010 Aruba Controller Installation Location
 - Will rack mount equipment – Plenty of room
 - Power is available
 - An Ethernet run will be needed from ICN's hardware to the main server room Aruba Controller
 - Two outdoor rated Cat5e runs will be terminated from the Aruba 7010 Controller to both AP-275's. The AP-275's will be powered by the 7010 Controllers PoE+ Capabilities.
 - Rough Estimate from Controller to AP-01 is 160 ft
 - Rough Estimate from Controller to AP-02 is 180 ft

1201 North Avenue, Norwalk, IA Aruba Wireless POC Project

- o Piping access to roof



Main Server Room Hardware:

- Aruba 7010 Controller (Rack mount included) QTY: 1
- Power Cord for Controller QTY: 2
- Drops to outdoor AP's QTY: 2
- Drop to ICN Server Room (Feed Controller) QTY: 1

Note: Only need one cable run from Main Server Room to ICN Server Room to Feed Aruba Controller from ICN's hardware

1201 North Avenue, Norwalk, IA Aruba Wireless POC Project



ICN Server Room Hardware:

- Drop to Main Server Room QTY: 1

Note: Only need one cable run from Main Server Room to ICN Server Room to Feed Aruba Controller from ICN's hardware

1201 North Avenue, Norwalk, IA Aruba Wireless POC Project

AP-01 Information:

- ICN will be responsible for all cabling and mounting aspects
- DataVizion will be onsite to assist with any questions
- Mounting bracket and AP will be provided
 - All other hardware needed to mount/secure the AP will be ICN's responsibility

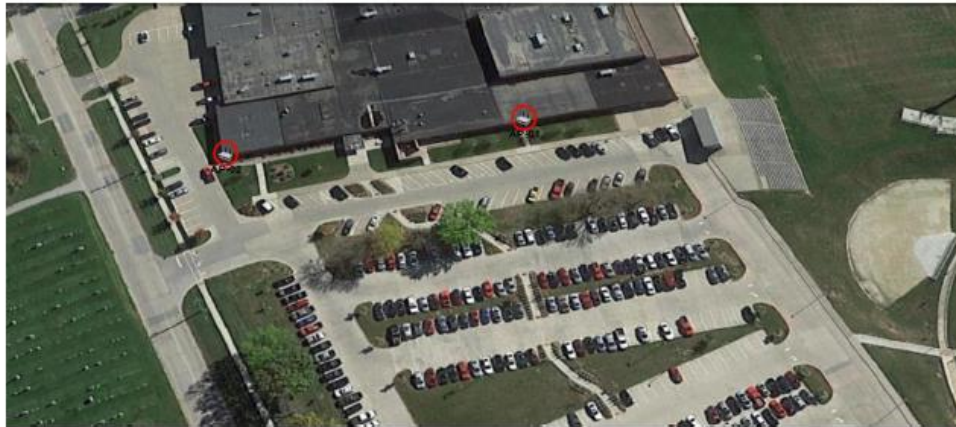
Refer to Overview of AP-275 below for mounting Ideas/Tips

AP-02 Information:

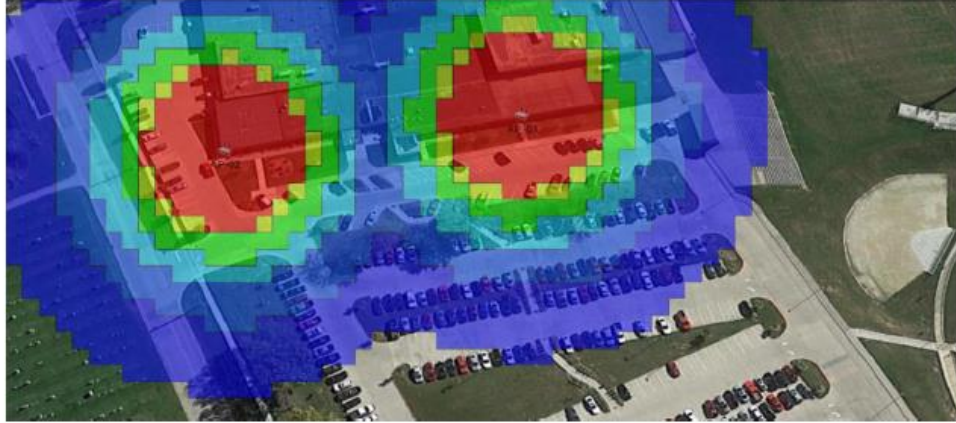
- ICN will be responsible for all cabling and mounting aspects
- DataVizion will be onsite to assist with any questions
- Mounting bracket and AP will be provided
 - All other hardware needed to mount/secure the AP will be ICN's responsibility

