



Michigan's Public Safety Communications Interoperability Board

Agenda

March 10, 2020, 1:00 PM – 4:00 PM
MSP HQ - 1917 Room
7150 Harris Drive, Dimondale, MI 48821

	Notes
I. Call to Order	
II. Roll Call	
III. Welcome	
IV. Approval of Meeting Minutes	December 2019 and February 2020
V. Approval of Meeting Agenda	
VI. Communications	<p>Outgoing: FCC letter on interoperability Encryption Moratorium Building and fire codes recommendations</p> <p>Incoming: Keith Bradshaw – Oakland County Bryce Alford – Ingham County Chris Petres – Northville Fire – Device management policy Chris Petres – Waterford Regional Fire - Encryption Matt Groesser – Kent County South East Michigan Urban Area Security Initiative (SEMI UASI) Lisa Hall – Midland Al Young – Taylor Fire Jim Jarvis – Cyber Security and Infrastructure Security Agency (CISA)</p>
VII. Public Comment	
VIII. Workgroup Reports <ul style="list-style-type: none"> A. Communications Unit Workgroup Co-chairs: Bryce Tracy and Ray Hasil <ul style="list-style-type: none"> 1. Workgroup Update B. Public Safety Broadband Workgroup Co-chairs: Pam Matelski and Brad Stoddard <ul style="list-style-type: none"> 1. Workgroup Update 2. Regional/National Activities/News C. Auxcomm Workgroup 	

<p>Co-chairs: Jaclyn Barcroft and John McDonough</p> <p>1. Workgroup Update</p> <p>D. Public Alerting Workgroup</p> <p>Co-chairs: Jaclyn Barcroft and Ron Bush</p> <p>1. Workgroup Update</p> <p>E. Fire Paging Workgroup</p> <p>Co-chairs: Al Mellon and Greg Janik</p> <p>1. Workgroup Update</p>	
<p>IX. Old Business</p> <p>A. MPSCS State Performance Audit</p>	
<p>X. New Business</p> <p>A. ECD – State Markers Presentation and Interaction – Joe Galvin DHS Emergency Communications Division</p>	
<p>XI. Federal Update –</p> <p>A. CISA – Jim Jarvis</p> <p>B. FEMA RECCWG – Jaclyn Barcroft and Brad Stoddard</p>	
<p>XII. Technology Update – Brad Stoddard</p> <p>A. MPSCS System</p> <p>1. MCM – radio programming and tracking package</p> <p>2. NICE Recording Solution</p> <p>3. County discussions: Map handout</p> <p>4. Agencies – 1,995; Radios – 106,399; Dispatch Centers – 88; Dispatch Consoles – 456; Computer Aided Dispatch (CAD) consoles – 59; Fire Pagers – 5,894</p> <p>5. FY 20 Budget</p> <p>6. FY 21 Budget</p> <p>7. MPSCIB Guidance</p> <p>a) Draft Device Management Policy</p> <p>b) Draft Encryption Policy</p> <p>B. Statewide Interoperability Coordinator (SWIC)</p>	
<p>XIII. Good of the Order</p> <p>A. Comments by Board Members</p>	
<p>XIV. Adjournment</p>	

2020 Meeting Dates

- March 10th – MSP HQ
- June 9th – MSP HQ
- September 15th – MSP HQ
- December 8th – MSP HQ



Michigan's Public Safety Communications Interoperability Board

MINUTES

December 10, 2019, 2:00 PM – 4:00 PM

MSP HQ, Centennial Room, 7150 Harris Drive, Dimondale, MI 48821

Dial In # 888-278-0296

Access Code: 8855666#

	Notes
I. Call to Order	Chair Lieutenant Colonel Sands called the meeting to order at 2:01 p.m.
II. Roll Call	<p>The following Board Members were present: Lt. Col. Tom Sands, Brad Stoddard, Assistant Chief Edwin Miller, Chief John Allen, Col. Lawrence Schloegl, Bryce Tracy, Jon Unruh, Lt. Jen Wolf for Chief Gary Hagler, State Fire Marshal Kevin Sehlmeier, Eileen Phifer, Jerry Ellsworth, Chief Bradley Kersten, Inspector James Grady for Captain Emmitt McGowan, Matthew Sahr and Ken Morris</p> <p>Absent: Chief Troy Stern</p> <p>Also Present: Cindy Homant, Al Mellon, Chief Greg Janik, Jim Jarvis, Jaclyn Barcroft, John McDonough (phone), Kate Jannereth, Inspector James Wolf Pam Matelski, John Hunt, Sgt. Ron Bush (phone), Allison Pemberton, Dominic DeMark, Chuck Cribley, F/Lt. Steve Temelko, Monica Jenkins, Tim Crane, Craig Swenson, Shelly Forbes, Matt Nixon, Col. Ken Morckel and Steve Miller</p>
III. Welcome New Members	Lt. Col. Tom Sands welcomed Matt Sahr to the board.
IV. Approval of Meeting Minutes	Motion to approve September 10, 2019 minutes by Bryce Tracy. Seconded by Chief Edwin Miller. Motion carried.
V. Approval of Meeting Agenda	Motion to approve by Chief Edwin Miller. Seconded by Matt Sahr. Motion carried.
VI. Public Comment	None.
VII. Communications	<p>Fire Paging Work Group Building and Fire Codes Recommendations</p> <p>Motion to recommended for public posting and distribution by Bryce Tracy. Seconded by Matt Sahr. Motion Carried.</p>

<p>VIII. Workgroup Reports</p> <ul style="list-style-type: none"> A. Communications Unit Workgroup Co-chairs: Bryce Tracy and Ray Hasil <ul style="list-style-type: none"> 1. Workgroup Update B. Public Safety Broadband Workgroup Co-chairs: Pam Matelski and Brad Stoddard <ul style="list-style-type: none"> 1. Workgroup Update 2. Regional/National Activities/News C. Auxcomm Workgroup Co-chairs: Jaclyn Barcroft and John McDonough <ul style="list-style-type: none"> 1. Workgroup Update D. Public Alerting Workgroup Co-chairs: Jaclyn Barcroft and Ron Bush <ul style="list-style-type: none"> 1. Workgroup Update E. Fire Paging Workgroup Co-chairs: Al Mellon and Greg Janik <ul style="list-style-type: none"> 1. Workgroup Update 2. Building Codes Communication 	<p>See attached handouts. In addition:</p> <p>A. Bryce Tracy presented Jeffry Bauer for COML recognition.</p> <p>Motion to approve by Eileen Phifer.</p> <p>Seconded by Matt Sahr.</p> <p>Discussion: Col. Schloegl asked if there are restrictions for non-governmental entities being on the system. Bryce described the role of a COML. Brad Stoddard mentioned utilities use it for back up today and the MCLs don't restrict it. Motion carried.</p> <p>B. Pam Matelski: Working with Allegan county on network coverage grid testing. Requested to present a FirstNet demo in the March 10, 2020 meeting. Bryce mentioned forms to request deployables are being shared without a process in place. Pam said they are working on a State policy to request deployables from FirstNet. Cautious on first come first serve strategy. Need to consider planned events vs. emergencies.</p> <p>D. Sgt. Bush: iPAWS is trying to improve proficiency. Several Emergency Managers were concerned what they would have to do to maintain proficiencies. They have to include their permissions in the proficiency messages and ensure results came through in the message viewer. iPAWS is not checking content, just ensuring message has correct formula, right priority, etc.</p> <p>E. Chief Janik thanked the Board for approving building code communications.</p>
<p>IX. Old Business</p> <ul style="list-style-type: none"> A. MPSCS State Performance Audit B. Statewide Communications Interoperability Plan (SCIP) – Posted online C. Encryption Task Force Update – Posted online D. MPSCIB Brochure – Posted online 	<p>A. MPSCS is currently in a 30 day response period to provide plan. Will move this to the MPSCS section for the March 10, 2020 meeting.</p> <p>B. Annual review of SCIP will be an item for the board moving forward.</p> <p>C. Passed guidelines which put pressure back onto MPSCS and the MPSCIB since interoperability has been impacted.</p> <p>Draft policy on encryption discussion:</p> <p>Bryce: The draft policy on encryption works well with the guidelines for future integration, but will this address current transitional issues?</p> <p>Brad Stoddard: Transitional would be those who currently do not use encryption. The goal is that now before a community is purchasing encryption, they have to provide a plan for the MPSCS to sign-off on before moving forward. Need to include adjacent partners and mutual aid. Large education that comes with encryption. Avoid them using encryptions that</p>

	<p>not all radios can use. Some are not capable of multiple keys and all types of encryption. Currently by the time encryption makes it to the MPSCS, decisions have been made and encryption has been purchased. It would be MPSCS asking what are you planning for? Lt. Col. Sands suspended discussion until item XII. A. 9. b.</p>
<p>X. New Business</p> <p>A. Next Generation Public Safety Interoperability – The Digital Decision (30 minutes)</p>	<p>Allison Pemberton – Verizon Col. Ken Morckel Digital Decision Steve Miller – Digital Decision FCC requested comment on requiring private carriers to be interoperable for public safety. Priority and preemption is not currently interoperable. Verizon believes it is possible. If FCC doesn't force it, three States have ensured interoperability by making it a contractual obligation as part of the procurement process.</p> <p>Brad Stoddard: Agreed the 30 day timeline the FCC set to provide comment was a tight constraint on State's ability to respond.</p> <p>TDD: Asked the Board if they considered a support letter to the FCC open comments, ensuring interoperability (priority and preemption) across all public safety carriers.</p> <p>Brad Stoddard: Verizon brought in a deployable patch and phones to test at the MPSCS. Locals have wanted to do a patch back into the MPSCS. Brad tested technology in Michigan and from two states away. It is imbedded in Verizon's core, as a push-to-talk. The MPSCS monitored traffic on the system, nothing concerning. Quality was great. Tested both radio and phone. Did not test on encrypted talkgroup. MPSCS will not let an unapproved console on the network (Verizon is awaiting MPSCS approval to use with the MPSCS before they offer the solution to Michigan as a Verizon offering). We also have Wave through Motorola. AT&T looking at a solution early 2020.</p> <p>Lt. Col. Sands: In car video – MSP looking at dual modems for video traffic. Video to cloud, data through private network.</p> <p>Lt. Col. Sands: We lucked out (GETS card/WPS) during the summer 2019 brown out where cell phones were not operating. He tested WPS and got right through. It's an app that we need to spread the word on. Suggested issuing board communications to recommend interoperability between carriers.</p> <p>Lt. Jen Wolf: We would like to see the recommendation and they have dual carriers.</p>