Refer to Overview of AP-275 below for mounting Ideas/Tips

AP-01 and AP-02 Wireless Data and Heat Map



1201 North Avenue, Norwalk, IA Aruba Wireless POC Project



RF Tool: Visual RF

Picture shows a heat map view from -45dBm(Red), -55dBm(Yellow), -65dBm(Green), -75dBm(Light Blue), -85dBm(Darker Blue), -95dBm(Darkest Blue)



RF Tool: Aruba Outdoor Planning Tool

Picture shows signal strength at -75 on the 5 GHz band

1201 North Avenue, Norwalk, IA Aruba Wireless POC Project
AP-275 Mounting Information:

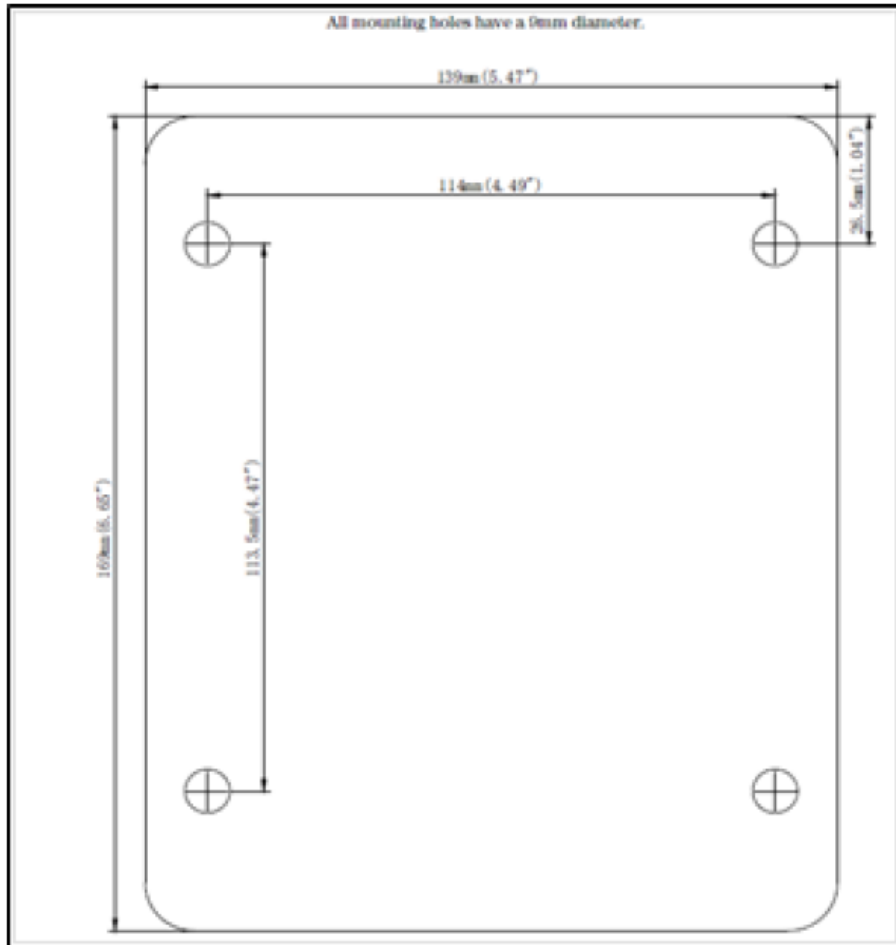
Overview of AP-275



Mounting Bracket:



1201 North Avenue, Norwalk, IA Aruba Wireless POC Project
Mounting Bracket Dimensions:



Width: 5.47"

Height: 6.65"

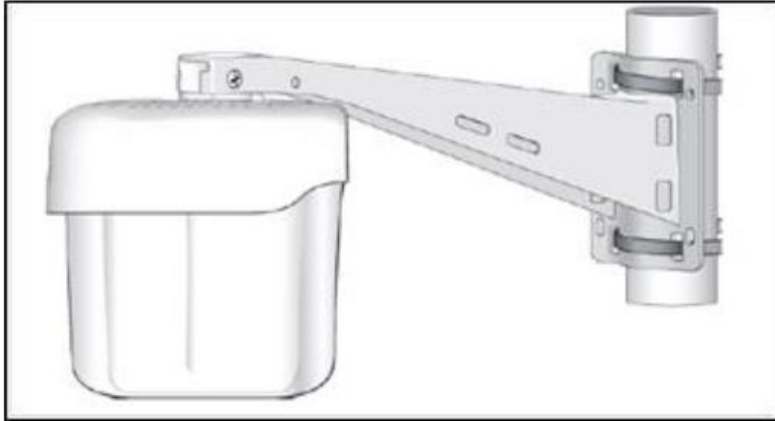
Distance Between Screw Holes:

Height between: 4.47"