	<p>Matt Sahr: We (the Board) shouldn't be making stance and mentioning Verizon.</p> <p>Lt. Col. Sands: Agreed. Letter would just be to ensure all carriers be able to be interoperable.</p> <p>Motion to approve the Board issuing communications to the FCC in support of interoperability between carriers for public safety communications by Col. Larry Schloegl.</p> <p>Seconded by Chief Edwin Miller.</p> <p>Motion Carried.</p>
<p>XI. Federal Update –</p> <ul style="list-style-type: none"> A. CISA – Jim Jarvis B. National Emergency Communications Plan – Jim Jarvis C. FEMA RECCWG – Jaclyn Barcroft 	<p>A. Working on ICS – Information Technology and Communications Branch under logistics.</p> <p>B. Released September 2019. 6 goals. 19 objectives with success indicators. Printed versions available if needed.</p> <p>C. End of September meeting in Chicago with MN, WI, IL, MI, Civil Air Patrol and Verizon. Statewide exercise coordination, MN shared several iPAWS planning documents. Democratic National Convention coordination. Lisa Dixon FirstNet presentation.</p> <p>Jarvis: Region 7 partnering with region 4,5,6 and 7 for an exercise.</p>
<p>XII. Technology Update – Brad Stoddard</p> <ul style="list-style-type: none"> A. MPSCS <ul style="list-style-type: none"> 1. MPSCS Lifecycle Remediation Project Status 2. MCM – radio programming and tracking package 3. NICE Recording Solution – Local call logging issues 4. County discussions: Clinton and Branch – Map handout 5. Mini Site – Michigan Tech 6. Agencies – 1,954; Radios – 105,978; Dispatch Centers – 88; Dispatch Consoles – 455; Computer Aided Dispatch (CAD) consoles – 59; Fire Pagers – 5,050 7. FY 20 Budget 8. FY 21 Budget 9. MPSCIB Guidance <ul style="list-style-type: none"> a) Draft Device Management Policy b) Draft Encryption Policy 	<p>A1. Completed except for software upgrade, January will kick off major planning of that upgrade.</p> <p>A2. Tool to give MPSCS members more access to work orders on radios. Potential inventory tool for users.</p> <p>A3. This will drop after next board meeting. A few issues with local dispatch centers. MPSCS and Motorola worked with NICE to troubleshoot. No final resolution to report.</p> <p>A4. Clinton working on quote. Looking at a millage to pay for it. Branch was not on our radar but we were notified they are considering migrating. Sanilac interested in next steps and quotes.</p> <p>We have had 2 meeting so far with Indiana on cross border communications with a third meeting Friday. Chief Larry Lamb reached out to MI Senator LaSata about a device that allows greater roaming between networks. Critical Connect is a cloud based ISSI solution to connect IN and MI networks. Still some patches and talkgroups issues that need to be worked out. MOUs needed county to county and state to state. Some fire service radios are incapable having a second system installed in their radios.</p> <p>Sgt. Ron Bush: Experienced issues with law enforcement chasing across borders and there have</p>

B. Statewide Interoperability Coordinator (SWIC)
1. SWIC/SAFECOM meeting update

been fatalities because of the inability for the law enforcement agencies to communicate.

Lt. Col. Sands: Encouraged cross border communications.

A5. This will be removed off the February 11, 2020 agenda. Mini site is active end of October. CMU and U of M Dearborn have requested quotes on the technology.

A7/A8. Staffing is greatest level of frustration. We have grown over 1000% with same staff levels 24 years ago. Second goal is infrastructure replacements that were not part of remediation.

A9a. Brad Stoddard: We see a lot of radios come in from different departments who are showing ownership different than the one requesting the programming. Our goal is be notified on both sides of transactions to ensure talkgroups are removed from the radios before transferred. Help the MPSCS track radio IDs as well. More than 60% of radios are over 10 years old.

A9b. Jim Jarvis – Agree that an encryption policy is needed. DHS's position is that AES 256 is the P25 standard. DHS S&T and P25 Compliance Acceptance Program agreed to a referendum that if a vendor is identifying its equipment as P25 it must have no encryption, AES256 or AES 256 and a proprietary voice privacy protocol. ADP alone is NOT P25 and does NOT qualify for grant funding. Strongly encourage we change the encryption type in the draft policy to AES 256 or eliminate that language all together.

Bryce Tracy: If we force the issue would the feds provide funding?

Jim Jarvis: DHS working with vendors to use AES 256.

Bryce: Require vendors to be multikey?

Jim: Long term goal is to get to P25 standard – how does MI get there? That should be SCIP strategy on use of funding.

Lt.Col Sands: The solution must be interoperable. Reference federal standard. Remove type of encryption? Approved guidelines recommend primary 9-1-1 channels be not encrypted. Main concern is public safety can talk vs. public safety is safe to encrypt. Primary dispatch channels cannot be encrypted. It's an option. It is on this board to ensure interoperability is maintained.

Lt. Jen Wolf: It is time for something like this document to move forward.

Brad Stoddard: What is the timetable for fraternal organizations to weigh in? Timetable for existing people to migrate to the standard, not guideline. Forces them to look at this and not just what a vendor is selling. Cost is a concern.

Bryce Tracy: If the policy points to the federal standard, it could hold people back from encryption.

Lt.Col. Sands: Maybe just target primary 911 dispatch talkgroups as non-encrypted.

Bryce: The standard should not touch proprietary or tactical talkgroups. Guidelines are posted and the recommendation is to not encrypt the primary talkgroups. The question is, if those particular talkgroups are going to be encrypted, it should be "this" type of encryption and "this" encryption key.

Lt. Col: We should not encrypt primary 9-1-1 channels.

Bryce: If an agency wants a parallel channel that is encrypted can they create one?

Brad Stoddard: Patched talkgroups are an issue

Bryce: It must be understood that patching cannot occur. What comms need to be secured and what don't. Even EMS is requesting to encrypt.

Al Mellon: We need to address the agencies not deployed. RPU needs formal process where all agencies are notified of this moratorium.

Bryce Tracy: Motion to share the 2 draft policies with fraternal organizations for feedback by February 19, 2020. Review responses in March board meeting.

Lt. Col. Sands: Add to recommendation to not approve any ongoing moves to encryption. Temporary hold.

Bryce: Agrees to add to motion.

Col. Larry Schloegl: Add in message that the primary responsibility of system and board is to maintain interoperability.

Bryce: Correct define why, the moratorium and that we will be discussing in March. We can discuss at the interop conference. Could also call a special meeting. Moratorium until formal policy is in place. Both policies tabled.

Final Motion by Bryce Tracy as edited by Board: Table both draft policies and share them with members of the MPSCS and Fraternal Organizations. Ensure to include mission of the MPSCS and MPSCIB is interoperability and request feedback by February 19th to be discussed at March 10, 2020 Interoperability Board Meeting or a special meeting of the MPSCIB. Effective immediately, a moratorium on any further encryption programming by the

	<p>MPSCS- Radio Programming Unit. Chief Edwin miller seconded. Motion carried.</p> <p>B1: DHS-ECD annual interoperability self-evaluation markers moved to March 10, 2020 meeting.</p>
<p>XIII. Good of the Order</p> <p>A. Comments by Board Members</p>	<p>2020 Meetings moved to 1917 room at MSP HQ. September meeting is the 15th NOT 8th. Board members cost covered at Interop Conference.</p>
<p>XIV. Adjournment</p>	<p>Motion to adjourn by Bryce Tracy.</p> <p>Seconded by Kevin Sehlmeier.</p> <p>Motion carried.</p>
<p>2020 Meeting Dates</p>	<ul style="list-style-type: none"> • Special Meeting February 11, 2020 Great Wolf Lodge, Traverse City • March 10th – MSP HQ • June 9th – MSP HQ • September 15th – MSP HQ • December 8th – MSP HQ



Michigan's Public Safety Communications Interoperability Board

Minutes

February 11, 2020, 10:00 AM – 12:00 PM
Great Wolf Lodge, Traverse City

	Notes
I. Call to Order	Chair Lieutenant Colonel Sands called the meeting to order at 10:00 a.m.
II. Roll Call	<p>The following Board Members were present: Lt. Col. Tom Sands, Brad Stoddard, Bryce Tracy, Jon Unruh, Lt. Jen Wolf for Chief Gary Hagler, Jerry Ellsworth, Inspector James Grady for Captain Emmitt McGowan, and Ken Morris</p> <p>Absent: Matthew Sahr, Chief Bradley Kersten, State Fire Marshal Kevin Sehlmeier, Eileen Phifer, Assistant Chief Edwin Miller, Chief John Allen, Gen. Lawrence Schloegl, Chief Troy Stern</p> <p>Also Present: Cindy Homant, Chief Greg Janik, Jim Jarvis, Kate Jannereth, Pam Matelski, Sgt. Ron Bush, Allison Pemberton, F/Lt. Steve Temelko, Michelle Kuzera, Monica Jenkins, Tim Jones, Craig Swenson, Matt Groesser, Eric Hutchinson, Dominique Clemente, Ray Hasil, Rhonda Grant, Kurt Fechter, Jerry Becker, Randy Williams, Jerry Nummer, Inspector James Wolf, Tina Bricker, Chris VanArsdale, Todd Fox, Chuck Cribble, Tom Duram, Dick Mirgon, Al Gillespie</p>
III. Welcome	
IV. Approval of Meeting Agenda	Motion to approve by Bryce Tracy. Seconded by Jen Wolf. Motion carried.
V. Public Comment	<p>Matt Groesser – Kent Co.</p> <p>Volunteered to help on encryption committee. Kent's templates are due to the MPSCS RPU with ADP encryption selected because it was free. Kent county is willing to work with the Board. Stated the Board needs to ensure locals have voice.</p>
VI. Communications	None.

<p>VII. Workgroup Reports</p> <ul style="list-style-type: none"> A. Communications Unit Workgroup Co-chairs: Bryce Tracy and Ray Hasil <ul style="list-style-type: none"> 1. Workgroup Update B. Public Safety Broadband Workgroup Co-chairs: Pam Matelski and Brad Stoddard <ul style="list-style-type: none"> 1. Workgroup Update 2. Regional/National Activities/News C. Auxcomm Workgroup Co-chairs: Jaclyn Barcroft and John McDonough <ul style="list-style-type: none"> 1. Workgroup Update D. Public Alerting Workgroup Co-chairs: Jaclyn Barcroft and Ron Bush <ul style="list-style-type: none"> 1. Workgroup Update E. Fire Paging Workgroup Co-chairs: Al Mellon and Greg Janik <ul style="list-style-type: none"> 1. Workgroup Update 2. Building Codes Communication 	<p>Public Alert and Warning, Sgt. Bush – Couple of month process to award RFP for statewide alerting system.</p> <p>Fire Paging – Chief Janik conveyed his appreciation to the Board for encouraging adherence and compliance with building code. They have educated 450 fire inspectors. Clearly realizing people do not understand in building coverage.</p>
<p>VIII. Old Business</p> <ul style="list-style-type: none"> A. MPSCS State Performance Audit B. Encryption Comments 	<p>A. MPSCS State Performance Audit Internal DTMB review of response to the audit. MPSCS is requesting copies of existing MOUs for talkgroups. Felony charge in MI for having TGs you aren't allowed to have. Board needs to look at control of TGs. MCM may help.</p> <p>B. Encryption Comments Recommendation document suggested not encrypting Primary TGs because of concerns to preserve interoperability. Ron Bush: Region V had a whole county came on and encrypted everything. They're re-looking at it after Board communications. Unencrypt Comms and P911. Eric Hutchinson: Local media and other citizens beat them to the scene. Example of media blocking K-9 scents. They have met with surrounding counties and are using State MPSCS key. Lt. Col. Sands: Statewide resources and mutual aid use clear talkgroups. Matt Groesser: Kent County does not plan to patch. Can strap radios to ensure safety. Patch key itself is an interesting issue. Board needs to work with the vendor to come up with a better solution. When radios have a different key the system can't force it to use the right one.</p>

Bryce Tracy: Biggest problem is education and outreach. It is a feature, not a flip of a switch. Moratorium was to stop it from getting worse. Need a hard stance to prevent officer safety issues. Need a process everyone can follow. The hard stop got everyone engaged. Vendors didn't realize the issues either. Not just encryption but comms plans and channel naming as well. We are doing the best we can to not have an unfunded mandate.