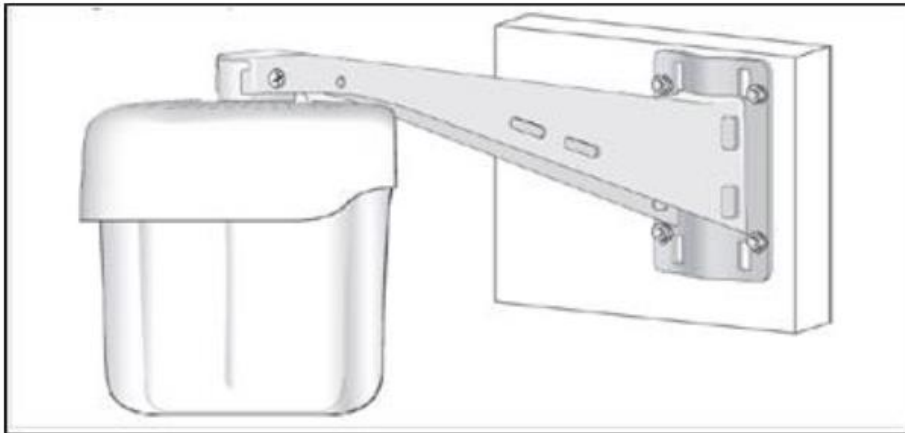
Width Between 4.49"

1201 North Avenue, Norwalk, IA Aruba Wireless POC Project

Pole Mount

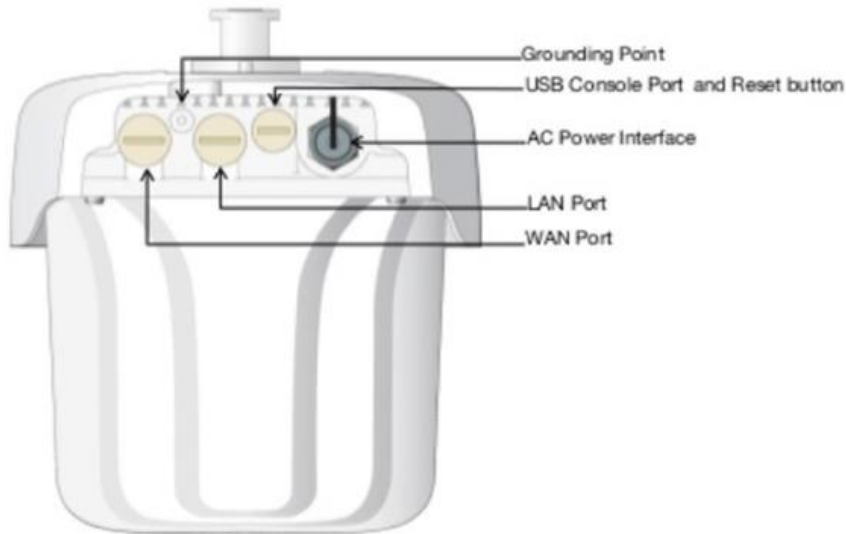


Wall Mount



1201 North Avenue, Norwalk, IA Aruba Wireless POC Project

Connections: Must Plug Ethernet into ENET0 (Wan Port)



Overview of all hardware requirements for project:

- Aruba 7010 Controller (Rack mount included) QTY: 1
- Power Cord for Controller QTY: 2
- Aruba AP-275 QTY: 2
- Aruba AP-275 Mounts QTY: 2
- Drops to outdoor AP's QTY: 2
- Drop to ICN Server Room (Feed Controller) QTY: 1
 - Roughly need:
 - 350 ft Outdoor Rated Cat5e Cable
 - 60 ft Cat5e cable
- AP-01 and AP-02 supplies to securely but temporary mount the (2) AP-275's.

Contact Information:

Mat Lehn
 DataVizion, LLC.
 Phone: 402-327-1880
 Email: mlehn@datavizion.com

Indoor/Outdoor Quotes

Price Estimate



Daniel Nielsen
 Cisco Systems, Inc.
 1089 Jordan Creek Parkway, Suite
 210
 WEST DES MOINES, IOWA-50266
 UNITED STATES
 Ph no: +1 408 894 8974

Cisco Systems, Inc.
 1089 Jordan Creek
 Parkway, Suite 210
 WEST DES MOINES, IOWA-
 UNITED STATES
 Ph no: +1 408 894 7867

Price Estimate for planning and information purposes only and is not a binding offer from Cisco.