Matt Groesser: Kent County templates need to be done by end of February. Concerns about extending life of old system and training becoming obsolete if project is delayed. Costs need to be considered that are delaying projects.

Jim Jarvis: The P25 compliance assessment program is working with all P25 vendors and what is considered allowable and impacts to grant money. Also through the federal partnership for interoperable communications, they have a series of documents on encryption and planning. They have a new one for review and comment that he will distribute.

Brad Stoddard: Local control is important. It is our system collectively. Task force can develop a decision matrix to make it easy for communities, the MPSCS and vendors to make easy decisions. Once we put the moratorium out in December, people outside of Michigan became engaged. Wisconsin wants to comment. It has been in Mission Critical magazine and online. Creating dialogue around the country. Other states have same challenges. Mission Critical would like to do a follow-up article.

Lt. Col. Sands: Thank you for bringing up the grant information. Greater part of radios on MPSCS are over 10 years old.

Eric Hutchinson: Every manufacturer but one provides AES to be SafeComm compliant. Motorola does not provide AES for free. Multi-million dollars to do AES through Motorola for Kent County.

F/Lt. Temelko: Training Sergeants were educating the locals and realized they were unaware of impact of encryption. MSP training Sgts are being contacted about encryption non-stop now. They are grateful for the Board's action.

Tim Jones: 2,000 radios with full encryption and the patches created issues with MSP cars. \$7M and 2 years. We all missed the patch issue. We put a temporary fix in place and the challenge is to find a statewide solution. Concerns need to be

	<p>communicated to the local officials. Their boards need to understand it too. The communications have to go to the right people.</p> <p>Brad Stoddard: This has been ongoing from September 2018. The people encrypting the talkgroups are not always the ones understanding the capabilities of the radios. Motorola contract re-write helps with costs of the encryption options. To get to the next phase we cannot stress enough that we need the requirements and use cases from all the different communities. Opportunity to get all the right people at the table to address 98% of issues statewide. Bryce will continue as the task force chair. Larger group in round 2 to make processes and standards. Look at fed partners and their guidance. Comments due by February 19th. March 10th might be tough to have a solution.</p> <p>Green lighted MSP in Genesee County and team of 10 in City of Detroit and Oakland County auto theft task force to go forward that were not on consoles.</p>
<p>IX. New Business</p> <p>A. Vince DeLaurentis – guest speaker</p>	<p>CISA – (formerly OEC)</p> <p>Driving National Emergency Communications Plan implementation. First time endorsed by SafeComm</p> <p>With the move to CISA they now have a direct relationship with the Cyber Security Division.</p> <p>Comms Section Task Force – idea of elevating Comms in ICS structure.</p>
<p>X. Federal Update –</p> <p>A. CISA – Jim Jarvis</p> <p>B. FEMA RECCWG – Jaclyn Barcroft</p>	<p>A. CISA</p> <p>Technical Assistance Program: Ready to rollout TA's. Encryption TA is available. SEMI UASI is interested in it. Comms section task force working on incident comms activity report, a lot like interop markers. The ICAR is specific to incident comms. Form fillable. How can we collect info and is it valuable? It might fit in the COMU recognition process. Could be a way to develop AAR.</p> <p>Bryce Tracy: Ron Bush working on the state-to-state aspect.</p> <p>B. FEMA RECCWG</p> <p>Joint plenary session in Tennessee in April. Central US Earthquake Consortium.</p>

<p>XI. Technology Update – Brad Stoddard</p> <p>A. MPSCS System</p> <ol style="list-style-type: none"> 1. MCM – radio programming and tracking package 2. NICE Recording Solution – Local call logging issues 3. County discussions - Map handout 4. Mini Site – Michigan Tech 5. Agencies – 1,986; Radios – 106,593; Dispatch Centers – 88; Dispatch Consoles – 455; Computer Aided Dispatch (CAD) consoles – 59; Fire Pagers – 5,135 <p>B. Statewide Interoperability Coordinator (SWIC)</p>	<ol style="list-style-type: none"> 1. Testing now. Pause in RPU/TDU as this rolls out. Should streamline information coming into the RPU/TDU. We will make sure we provide a much greater detail of what this tool looks like at future meeting. We solicit feedback on draft salvage process notifying the MPSCS of radios that are no longer on the system. 2. Call logging would drop when patching? 7500 with Nice IP logger there are occurrences when it says it is logging but its not logging. Not 100% repaired. 3. Map handout. Clinton County on March 10th ballot. Most counties are facing funding issues for radios and or/towers. There has been a lot of effort the last couple of years for a grant program. Lt. Col. Sands and Rhonda Grant have met with Vince DeLaurentis to gain support of the concept of the grant. Congressman Moolenaar conversations. In parallel Sands and Grant have been meeting with Senator Wayne Schmidt who has been very supportive. <p>Lt. Col. Sands: Talk to your local reps. Reach out to them and educate them. Grant is eligible for infrastructure. State not eligible – just locals.</p> <p>Rhonda Grant – The proposal establishes a single dedicated grant prog. \$50k a piece but can apply for more than one. Looking for a state companion bill. Senator Barret and Schmidt have been key.</p> <p>4. Minisite –Chris VanArsdale Houghton County and Todd Fox works for Michigan Tech but volunteers for Houghton Co. Site is on taller building, 60% of population now has in-building coverage. Fire response now has communications on campus. Approximate cost of the site was \$500k. Full tower site is about \$1.5M.</p> <p>Brad Stoddard: Preventative maintenance on radios can help with coverage as well.</p> <p>5. Agencies = north of 2,000 agencies. Radio count is closer to 107K.</p> <p>L3Harris is vetting Symphony console. As well as Z-tron. Taking on some effort in our lab we hope to share in June. MPSCS is looking to move the needle forward in multiple areas.</p> <p>B. SWIC UPDATE: Brad is the co-chair of NCSWIC. John Miller in NJ is the Chair. NCSWIC academy trains all new SWICs that come in. November of 2019 ad 40 people in attendance. Lori Flaherty wants to do that for State 911 Directors. Harriet Miller-Brown (former Michigan 911 Director) wants more combined efforts</p>
---	--

	<p>with State 911 committee and the MPSCIB and touch points together.</p> <p>Also, how to continue engagement of SWICs that move on. Vince's offices may need to address participation and legal efforts. As people move on a lot of institutional knowledge is lost.</p> <p>The NCSWIC has materials they have developed across the country and are looking at creating a video to educate policy leaders as well as for new SWICs. Tying the video to the mentoring program.</p>
<p>XII. Good of the Order</p> <p>A. Comments by Board Members</p>	<p>Inspector Grady:</p> <p>Corona Virus – none in Michigan even with DTW as a funneling point. Keep an eye open for activities like emptying stores. Be prepared. Have resources at home.</p> <p>Thanks to Lt. Col. Sands and the MPSCIB for their efforts. Great progress in Michigan. Stressed importance of communications and encryption.</p> <p>Brad Stoddard: Closing comments: Years ago setup the special meeting for conference attendees to see the Board activities. Used to be not a lot of people at these but appreciate the attendance and welcome it regularly. Bring in the local voice. The board does not know all of the details of local day-to-day operations. September is the MPSCS 25th anniversary. This year is 10th conference anniversary at GWL. Appreciate the Board and support of the MPSCS.</p> <p>Lt. Col. Sands: As a private citizen thanked the Board for their knowledge and passion.</p>
XIII. Adjournment	<p>Motion to adjourn by Brad Stoddard. Seconded by Ken Morris. Motion Carried.</p>
2020 Meeting Dates	<ul style="list-style-type: none"> • Special Meeting February 11, 2020 Great Wolf Lodge, Traverse City • March 10th – MSP HQ • June 9th – MSP HQ • September 8th – MSP HQ • December 8th – MSP HQ



STATE OF MICHIGAN

MICHIGAN PUBLIC SAFETY COMMUNICATIONS INTEROPERABILITY BOARD

LANSING

STATUS OF CURRENT ACTIONS REPORT TO THE MPSCIB – MARCH 2020 – COMU WG

Interop Board Action Items

None at this time...

Current Tacks & Projects

AUXCOMM Recognition – Draft versions being reviewed at this time. Final draft to be approved by the COMU WG in May, then brought to the MPSCIB for final approval for inclusion within the Communications Unit Position Guidelines at the June 2020 meeting.

NEW Communications Unit Positions - Incident Tactical Dispatcher (INTD), Information & Technology Service Unit Leader (ITSL), Radio Operator (RADO) – These positions will be considered for future inclusion to the existing Michigan Communications Unit Position Guidelines

E-MIFOG (Electronic version of the Michigan Communications Field Operations Guide) Technical Assistance from OEC & DTMB = development an electronic application version of the MIFOG.

COML/COMT Renewal Process – Database Audit

Beta Testing of ICAR (Incident Communications Activity Report) with CISA-EC. COMU WG is going to use the ICAR form to track communications after action reporting after events. The ICAR could also be used to help document communications activity for COML's/COMT's to help log their activities for the renewal process. This is a collaboration testing project with CISA EC.

Ongoing – Credentialing & MICIMS Data = Collaboration with AUXCOMM and MSP-EMHSD and DTMB regarding credentialing and resource/asset typing practices.

Ongoing - AUXCOMM Database = Collaborate with AUXCOMM WG regarding tracking of verified personnel, similar to the existing COML/COMT database in CASM.

What's on the Horizon?

Collaboration with MSP/EMHSD, AUXCOMM WG, Public Safety Broadband WG, Public Alerting WG, State NG911 on transitions to Emergency Management – Emergency Support Functions Format for SEOC and Local EOC Operations (ESF #2 – Communications)

Training and Exercises

Completed:

Nothing to report...