Date : 25-Apr-2017

Estimate ID: QG71248654CG
 Deal ID: NA

All Prices Shown in USD

Part Number	Description	Service Duration (Months)	Lead Time	Unit List Price	Qty	Unit Net Price	Disc(%)	Extended Net Price
MR42-HW	Meraki MR42 Cloud Managed AP	---	3	1,099.00	65	1,099.00	0.00	71,435.00
	SubTotal							71,435.00
MR74-HW	Meraki MR74 Cloud Managed AP	---	7	1,399.00	8	1,399.00	0.00	11,192.00
	SubTotal							11,192.00
LIC-ENT-1YR	Meraki MR Enterprise License 1YR	---	3	150.00	73	150.00	0.00	10,950.00
	SubTotal							10,950.00
LIC-ENT-3YR	Meraki MR Enterprise License 3YR (First Year On Us)	---	3	300.00	73	300.00	0.00	21,900.00
	SubTotal							21,900.00
R-ISE-VM-K9=	Cisco Identity Services Engine VM (eDelivery)	---	2	5,990.00	1	5,990.00	0.00	5,990.00
CON-ECMU-ISEVM	SWSS UPGRADES Cisco Identity Services Engine VM (eDelivery)	12	N/A	1,198.00	1	1,198.00	0.00	1,198.00
L-ISE-BSE-1K=	Cisco Identity Services Engine 1000 EndPoint Base License	---	2	5,000.00	1	5,000.00	0.00	5,000.00
	SubTotal							12,188.00

Valid through		Product Total	126,467.00
FOB Point	None	Service Total :	1,198.00
Note:		Subscription Total	0.00
		Total Price:	127,665.00

Signed: _____
 Daniel Nielsen

This Price Estimate does not constitute an offer by Cisco to sell products, but is instead an invitation to issue a purchase order to Cisco until the valid date specified in this Price Estimate. Such a purchase order will be subject to Cisco standard procedures, terms and conditions for the acceptance of purchase orders. This order may be subject to sales tax, VAT, duty and freight charges even if not noted on this estimate.

The Fortinet logo is displayed in a bold, black, sans-serif font. The letter 'O' is replaced by a red square with a white grid pattern. A registered trademark symbol (®) is located to the right of the word.

FORTINET®

Fortinet WISE Proposal



Sam Belongia – Account Manager
Jeff Olson – Systems Engineer

Table of Contents

Fortinet Overview 2
Fortinet Secure Access Solution..... 2
Integrated Wireless..... 3
Cloud Wireless 4
FortiCloud with FortiDeploy..... 5
Pricing..... 7

Fortinet Overview

Fortinet’s mission is to deliver the most innovative, highest performing network security fabric to secure and simplify your IT infrastructure. We are a leading global provider of network security appliances for carriers, data centers, enterprises and distributed offices.

From the start, the Fortinet vision has been to deliver broad, truly integrated, high-performance security across the IT infrastructure.

We provide top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Our unique security fabric combines Security Processors, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control--while providing easier administration.

Our market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and media outlets worldwide. We are proud to count the majority of Fortune 500 companies among our satisfied customers.

Fortinet is headquartered in Sunnyvale, California, with offices around the globe. Founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen, Fortinet is led by a strong management team with deep experience in networking and security.

Fortinet Secure Access Solution

Securing business communications, personal information, financial Transactions, and mobile devices involves much more than network access control. It requires scanning for malware, preventing access to malicious websites, end-point integrity checking, controlling application usage, and much more.

But typical Wi-Fi solutions do not cater to these requirements. They only address connectivity and access security. Security above Layer 2 is typically provided as an overlay by a variety of security appliances, or as a cut-down security feature inside the product, which often conflicts with any existing UTM or firewall on-site. Fortinet’s network access solutions are different. They include comprehensive world-class network security at their core.

Fortinet’s Secure Access Solution ensures the same award-winning security that is validated by independent certification agencies (NSS Labs, etc.) is available to every type of Wi-Fi deployment, from a stand-alone AP in an isolated office, to a handful of APs in a retail store, to thousands of APs deployed across a large campus or even a distributed enterprise.

To meet the diverse requirements of different use cases from large to small, on-premise versus cloud-based management, and organizational differences, different WLAN solutions and topologies have emerged. While other WLAN vendors focus on a single architecture and present identical solutions as the answer for every problem, Fortinet enables enterprises of any size, in any industry, to choose the topology and network management that's best suited for their network, organizational structure, or management requirements without ever having to compromise on security protection.

Fortinet Secure Access Offerings

Only Fortinet delivers three offerings designed to address different WLAN requirements: An integrated solution in which switching, WLAN control, and security services are integrated in a single, high-performance appliance; a more traditional WLAN controller solution designed to support high-density and high-mobility environments with security services unmatched in the industry; and finally a cloud-managed wireless solution providing the simplest deployment option, yet still maintaining the highest level of security.

To provide the level of security equivalent to Fortinet, other vendors need a variety of different supplementary security products, which add to the operational complexity and TCO (Total Cost of Ownership) of their solutions. In contrast, Fortinet's secure access portfolio offers the same comprehensive security across all three access platforms, whether on-premise or cloud-managed. This enables businesses to mix and match deployment models for different use cases, without giving up critical security protection.

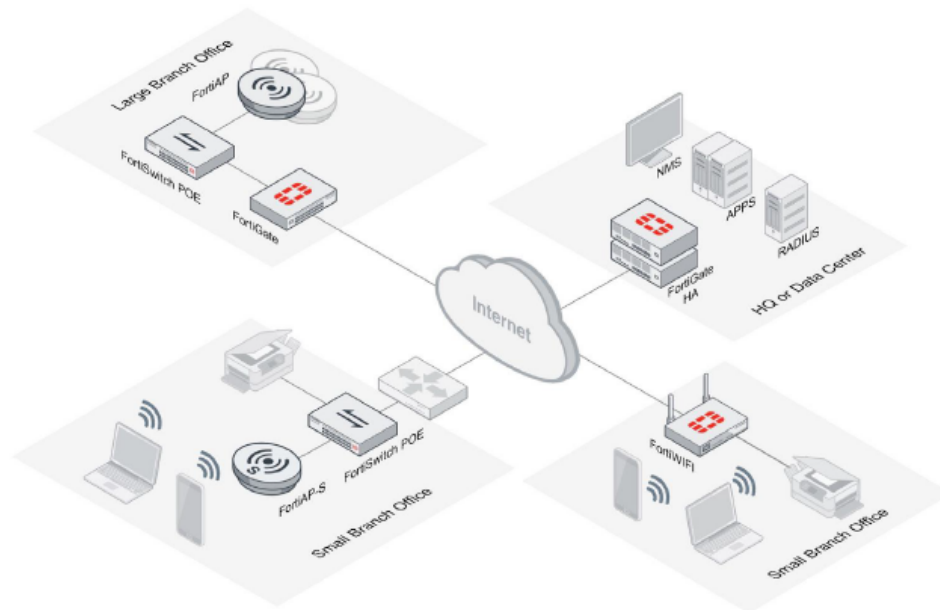
Integrated Wireless Offering – Unified Management, Superior Visibility, and Control

Fortinet's Integrated Secure Access offering is a family of access points and switches that are managed via an on-premise or remote FortiGate. Fortinet's integrated solution is built upon products recognized in Gartner Group's Magic Quadrants for Wired/Wireless LAN Access, Unified Threat Management, and Enterprise Firewalls. In this way, the FortiGate consolidates the functions of Network Firewall, IPS, Anti-malware, VPN, WAN Optimization, Web Filtering, and Application Control together with WLAN and switch control in a single platform. For branch office deployments, FortiGate is also available with an integrated AP known as FortiWiFi.

With security, connectivity, and access control, unified through a "single pane of glass," enterprises can centrally administer consistent user, device, and application policies across wired and wireless with ease. FortiGate provides unprecedented visibility and control of applications, and enables effortless BYOD onboarding.

Complete PCI-DSS and HIPAA compliance is assured, along with the industry's most comprehensive protection for all manner of wireless and Internet threats. And like other Fortinet security products, FortiGate is Secured by FortiGuard Labs, an internal security intelligence and research agency, which delivers regular signature updates, ensuring immediate protection from emerging cyber threats.

The combination of FortiGate security and FortiAPs gives enterprises of all sizes, in various industries, the scalability to deploy thousands of APs. It also enables secure access for tens of thousands of clients, without the complexity of additional point security products, in order to provide comprehensive, world-class threat protection.



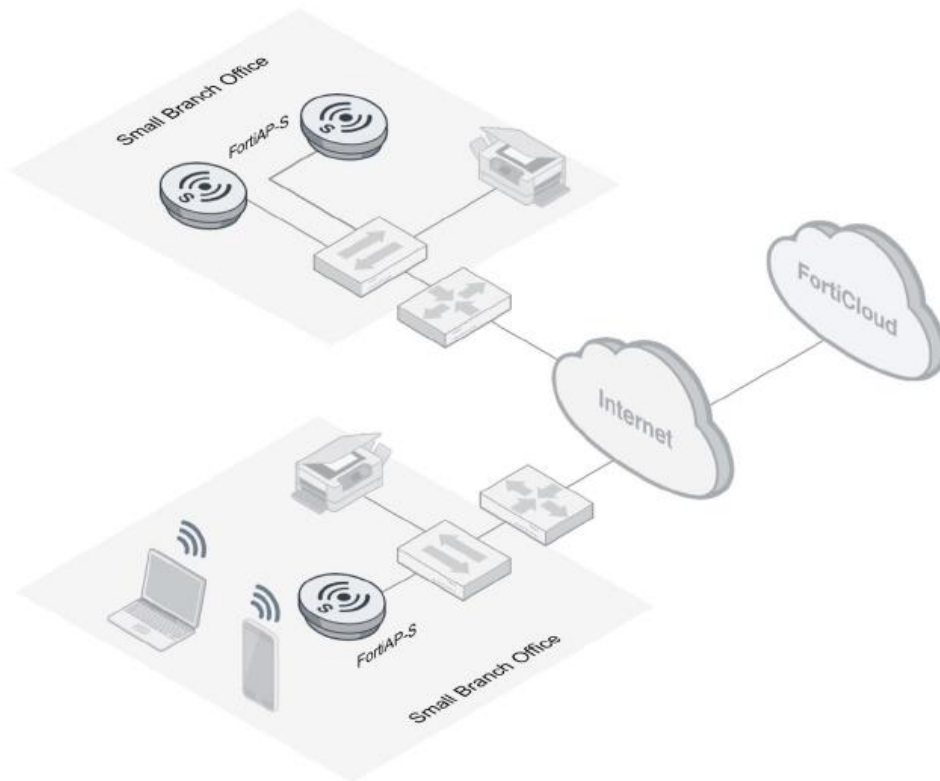
Cloud Wireless – Industry’s Most Secure, Cloud Managed Wi-Fi