Future:

COML Class – October 6-9 (Lansing Area)

AUXCOMM Classes in consideration (Pending)

Basic Incident Information and Scope

Event Date:	Event Duration in Days:	Type of Event:	Situation	Explosion	Marathon/Race	Location:
		Incident	Collapse	Natural Disaster	Concert	Local/Jurisdiction
		Planned	Haz Mat	Search & Rescue	Festival	State/Tribal/Territory
		Exercise	Transportation Accident	Barricade	Other	
IAP Developed	Yes <input type="checkbox"/> No <input type="checkbox"/>		Active Assailant	Fire		
			Manhunt			
# of Disciplines Involved	# of Jurisdictions Involved	Types of Jurisdictions Involved	Local	Tribal		
		State / Territorial	Federal	NGO's		
ICS Positions Staffed	IC/UC	Plans Section	Finance Section	Logistics Section	Operations Section	# of Ops Branches

What ICS Position did the Communications/Information Technology Functions Report to?

Communications Functional Positions Utilized

Branch	Utilized	Completed Training	Completed PTB	If applicable, response time objective met	Not met
COML	Utilized	Completed Training	Completed PTB	If applicable, response time objective met	Not met
If COML function was NOT conducted on-site, then where?					
				Dispatch Center	Emergency Operations Center
Incident communications requirements did not overwhelm the scope of current SOPs and pre-planned resource utilization.					
ITSL	Utilized	Completed Training	Completed PTB	If applicable, response time objective met	Not met
If ITSL function was NOT conducted on-site, then where?					
				Jurisdiction IT Back-office	Emergency Operations Center
Incident IT requirements did not overwhelm the scope of current SOPs and pre-planned resource utilization.					
COMT	Utilized	Completed Training	Completed PTB	If applicable, response time objective met	Not met
INCM	Utilized	Completed Training	Completed PTB	If applicable, response time objective met	Not met
INTD/RADO	Utilized	Completed Training	Completed PTB	If applicable, response time objective met	Not met
AuxCom	Utilized	Completed Training	Completed PTB	If applicable, response time objective met	Not met
Provided communications support for Government Organization(s)				Provided communications support for non-Government Organization(s)	
Provided technical expertise to supplement Public Safety communications				Other:	

Communications Plan

Plans/SOPs referenced during Comms Plan development.	TICP	NIFOG	Region IFOG	Other:
Were back-up communications (voice and data) methods planned?				
PACE (Primary, Alternate, Contingent, Emergency)	Alternate	Contingent	Emergency	
Did a primary mode fail during the event at any time? Yes	What level of PACE did system regain operation?			
	Alternate	Contingent	Emergency	

Were any **VOICE** communications problems reported or encountered during the event, that were **RESOLVED** by Communications Unit Personnel? *If yes, categorize the problem below.*

Equipment Configuration/Performance	Equipment Familiarity	Governance/SOPs	Malicious Activity
Deficiency in the Communications Plan	Deviation from the Communications Plan	Other:	

Were any **DATA** communications problems reported or encountered during the event, that were **RESOLVED** by Communications Unit Personnel? *If yes, categorize the problem below.*

Equipment Configuration/Performance	Equipment Familiarity	Governance/SOPs	Malicious Activity
Deficiency in the Communications Plan	Deviation from the Communications Plan	Other:	

Were any **VOICE** communications problems reported or encountered during the event, that were **NOT RESOLVED** by Communications Unit Personnel? *If yes, categorize the problem below.*

Equipment Configuration/Performance	Equipment Familiarity	Governance/SOPs	Malicious Activity
Deficiency in the Communications Plan	Deviation from the Communications Plan	Other:	

Were any **DATA** communications problems reported or encountered during the event, that were **NOT RESOLVED** by Communications Unit Personnel? *If yes, categorize the problem below.*

Equipment Configuration/Performance	Equipment Familiarity	Governance/SOPs	Malicious Activity
Deficiency in the Communications Plan	Deviation from the Communications Plan	Other:	

Incident Communications Activity Report

DRAFT

Tactical Equipment/Systems Deployed

Cache Radio Cache Radio TSP	Mobile/tactical Repeaters Mobile/tactical Repeaters TSP	Data/IT/LTE/Broadband Data/IT/LTE/Broadband TSP	Gateway Gateway TSP
Geographic Information Systems (GIS) Geographic Information Systems (GIS) TSP	Mobile Comms Unit/Vehicle Mobile Comms Unit/Vehicle TSP	Satellite Comms (SatCom) Voice & Data Satellite Comms (SatCom) Voice & Data TSP	Video Systems Video Systems TSP
Teleco/Telephone Systems Teleco/Telephone Systems TSP	Site on Wheels (SOW) Site on Wheels (SOW) TSP	LMR/Radio Technician LMR/Radio Technician TSP	Other: Other TSP:

Incident Scene Voice Usage

Shared Channels	Yes	Radios Pre-Programmed	Common Naming
Regional/National Interop Channels	Yes	Radios Pre-Programmed	Common Naming
Federal Interop Channels	Yes	Radios Pre-Programmed	Common Naming
LMR Digital Voice Modes	Yes	Project 25 (P25) Standard	Vendor Proprietary:
LMR Encryption Used	Yes	Advanced Encryption Standard (AES)	Vendor Proprietary or Other:
Access to WPS?	Yes	Used	Access to GETS? Yes Used

Incident Scene Data Usage

List network methods by which data was accessed in the field:			
FirstNet	Other Commercial Data / Long Term Evolution (LTE) Network	Private/Closed Data Network	Satellite Network
Wired Network	WiFi	Other networks/other access configurations	

Choose the functions performed which required access to data.

Records Management System (RMS)	Calls for service through Computer Aided Dispatch (CAD)		
Situational Awareness Tools/Common Operating Picture (COP)	Did the incident leverage CAD to CAD connectivity		
Collaboration tools such as WebEOC	Bi-directional interface with another agency's CAD system		
National Crime Information Center (NCIC) / wants and warrants/criminal databases	Uni-directional interface with another agency's CAD system		
Tactical Information Exchange within Operations' Branches	Other		
Responder Level Tracking (Blue-Force Tracking)	Software applications for field reporting		
Automatic Vehicle Location (AVL)	Remote Sensor Monitoring		
Internet	GIS maps	Corrections systems	Traffic/transport systems
	Video surveillance	Patient Tracking	Reunification (Missing Persons)
			Other:

List the device(s) used to access data.

SmartPhone	Tablet	Tactical Wearable Device
Laptop / Mobile Data Computer (MDC)	Cellular Phone (not SmartPhone)	Other Devices:

Alerts and Warnings

Did agencies have access to or the capability to generate emergency notifications, alerts, or warnings to the community?

Integrated Public Alert and Warning System (IPAWS)	Local independent notification system	Traffic/transportation alerting system
Used	Used	Used
Weather alert system	Visual message board	Other:
Used	Used	Used

Social Media

Was social media used by public safety for any purpose while managing the event?

Facebook	Twitter	Other:
----------	---------	--------

Who managed the analysis and collection of social media inputs from the public? (In-bound use)

Fusion Center	PIO	Multiple PIO's	JIC Personnel	Command Personnel	Investigative/Intelligence
EOC Personnel	PSCC/PSAP	Other:			

Who managed dissemination and messaging via social media? (Out-bound use)

PIO	Multiple Public Information Officer (PIOs)	Joint Information Center (JIC) Personnel	Command Personnel
Field Personnel	Emergency Operations Center (EOC) Personnel	Public Safety Communications Center/PSAP	Other:



STATE OF MICHIGAN

MICHIGAN PUBLIC SAFETY COMMUNICATIONS INTEROPERABILITY BOARD

LANSING

STATUS OF CURRENT ACTIONS REPORT TO THE MPSCIB MARCH 10, 2020 – AUXCOMM WORK GROUP

Interop Board Action Items

New Items

Continued work on Auxcomm position implementation which includes a team completing the following:

1. Completing the Auxcomm Recognition Guidance which details the process from completion of the Auxcomm class to state recognition – expected completion date is March 2020.
2. Position Task Book (PTB) Training – developing an additional class to cover the technical aspects of page 13 of the PTB which are not covered in the Auxcomm class.
3. Task Book Completion – incorporating Auxcomm tasks into an exercise (either the COMMEX or an additional exercise) to allow for the opportunity of participants working on their PTB.
4. Emergency Manager Presentation – A detailed presentation explaining what the AUXCOMM position is, what it isn't, and how it can benefit Emergency Management needs to be developed and delivered at the state and regional (and possibly local) levels.

The Auxcomm WG sent in a comment to the FCC regarding WT Docket No. 19-348: In the Matter of Facilitating Shared Use in the 3.1-3.55 GHz Band. The Auxcomm WG urged the commission to maintain the 3GHz band for the amateur radio community.

What's on the Horizon

Continue to work with other communications/ESF2 stakeholders to update the Michigan Emergency Management Plan (MEMP) and State Emergency Operations Center (SEOC) communications operational procedures.

Training and Exercises

Continue planning for the 2020 Statewide Exercise to be held April 14-16, 2020 to make sure Auxcomm participation is incorporated into the scenario.

Region 8 Auxcomm continues to participate in the planning efforts for an Isle Royale exercise in June 2021 with the US Coast Guard and other partners. They are coordinating with Auxcomm groups in WI and MN.



Michigan Auxcomm Workgroup
7150 Harris Drive
Dimondale, MI 48821

February 21, 2020

Chairman Pai, Commissioners O'Rielly, Carr, Rosenworcel and Starks
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

RE: WT Docket No. 19-348: In the Matter of Facilitating Shared Use in the 3.1-3.55 GHz Band

Dear Chairman Pai and Commissioners O'Rielly, Carr, Rosenworcel and Starks

The amateur radio community in Michigan utilized the 3GHz band to develop a microwave data network used for auxiliary communications (Auxcomm) to support emergency management across the state. The band was chosen as part of the network design because of the inherent protection of the band, as compared to Part 15 consumer-oriented bands. The inherent protection of the 3GHz band allocated by the Federal Communications Commission (FCC) helps to ensure reliability of the network in times of emergency by minimizing risk of interference from nearby users. Construction of the Michigan microwave network began in 2010. To date over 42 sites have been installed across the state at a cost of \$105,000 plus 11,453 hours of volunteer effort. Growth of the network is ongoing, at a rate of 2-4 new sites per year.

If the FCC removes the amateur radio allocation as part of the removal of the non-federal allocation, the Michigan Auxcomm community will be forced to replace the equipment to support moving the network to a new frequency. Given the significant volunteer effort and equipment cost involved, it will likely lead to problems being able to convert all the equipment in a timely manner. This could cause the network to become unavailable to support emergency management functions. Further, if the new band is not allocated strictly for amateur radio use, the network's reliability may be compromised due to interference from nearby users.