Fortinet’s Cloud Wireless Solution is unlike any other cloud Wi-Fi offering. Based on the FortiCloud Provisioning and Management Service, and a new class of access points, the solution combines advanced security protection at the network access edge, with the simplicity and convenience of cloud management.

Equipped with extra memory and twice the processing power of typical access points, the FortiAP-S series performs real-time security processing on the access point itself, while configuration management and reporting via FortiCloud provides complete visibility of user, device, and application usage, comprehensive threat analysis, and all the identity management tools needed for BYOD onboarding and guest access through captive portals.

Combining Wi-Fi access and network security into the compact footprint of a single AP provides an exceptionally elegant and affordable WLAN solution for SMBs (Small Medium Businesses) and distributed enterprises. It lets users at small and remote sites connect to the Internet safely, without sacrificing security.

Corporate users can still be authenticated against RADIUS servers over the WAN, if desired, or via user accounts provisioned in FortiCloud, while all employee and guest traffic is subjected to enterprise-class cybersecurity protection locally at the network edge. Distributed enterprises can at last implement comprehensive security at remote sites, without needing to alter the security framework at corporate or backhaul all traffic through the corporate network.



How FortiCloud Addresses Key Enterprise Wireless and Security Challenges

Challenge	Solution
Facilitating turnkey provisioning of wireless and security devices at remote sites when on-site configuration expertise is unavailable	FortiAPs, FortiWiFis and FortiGates include FortiCloud registration functionality in their firmware that allow individual or multiple devices to provision themselves with minimal on-premise expertise.
Keeping initial investment costs down and preference for a consumption-based, OPEX model	FortiCloud uses a Software as a Service (SaaS) model that alleviates the need for upfront capital purchases.
Maintaining single pane of glass management for overseeing a wireless and security infrastructure	FortiCloud provides control over wireless and security devices while providing granular visibility and reporting at the same time.
Protecting the network from advanced threats and allowing granular access controls and application usage policies	Leveraging FortiCloud Sandbox technology from FortiGuard, FortiCloud is able to inspect potentially malicious payloads for zero-day threats.
Investing in a future-proof wireless and security solution that will scale with your business	As FortiCloud is cloud-based, it can grow as your business grows and accommodate additional event log storage as needed.

FortiCloud with FortiDeploy

Initial configuration of firewalls and access points can be a difficult proposition, often requiring expert staff on site to configure each device individually. FortiDeploy greatly simplifies initial configuration and onboarding by providing one-touch provisioning when devices are deployed, locally or remotely.

FortiDeploy provides deployment for FortiAPs into a Cloud AP Network, and automatic connection of FortiGates to be managed by FortiCloud. Hundreds of FortiGates or FortiAPs can be provisioned by using a bulk key in distributed environments, such as large retail or education networks. Once a communication tunnel is established, FortiCloud leverages provisioning profiles and setup wizards to quickly configure managed devices as required.

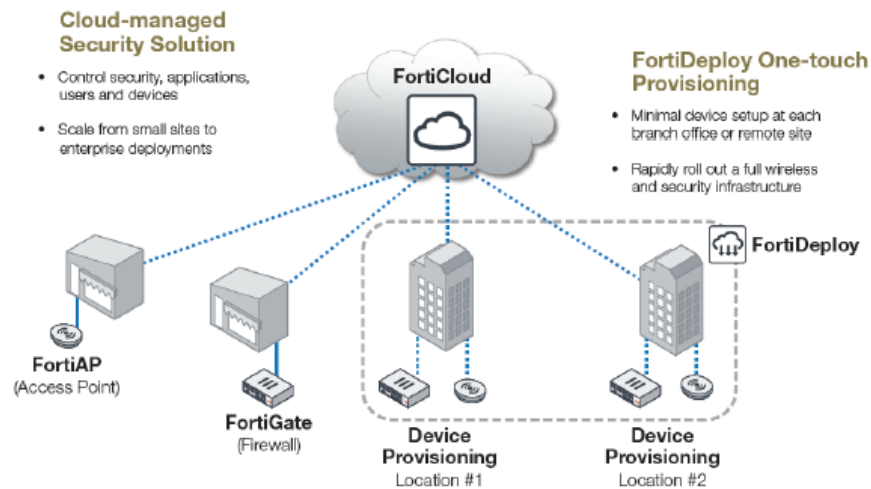
Configuration and device management from a single pane of glass

Consistent configuration of the devices within your network is essential to maintaining an optimal performance and security posture. FortiCloud provides a central web-based management console to control Fortinet devices. Device settings such as IP addresses or SSIDs can be centrally configured for individual devices or pushed to multiple devices. Configuration backups are kept in FortiCloud to assist with replacement or recovery efforts. Device firmware updates can also be centrally managed and controlled, thereby ensuring uniformed policy enforcement and allowing you to take advantage of the latest features.

Hosted log retention and cloud-based storage

Log retention is an integral part of any security and compliance best practice, but administering a separate storage system can be burdensome and costly. FortiCloud takes care of this automatically and stores your valuable log information securely in the cloud. Depending on your device, you can easily store and access different types of logs including traffic, system, web, applications and security events.

FortiCloud with FortiDeploy



FortiCloud is able to manage FortiAP wireless access points and FortiGate firewalls from a centralized, cloud-based management console.

Option 1 – Cloud Managed

- FortiAP – Outdoor and Indoor AP's
- FortiCloud – Cloud Management
- FortiDeploy – Zero Touch Provisioning
- FortiAuthenticator – Identity Management

Product	Description	Unit	Quantity	List
FortiAP 222C	Outdoor wireless AP - 1 x GE RJ45 port, dual radio (802.11 a/n/ac and 802.11 b/g/n, 2x2 MIMO), external antennas, Ceiling/wall mount kit included, Proprietary PoE injector with AC power adapter included.	\$1,295	6	\$7,770
FortiAP 223C	Indoor wireless AP - 1 x GE RJ45 port, dual radio (802.11 b/g/n and 802.11 a/n/ac, 2x2 MIMO), external antennas, Ceiling/wall mount kit included, Power adapter not included. For Gigabit PoE injector order: GPI-115. For AC power adapter order: SP-FG20C-PA.	\$495	65	\$32,175
FortiCloud Enterprise Management License - 1 Year	FortiCloud FAP (FAP/FAP-C/FAP-U) Enterprise Management License includes: Premium FAP Management Features, 1 Year Log Retention, 8x5 Forticare.	\$30	71	\$2,130
FortiCloud Enterprise Management License - 3 Years	FortiCloud FAP (FAP/FAP-C/FAP-U) Enterprise Management License includes: Premium FAP Management Features, 1 Year Log Retention, 8x5 Forticare.	\$79	71	\$5,609
FortiDeploy	Enables zero touch bulk provisioning for your FortiGate, FortiWifi, or FortiAP products.	\$100	1	\$100
FortiAuthenticator VM License	Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU. Designed for VMware and Microsoft Hyper-V platforms.	\$1,495	1	\$1,495
1 Year	1 Year 24x7 FortiCare Contract (1 - 500 USERS)	\$374	1	\$374
3 Years	3 Year 24x7 FortiCare Contract (1 - 500 USERS)	\$981	1	\$981

1 Year Total \$44,044
3 Year Total \$48,130

Option 2 – Virtual Controller

- FortiAP – Outdoor and Indoor AP's
- FortiGate – Wireless Controller
- FortiAnalyzer – Logging and Reporting
- FortiAuthenticator – Identity Management

Product	Description	Unit	Quantity	List
FortiAP 222C	Outdoor wireless AP - 1 x GE RJ45 port, dual radio (802.11 a/n/ac and 802.11 b/g/n, 2x2 MIMO), external antennas, Ceiling/wall mount kit included, Proprietary PoE injector with AC power adapter included.	\$1,295	6	\$7,770
FortiAP 223C	Indoor wireless AP - 1 x GE RJ45 port, dual radio (802.11 b/g/n and 802.11 a/n/ac, 2x2 MIMO), external antennas, Ceiling/wall mount kit included, Power adapter not included. For Gigabit PoE injector order: GPI-115. For AC power adapter order: SP-FG20C-PA.	\$495	65	\$32,175
FortiGate VM License	FortiGate-VM "virtual appliance" designed for VMware ESX and ESXi platforms. 1 x vCPU core and (up to) 2 GB RAM.	\$3,675	1	\$3,675
1 Year	24x7 FortiCare Contract	\$919	1	\$919
3 Years	24x7 FortiCare Contract	\$2,412	1	\$2,412
FortiAnalyzer VM License	Base license for stackable FortiAnalyzer-VM; 1 GB/Day of Logs and 500 GB storage capacity. Unlimited GB/Day when used in collector mode only. Designed for VMware vSphere, Xen, KVM and Hyper-V platforms.	\$1,800	1	\$1,800
1 Year	24x7 FortiCare Contract (for 1-6 GB/Day of Logs)	\$950	1	\$950
3 Years	24x7 FortiCare Contract (for 1-6 GB/Day of Logs)	\$2,494	1	\$2,494
FortiAuthenticator VM License	Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU. Designed for VMware and Microsoft Hyper-V platforms.	\$1,495	1	\$1,495
1 Year	1 Year 24x7 FortiCare Contract (1 - 500 USERS)	\$374	1	\$374
3 Years	3 Year 24x7 FortiCare Contract (1 - 500 USERS)	\$981	1	\$981