We are opposed to the approval of this docket and strongly urge the commission to allow the amateur community to continue to support Auxcomm for emergency management on the 3GHz band.

Respectfully,

Michigan Auxcomm Workgroup

John McDonough, WB8RCR - Co-Chair, ARRL Section Emergency Coordinator
Jaclyn Barcroft, Co-Chair - Michigan State Police Emergency Management Homeland Security Division
Tim Crane, WM8A - ARRL District Emergency Coordinator, District 1
Mark Breckenridge, WD8MWD - ARRL District Emergency Coordinator, District 2
Max Schneider, KE8DON - ARRL District Emergency Coordinator, District 3
Carl Flickinger, KB8FQJ - ARRL District Emergency Coordinator, District 5
Dave Robertson, N8UKH - ARRL District Emergency Coordinator, District 6
Charles Brew, N8NXP - ARRL District Emergency Coordinator, District 7
Peter Costa, K8PDC - ARRL District Emergency Coordinator, District 8
Jim Richardson, AB8JR - ARRL Emergency Coordinator, Oakland County
Kevin Scheid, KD8ZVO - St. Clair County Emergency Management, Auxcomm Trainer
Bob Dennis, WX8BOB - Salvation Army SATERN
Geoff Richardson, N8CE/NCS187 - Michigan SHARES

LT Col Shawn Wyant, K8SAW – Michigan Wing, Civil Air Patrol
John Imeson, N8JI – Eaton County Radio Systems Manager, Auxcomm Trainer
Jay Nugent, WB8TKL, ARRL Michigan Section Assistant Section Manager
Randy Love, WF5X, ARRL District Emergency Coordinator, NWS-Detroit
Randy Williams, KD8MOK, Michigan Public Safety Communication System
Fred Moses, W8FSM, Central Michigan Emergency Network



STATE OF MICHIGAN

MICHIGAN PUBLIC SAFETY COMMUNICATIONS INTEROPERABILITY BOARD

LANSING

STATUS/UPDTAE OF CURRENT ACTIONS REPORT TO THE MPSCIB – MARCH 2020 PUBLIC ALERTING WORKGROUP

Interop Board Action Items

Identify actions or decisions the workgroup is requiring of the board

New Items

List items for update and awareness for the boards knowledge since the last quarterly report

Statewide Emergency Alert and Mass Notification System Request for Proposal (RFP). Several vendors provided proposals which have been reviewed. Vendor demonstrations were then conducted on February 25, 2020. A final decision/award in early March 2020.

The release of the IPAWS 3.0 and Wireless Emergency Alerts (WEA) 2.0 implementation was completed by FEMA. FEMA IPAWS PMO wanted to ensure the legacy WEA 1.0 connections to the wireless provider systems will continue to be supported during the transition to the IPAWS 3.0 and WEA 2.0 enhancements. FEMA Testing Lab migrated to the new cloud-based system to be more robust for supporting 1400+ alerting authorities. The old lab was decommissioned October 1. Due to system problems, the required Proficiency Demonstrations began on November 1 instead of October 1. The month of October was used as a test for Alerting Authorities. All Alerting Authorities are required to send an alert message that corresponds to their alerting privileges to the FEMA Lab.

Ingham Co worked with the FEMA IPAWS PMO to complete the first LIVE test of WEA in the United States to after the IPAWS 3.0 and WEA 2.0 updates. They had several people in the area turn on the WEA test feature on their cell phones and sent out a couple of WEA messages. Feedback was provided to FEMA so that they can continue to refine their system.

The review process is continuing to finalize the updated IS-247.a and IS-251 IPAWS Independent Study Courses. The IS-247.b and IS-251.a courses are currently in Beta testing.

Sgt. Bush participated in a conference call with the DHS Science and Technology Directorate to assist in the development of alert, warning, and notification program planning guidance materials to assist alerting authorities on the use of IPAWS.

IPAWS MOU Status Report – As of February 5, 2020, there are 56 Michigan agencies (increase of 2 from November 2019) with completed MOUs and 16 agencies with MOUs in progress with FEMA.

What's on the Horizon

Identify any work efforts, meetings, or information for upcoming activities the board should be aware of

The meeting occurs on the 3rd Tuesday of February, May, August and November. The next scheduled meeting is May 19, 2020 at 10:00.

Waiting for the release of the Federal Communications Commission (FCC) National EAS Plan Template so updates can begin to the State and Regional EAS Plans in 2020.



STATE OF MICHIGAN

MICHIGAN PUBLIC SAFETY COMMUNICATIONS INTEROPERABILITY BOARD

LANSING

The Michigan Association of Broadcasters sent out the 2020 Required Monthly Test schedule for all EAS broadcast areas. Looking to get more local involvement in the issuance of these live tests.

Training and Exercises

Identify any training or exercises the workgroup has or will be participating in

Local EM programs continue to train on the use of IPAWS and originate test messages and live Required Weekly Test (RWT) alerts.

There will be opportunity for several counties throughout the state to practice sending EAS and WEA messages to the IPAWS Lab during the 2020 statewide exercise Rising Waters (April 14-16, 2020).



STATE OF MICHIGAN
MICHIGAN PUBLIC SAFETY COMMUNICATIONS INTEROPERABILITY BOARD
LANSING

STATUS OF CURRENT ACTIONS REPORT TO THE MPSCIB
March 2020 – FIRE PAGING

Interop Board Action Items

Building Code Communications from the Board

- None

Fire Paging Work Group Website Approval

- None

New Items

Micro Site Technology Update – In MPSCS lab testing 3 channel system 130 Watt capability per channel

- Requested features verified in lab testing
- Moving to Phase II (field testing Grand Travers, St Clair, Allegan) – Equipment still at MPSCS

New counties testing

- Alcona - Testing
- Iosco - Testing
- Calhoun - Testing
- Antrim - Declined (Testing Did Not Pass)

New counties implementing

- Lenawee - Go Live March to May 1st, 2020 (Digi-Com 487)
- Roscommon Misc. Agencies - Training Oct 2019
- Charlevoix / Cheboygan / Emmet - Pagers ETA Shipping Spring 2020 (731)
- Kent 2020
- Alpena ETA 9/1/2020 Already purchased pagers 60k
- Berrien Majority ETA 12/31/2020
- The MPSCIB Conference generated a great deal of interest in Emergency Responder Radio Coverage
- Numerous counties have reached out for more information on the Michigan Building Code 916 and International Fire Code 510
- YouTube – interest was expressed to create 90 second informational communication on Emergency Responder Radio Coverage Power Point
- Several invitations were extended to present the Emergency Responder Radio Coverage Power Point
- On February 21st, Greg met with Bureau of Construction Codes Keith Lambert and Bureau of Fire Services Director/State Fire Marshal Kevin Sehlmeier to discuss educational outreach and the MBC 916 applications. Both Directors offered very solid and useful guidance on educating and informing various stakeholders and engaging law various enforcement agencies
- Educational Outreach Plan – additional contacts
 - Michigan Association of Chiefs of Police – Educational and Training Committee
 - Saugatuck Public Schools – Dr. Tim Travis
 - National Fire Protection Association (NFPA) – Clarification submittal for NFPA 101 Technical Committee
 - On March 13th Greg will meet Sheriff Frank Baker and Michigan Sheriffs Director Blaine Koops to discuss

What's on the Horizon

Micro-Site Beta Test in field locations

Unication new portable radio – On Hold RPU workload

Unication CAD text paging – On hold RPU workload

Training and Exercises

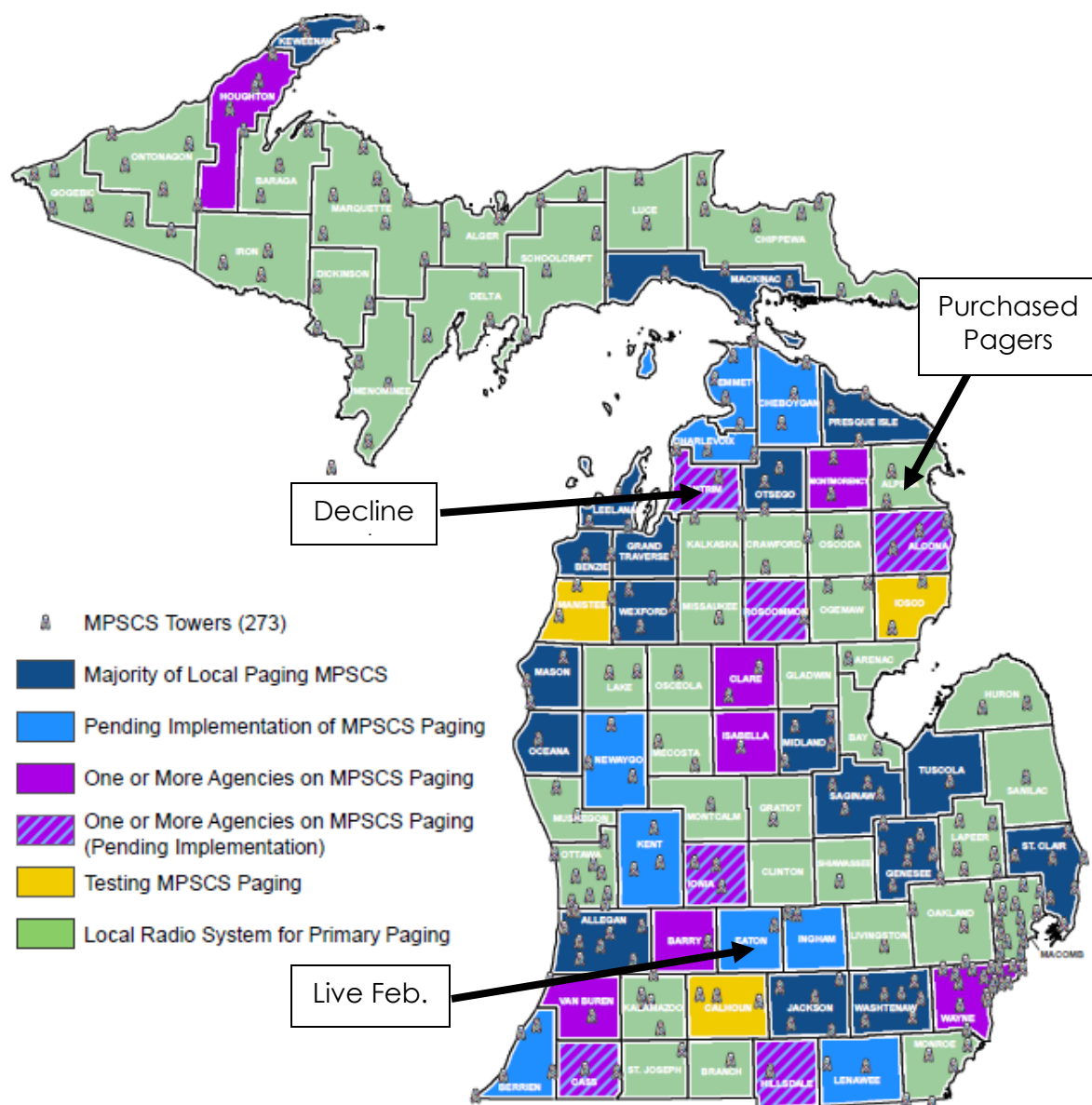
Discussing a brief test for firefighters to pass before getting a pager

Dealers should be required to provide the training



Michigan's Public Safety Communications System

Public Safety Paging



*State, federal, tribal, and private first responders utilize MPSCS communication in all 83 counties.