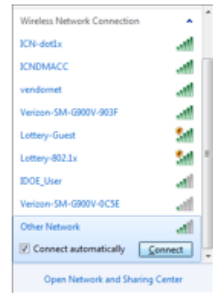

1 Year Total \$49,158

3 Year Total \$52,802

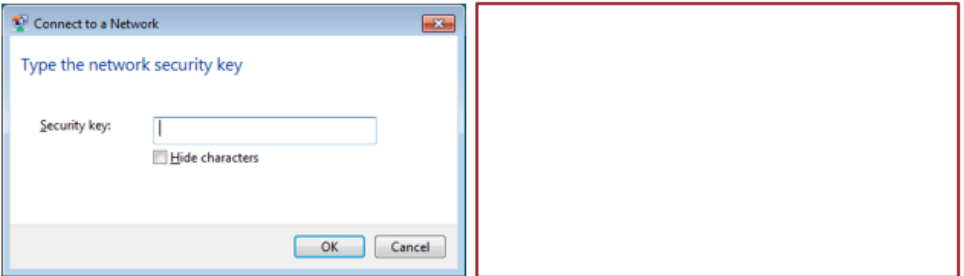
Appendix C: Instructions to join networks



WISE (Wi-Fi Internet for School Emergencies) Tech Setup Instructions

1.	<p>Select wireless radio by click on bottom right of pc by the time</p> 																								
2.	<p>Select OTHER Network and left click it an select connect</p> 																								
3.	<p>Enter WISE for the network select OK</p>  <table border="1" data-bbox="883 1201 1357 1524"> <thead> <tr> <th>Agency</th> <th>SSID</th> </tr> </thead> <tbody> <tr> <td>DPS State Patrol</td> <td>WISE</td> </tr> <tr> <td>Marshall County Sheriff</td> <td>WISE-MSD</td> </tr> <tr> <td>Warren County Sheriff</td> <td>WISE-WSD</td> </tr> <tr> <td>Marshalltown PD</td> <td>WISE-MPD</td> </tr> <tr> <td>Norwalk PD</td> <td>WISE-NPD</td> </tr> <tr> <td>Marshalltown HS EVENT</td> <td>WISE-MRTW</td> </tr> <tr> <td>Martensdale HS EVENT</td> <td>WISE-MRDL</td> </tr> <tr> <td>Norwalk HS EVENT</td> <td>WISE-NRWL</td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table> <p><i>Continued on back....</i></p>	Agency	SSID	DPS State Patrol	WISE	Marshall County Sheriff	WISE-MSD	Warren County Sheriff	WISE-WSD	Marshalltown PD	WISE-MPD	Norwalk PD	WISE-NPD	Marshalltown HS EVENT	WISE-MRTW	Martensdale HS EVENT	WISE-MRDL	Norwalk HS EVENT	WISE-NRWL						
Agency	SSID																								
DPS State Patrol	WISE																								
Marshall County Sheriff	WISE-MSD																								
Warren County Sheriff	WISE-WSD																								
Marshalltown PD	WISE-MPD																								
Norwalk PD	WISE-NPD																								
Marshalltown HS EVENT	WISE-MRTW																								
Martensdale HS EVENT	WISE-MRDL																								
Norwalk HS EVENT	WISE-NRWL																								

Questions? Contact ISICSB at iowanet@iowa.gov or 515-725-6113 / www.isicsb.iowa.gov
 Iowa Statewide Interoperable Communications System Board - www.isicsb.iowa.gov
 Oran Pape State Office Building | 215 East 7th Street | Des Moines, IA 50319

4.	<p>Enter the Network password _____ . And hit OK. You should connect.</p> 
5.	<p>You should be able to go back to the radio in step 1 and see both Verizon and WISE connected. You need to right click Verizon and select disconnect to use WISE for the upload. Do reverse to get back on Verizon right click WISE disconnect and right click Verizon connect.</p>

WISE Contacts:

ICN Technical Contact	Jeremy Howard	e: jeremy.howard@iowa.gov	o: 515-725-4081 c: 515-491-6013
Technical Contact	Helen Troyanovich	e: helen.troyanovich@iowa.gov	o: 515-725-4619
DPS Contact	Thomas Lampe	e: lampe@dps.state.ia.us	o: 515-725-6113
Outreach Contact	Shawn Wagner	e: swagner@dps.state.ia.us	c: 515-419-3688

Questions? Contact ISICSB at iowanet@iowa.gov or 515-725-6113 / www.isicsb.iowa.gov
Iowa Statewide Interoperable Communications System Board - www.isicsb.iowa.gov
Oran Pape State Office Building | 215 East 7th Street | Des Moines, IA 50319