1/31/2020



Encryption – Current state of encryption on the MPSCS:

- Three Encryption Algorithms in use.
Ninety Seven unique encryption keys
- Almost 2000 agencies on MPSCS with different levels of encryption needs
- Network Connected Dispatch Consoles can patch encrypted talkgroups together and invoke “Patch Key”
- Radio software allows for only one patch key per radio



Encryption on the MPSCS

1996-2012 14 Keys added

2013-2020 83 Keys added

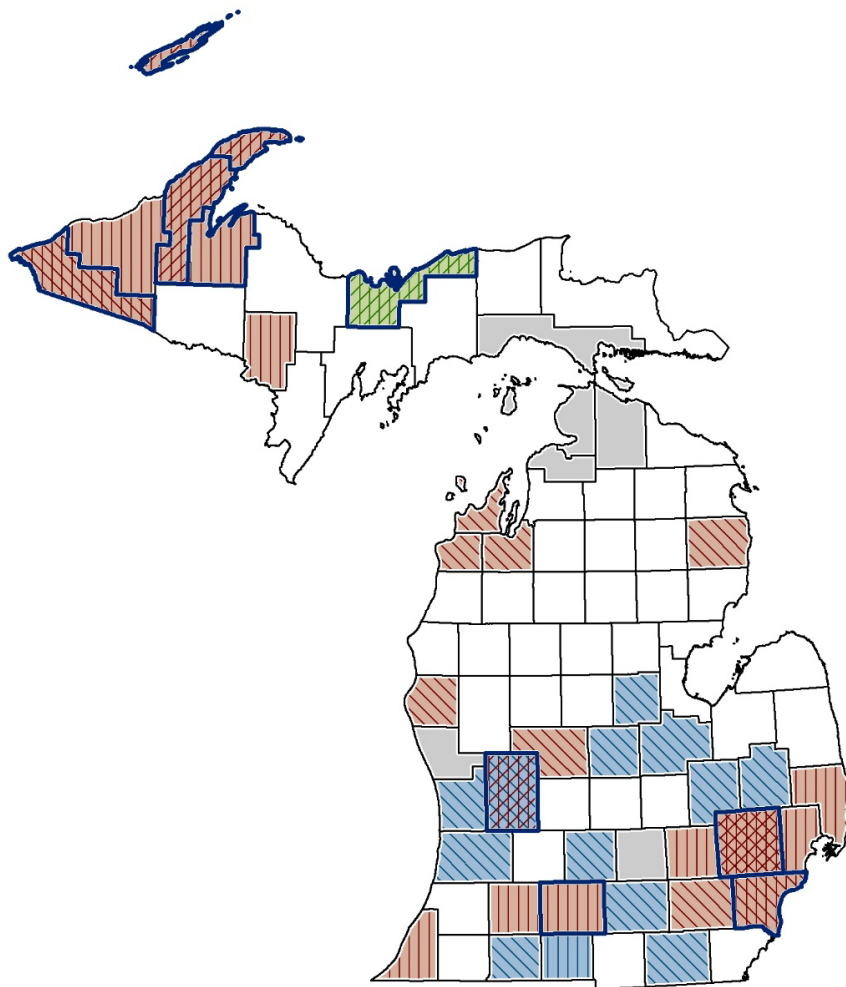
ADP/ARC4 – 28 Keys

DES-OFB – 47 Keys

AES – 20 Keys

UKEK – 2 Keys

Total Keys – 97





Encryption - What goes wrong?

- Patch Key
- One patch key per MPSCS radio
 - MSP Patch = MSP Key
 - Kalamazoo Patch = Kalamazoo Key
 - Genesee Patch = MPSCS ADP Key
 - Washtenaw Patch = Washtenaw Key
 - Livonia Patch = Lavonia Key
 - And so on all encrypted radios.



Patch/Failsoft/Private Call Keys

- This setting in the radio programming file determines key to use during certain events. Only one key can be selected for each event and is applied on a radio wide basis.
- If you have the wrong key for the conversation, then you will not be heard on the other end.
- If you have the wrong key for the conversation, you may not hear the other users.
- There is no notification that you are using the wrong key.

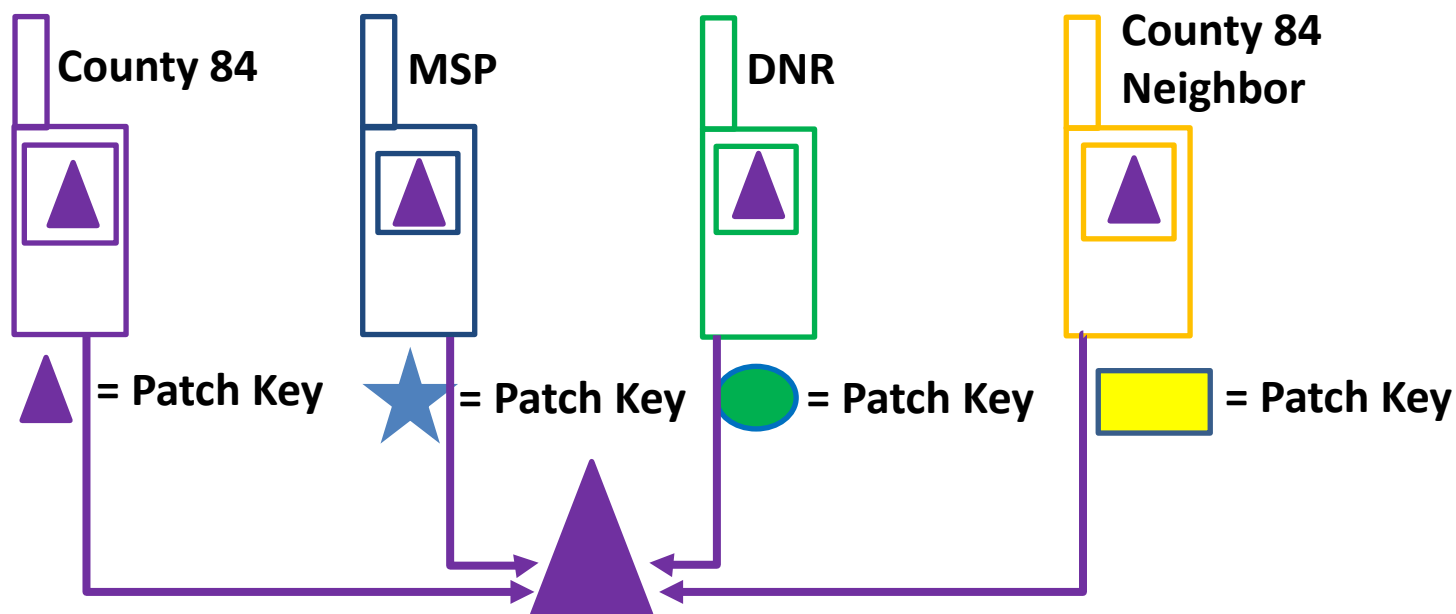
Patch Key Select	MPSCS
------------------	-------

Failsoft	
Secure/Clear Strapping	Clear
Key Select	MPSCS

Private Call	
Secure/Clear Strapping	Select
Key Select	MPSCS



Non-Patched 84P911 Encrypted

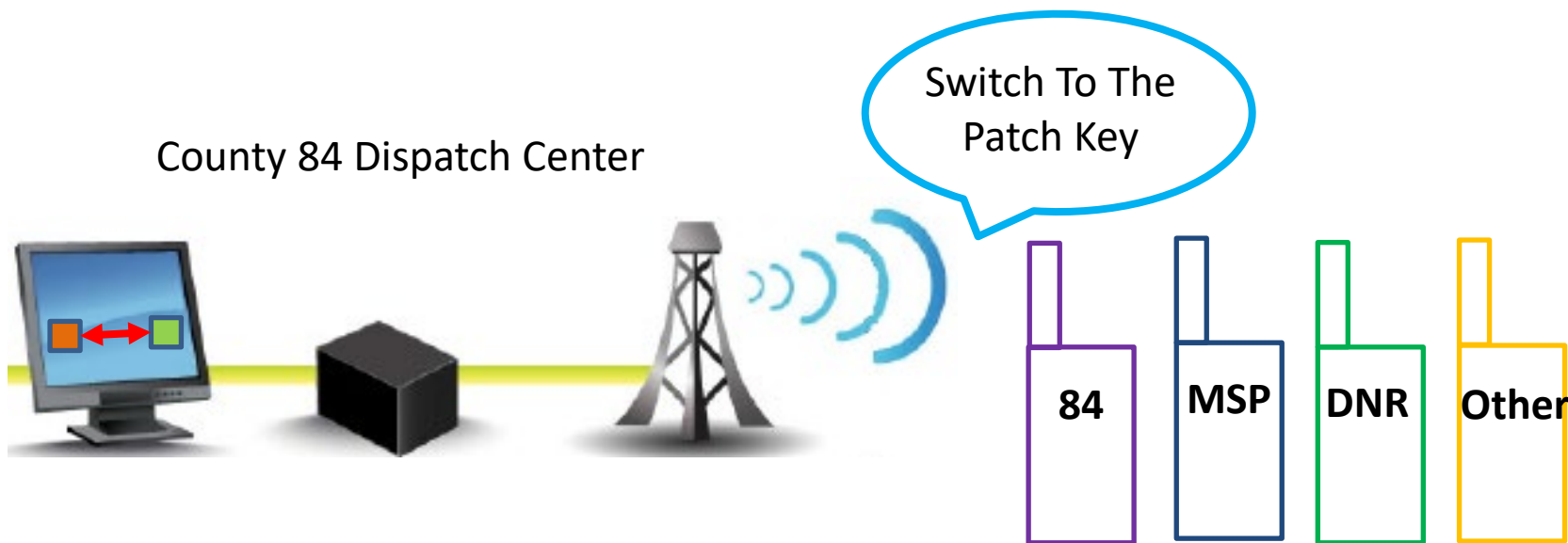


84P911 Encrypted Local Purple Triangle Key.

State Police, DNR, Neighbor Using Same Key ▲ on this Talkgroup



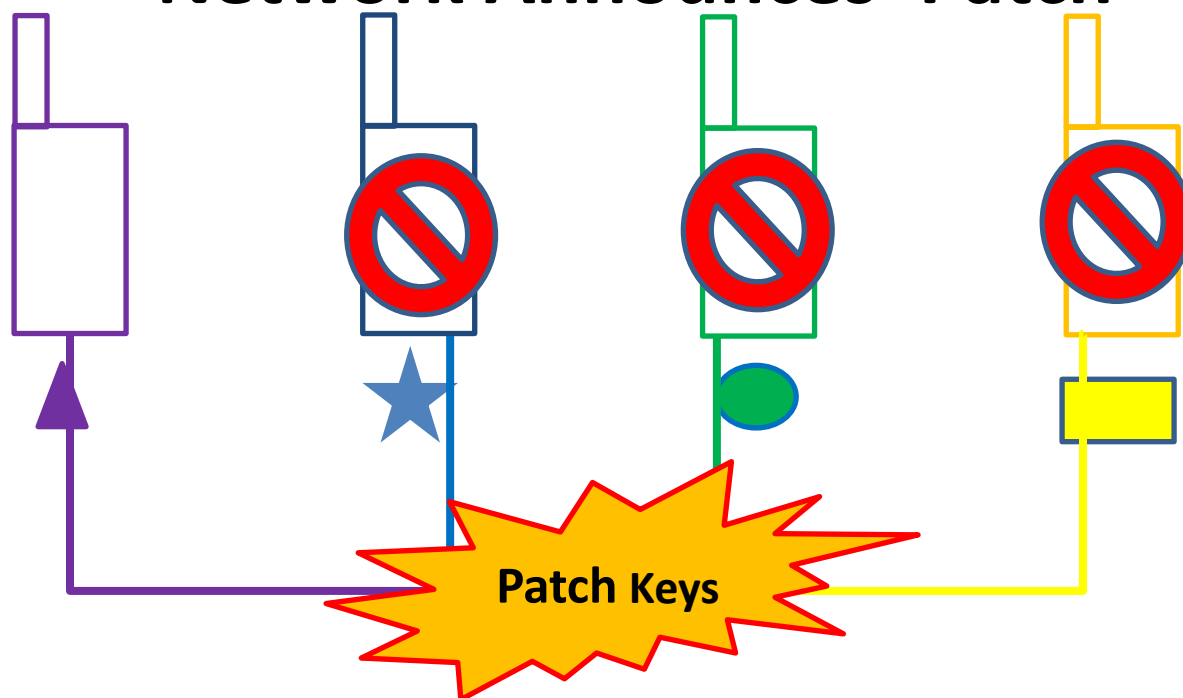
84P911 Patched to 84EMER1 Both Encrypted Same Key ▲



Network Announces 'Patch' to all radios on 84P911 and 84EMER1



84P911 Patched to 84EMER1 Both Encrypted Network Announces 'Patch'



County 84 Radios Use Local Purple Triangle Key.
State Police, DNR, Neighbor Use Programmed Patch Key



Path Forward

- Communicate that the purpose of the MPSCS is Interoperability – not individualized encryption
- Disable console patching of encrypted talkgroups until ALL involved agencies agree on a patch key and all radios are programmed to match decision.
- Migrate state agencies and all multi-key users to agreed patch key in geographic areas.

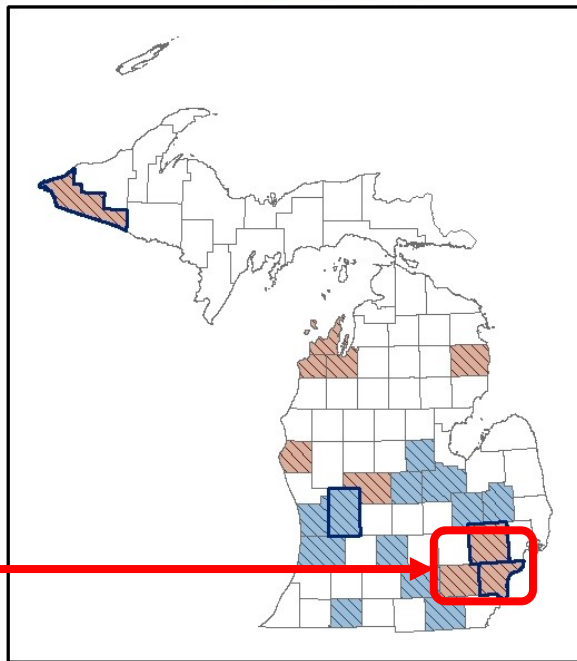


Path Forward – Determine Common Patch Key

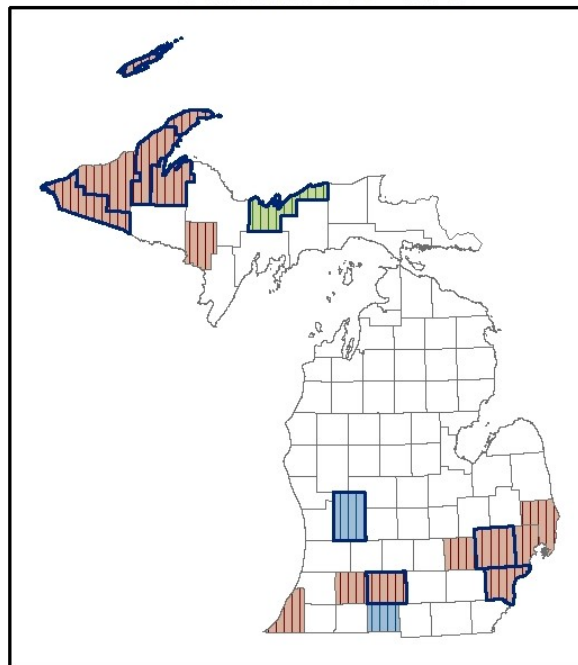
4 Common Patch Keys

- MPSCS ADP Key
- MPSCS DES-OFB Key
- Wayne County Agencies Common ADP Key

Current ADP



Current DES-OFB



State-Wide
51K APX
radios

Estimated 20K
APX radios



Path Forward

All of these efforts require significant resources and coordination on the part of the MPSCS Radio Programming Unit, the local agencies / vendors and dispatch centers, state agencies and MPSCS field technicians.

- Area encryption plan to be reviewed by MPSCIB encryption work group.
- RPU fully staffed can typically produce 2,000 radio files per month. Routine maintenance reprogramming and normal radio additions 2,000 to 3,000 radios per month. Nine counties on waiting list to move to MPSCS. What percentage of resources to use for encryption issue?
- Dispatch process changes and training required – no encrypted patching.
- Local agencies may have cost to load updated programming files.
- MPSCS field technicians will need to touch all involved state-owned radios.
- Dispatch process changes and training required to re-enable encryption patching when all involved radios are ready.



Path Forward – Implement System Wide Common Patch Key - P25 Standard AES-256 With Multi-Key



What are the talk-groups on the MPSCS that are widely shared? Considered as Interoperable Channels/Talk-groups?

- a. XXP911, XXE911, XXF911, XXFE911, (1-83)XXCOM
- b. Zone E STATW 1/2/3/5/6/7/8
- c. Zone F / NIFOG / MIFOG Interoperability Channels

Frequency	Alpha Tag	Description
769.24375	7CALL50/50D	7CALL50 - Primary Calling
769.14375	7TAC51/51D	7TAC51 - General Public Safety
769.64375	7TAC52/52D	7TAC52 - General Public Safety
770.14375	7TAC53/53D	7TAC53 - General Public Safety
770.64375	7TAC54/54D	7TAC54 - General Public Safety
769.74375	7TAC55/55D	7TAC55 - General Public Safety
770.24375	7TAC56/56D	7TAC56 - General Public Safety
770.99375	7GTAC57/57D	7GTAC57 - Other Public Service
770.89375	7MOB59/59D	7MOB59 - Mobile Repeater
770.39375	7LAW61/61D	7LAW61 - Law Enforcement
770.49375	7LAW62/62D	7LAW62 - Law Enforcement
769.89375	7FIRE63/63D	7FIRE63 - Fire
769.99375	7FIRE64/64D	7FIRE64 - Fire
769.39375	7MED65/65D	7MED65 - EMS
769.49375	7MED66/66D	7MED66 - EMS
770.74375	7DATA69/69D	7DATA69 - Mobile Data
773.25625	7CALL70/70D	7CALL70 - Secondary Calling
773.10625	7TAC71/71D	7TAC71 - General Public Safety
773.60625	7TAC72/72D	7TAC72 - General Public Safety
774.10625	7TAC73/73D	7TAC73 - General Public Safety
774.60625	7TAC74/74D	7TAC74 - General Public Safety
773.75625	7TAC75/75D	7TAC75 - General Public Safety
774.25625	7TAC76/76D	7TAC76 - General Public Safety
774.85625	7GTAC77/77D	7GTAC77 - Other Public Service
774.50625	7MOB79/79D	7MOB79 - Mobile Repeater
774.00625	7LAW81/81D	7LAW81 - Law Enforcement
774.35625	7LAW82/82D	7LAW82 - Law Enforcement
773.50625	7FIRE83/83D	7FIRE83 - Fire
773.85625	7FIRE84/84D	7FIRE84 - Fire
773.00625	7MED86/86D	7MED86 - EMS
773.35625	7MED87/87D	7MED87 - EMS
774.75625	7DATA89/89D	7DATA89 - Mobile Data

851.01250	8CALL90/90D	8CALL90 - Calling
851.51250	8TAC91/91D	8TAC91 - Tactical
852.01250	8TAC92/92D	8TAC92 - Tactical
852.51250	8TAC93/93D	8TAC93 - Tactical
853.01250	8TAC94/94D	8TAC94 - Tactical

- d. Zone G EVENT 1-15
- e. Zone H EVENT 16-30
- f. Zone I 31-46 ***MPSCS Key DES-OFB Selectable - Encryption Allowed**
- g. Zone J 47-62 ***MPSCS Key DES-OFB Selectable - Encryption Allowed**
- h. MABAS 800MHz Talk-groups
- i. Hospital ED/ER 800MHz Talk-groups (Ambulance/EMS to Hospital and vice versa use)
- j. AIRLZ1 & AIRLZ2
- k. CHOPHP1 / CHREG -1/2N/2S/3/5/6/7/8
- l. DNREEM - 1/2/3/5/6/7/8
- m. EMMD - 1/2/3/5/6/7/8
- n. INTERDIST Dispatch Console Talk-group

A. Current state of encryption on the system:

1. A description about the current state of encryption in Michigan. What is currently broken?
 - a) Three Encryption Algorithms in use. Ninety Seven unique encryption keys
 - b) Almost 2000 agencies on MPSCS with different levels of encryption needs
 - c) Network Connected Dispatch Consoles can patch talkgroups together and invoke "Patch Key"
 - d) Radio software allows for only one patch key per radio
2. Strategy for relief that describes the patch issue. **(Note: All of these efforts require significant resources and coordination on the part of the MPSCS Radio Programming Unit, the local agencies / vendors and dispatch centers, state agencies and MPSCS field technicians.)**
 - a) Priority is Interoperability – not individual encryption.

- b) Disable console patching of encrypted talkgroups until ALL involved agencies in geographic area affected, agree on a patch key and all radios are programmed to match said decision.
- c) Migrate state agencies and all multi-key users to agreed patch key in geographic areas.

B. Establishment of an expanded management framework for voice encryption in Michigan:

- 1. Establish an “Encryption Workgroup” under MPSCIB.
- 2. Work with Vendors and the agencies to document/determine the current state of console and subscriber encryption capabilities.
- 3. Add resources to MSPCS to handle subscriber/console/gateway encryption management. Including coordination with The National Law Enforcement Communications Center (NLECC).

C. Utopian goal of standardized encryption on the MPSCS by 2030:

- 1. Match the current P25 encryption standard of AES 256 Encryption with multi key capability on the MPSCS by 2030.
- 2. Leveraging these systems will help us accomplish the goal:
 - a) Establish Encryption Key Reference Fleet Mapping
 - b) OTAR “Over the Air Re-keying”
 - c) OTEK “Over the Ethernet Keying”

Recommend lifting of the current Encryption Moratorium, and recommend actions to take afterwards;

- 1. Implement the patch relief strategy as mentioned in A-2 above:
 - a) Priority is Interoperability – not individual encryption.
 - b) Disable console patching of encrypted talkgroups until ALL involved agencies in geographic area agree on a patch key and all radios are programmed to match said decision.
 - c) Migrate state agencies and all multi-key users to agreed patch key in geographic areas.
- 2. With proper communication/correspondence to the RPU by the requesting agency/entity/vendor, **encryption features can proceed to be added to current and future programming orders** so long as the following criteria are met before approved programming is set forth:
 - a. A detailed plan for encryption implementation must be submitted to the RPU along with the programming order by the requesting party.

- b. That plan must ensure and validate that any talk-group identified within the programming order adding encryption does **NOT VIOLATE INTEROPERABILITY** with other local/regional/state/federal entities on that talk-group.
- c. The plan must also identify that the talk-group(s) are of a proprietary use in nature, and are **not shared** with other agencies or entities. Unless all agencies and entities affected are in written concurrence (Example = MOU or Authorization) to use a shared encryption key.
- d. If a talk-group(s) that are going to be shared with multiple local agencies (example = local/county Drug Team), those agencies must provide a listing of all user agencies, and also define the type of encryption to be used within their “talk-group authorization” documents submitted to the RPU with the programming order.
- e. The RPU shall document (for each programming order) the encryption key reference, key ID’s issued and used, in order to provide reports or give a scope of current encryption use to the MPSCS System to the Executive Staff of the MPSCS and the MPSCIB respectively.

3. Implement Solution Steps B & C Above

DATE: 2/18 /2020

TO: Michigan Public Safety Communications Interoperability Board

FROM: Detroit South East Michigan Urban Area Security Initiative Interoperable Communications Committee Encryption Work Group

RE: MPSCS Member Encryption Policy

At the January 14, 2020 meeting of the Detroit South East Michigan Urban Area Security Initiative Interoperable Communications Committee (ICC), MPSCS representatives presented a letter from the Michigan Public Safety Communications Interoperability Board (MPSCIB) announcing a moratorium, effect December 10, 2019, on “all new encryption programming on the MPSCS until further notice”. This moratorium seems to apply to subscriber units and dispatch consoles. The letter also requests comment on two policies proposed for adoption by Michigan’s Public Safety Communications System (MPSCS).

A special meeting of the Detroit SEMI UASI ICC Encryption Work Group was convened on January 29, 2020 to discuss the two policies introduced by MPSCS: Member Encryption Policy and Member Device Management Policy. Representatives from Macomb, Wayne, Oakland, Washtenaw and St Clair counties as well as City of Detroit, SERESA, Livonia PD and FD, DHS, MPSCS and Motorola were in attendance. The UASI Board was represented as well.

We offer no comment on the Member Device Management Policy.

As to the MPSCS Member Encryption Policy, the Detroit SEMI UASI ICC offers the following comments:

Point 1

The Committee is in general agreement that the State should adopt a P25 compliant encryption algorithm for all MPSCS member agencies across all disciplines statewide.

Discussion

MPSCS has been touted as the interoperable communications system of choice for the entire state. In fact, this committee has adopted the MPSCS as the interoperable system of choice in the Detroit SEMI UASI region. Adoption of MPSCS by most agencies in the region, fulfills the Department of Homeland Security SAFECOM Interoperability Continuum best practice by providing first responders the most amenable circumstance for interoperable communications – a common system in routine daily use. The uncoordinated use of multiple encryption

algorithms on MPSCS effectively curtails interoperability as recent events in Genesee County have demonstrated.

While extraordinarily useful to maintain safety and security, encryption is a two-edged sword. Should first responders find it necessary to utilize encrypted communication at a common incident scene, yet lack common encryption means, they can't talk to each other. Therefore, it is the Committee's opinion that the problem of multiple encryption algorithms can only be remedied by adopting a common encryption algorithm for use on MPSCS.

Point 2

The Committee generally agrees that MPSCS is best suited to coordinate encryption use statewide for members.

Discussion

It is the opinion of some discussion participants that there is no need for an encryption policy promoted at the State level. Rather a "Home Rule" approach should be adopted where encryption planning and decision making is left in the hands of local agencies. However, most participants agree that the MPSCS is best positioned to perform this function.

For example, it was brought forth in our discussion that MPSCS is already performing key tasks of an encryption administrator such as, keeping databases for such items as encryption keys IDs, encryption keys and Memoranda of Understanding. The Committee recommends this practice be continued and expanded into a centralized database and clearing house for encryption matters. It is also our opinion that utilizing these databases to coordinate encryption deployments will contribute immensely to avoiding encrypted communications issues in future.

Point 3

The Committee agrees that as Encryption Administrator, the MPSCS should develop a plan to achieve the goal of a common encryption methods and practices in use across MPSCS.

Discussion

A general "road map" or timeline of events that map out a strategy to obtain the goal of a common encryption scheme statewide needs to be developed. Some elements of this timeline may include specific lines of authority, a model encryption plan, a model encryption MOU and action steps. The Administrator must also provide a streamlined process of approval of encryption plans. The process must include definite and brief timelines and the right of agencies to appeal when proffered encryption plans are disapproved. Due consideration must be given to legacy deployments. Unless funding is centralized, individual communities may find it extremely difficult to comply with planned changes that fall outside internal fiscal timelines.

Point 4

MPSCS should adopt a P25 compliant encryption algorithm.

Discussion

AES-256 is currently the only encryption algorithm that is P25 compliant. Therefore, AES-256 should be adopted by MPSCS as the common encryption algorithm for all member MPSCS agencies.

Point 5

The Committee agrees that legacy systems must be protected during any proposed changes.

Discussion

Many flavors of encryption are in use by MPSCS members in the Detroit SEMI UASI with a very high degree of success. There have been very large very recent expenditures for new subscriber equipment that included the MPSCS DES algorithm. Any proposed change of encryption algorithms will have an impact to local budgets and policy makers should keep these fiscal issues in mind. Should the MPSCS adopt the AES-256 standard for encryption, this should be accompanied by a ban on other algorithms.

Point 6

The Committee agrees that the State of Michigan should develop a standard "Encryption Plan". This plan should be a template for use of MPSCS users interested in adding encryption to their operations. An "Encryption Plan" should be a mandatory component for all encryption deployments.

Discussion

Along with standardized implementation, standardized planning is essential to ensuring efficient, cost effective interoperable communications. Each agency should be required to provide an interoperable communications plan to MPSCS as standard MPSCS practice. These plans should include the name or title of the agency "Encryption Manager", the type(s) of encryption to be used, CKR key numbering, the storage and handling procedures for encryption devices and keys and a standardized encryption MOU. Along with these items, any other items of importance MPSC deems necessary.

Point 7

The Committee agrees that the State of Michigan should develop a standard "Interoperable Communications Plan" for MPSCS users. This plan should be a mandatory component for all MPSCS deployments.

Discussion

While interoperable communications may be stifled by improper use of encryption, it can also be adversely impacted from a lack of consistent implementation at the state and local level. Much analysis went into a strategy to improve first responder communications in the US post 911. One of the main points brought out was this; before you can have "interoperable" communications, you must first enjoy "operable" communications. Thus, questions such as, who uses the system now? Who needs to talk to each other? How do they talk to each other now? Is the coverage of the existing system adequate? were posed so that public officials could make informed decisions on how to cost effectively solve daily communications issues and then, tackle interoperability.

Discussion participants remarked on the level of interoperable communications in their region and other regions and how the level of proficiency varies dramatically across the State. It seems some regions enjoy a high level of interoperability and participation while others do not. In some cases, agencies

won't talk to each other. It seems to us that the addition of encryption into this mix only adds another layer of complexity to an already problematic interoperable communications landscape. Much empirical evidence may be found to support this contention.

But this begs the question of interoperability implementation in Michigan and on the MPSCS. It seems to us that interoperability on MPSCS is left exclusively in the hands of local MPSCS members. Now, there are mechanism such as the Regional 800 and 700 MHz plans which promote the idea of interoperability, but post FCC license approval, these plans have no enforcement mechanisms. We suggest that this is a good time to consider including interoperability provisions into MPSCS standard procedures to address this issue. With the "encryption Moratorium" MPSCS can no longer make the claim that "we can't tell people what to do". As the MPSCS is a wholly tax-payer funded system, it seems appropriate that MPSCS administration adopt a policy of ensuring tax dollars are not wasted on an "interoperable radio system" that is not used for interoperability because members are not aware of or did not plan for such use. The provisions need not be onerous or costly to be effective.

Point 8

Dispatch systems must be included in planning and funding.

Point 9

The Committee believes the MPSCS should seek and secure grant funding or state appropriation to promote encryption interoperability within the State of Michigan.

Discussion

The MPSCS is in position to assist in brining P25 standardized encryption to the users of the MPSCS. By providing a funding model and development governance structure the MPSCS can prepare users across the state with technology and planning to ensure no agency is left without encryption options when their community has determined it is an essential part of their emergency communications plan.

Respectfully Submitted by

Keith M. Bradshaw, Chair

A handwritten signature in cursive script that reads "Keith M. Bradshaw".

Detroit South East Michigan Urban Area Security Initiative
Interoperable Communications Committee

From: [Bryce Alford](#)
To: [Jannereth, Kate \(DTMB\)](#)
Cc: [Terri Thornberry](#); [Bruce Gaukel](#)
Subject: Encryption interop on MPSCS
Date: Wednesday, February 19, 2020 11:21:44 AM

Kate, here are some comments on the policies for encryption recommendations.

On the 3 different states for encryption, we believe that the encrypted talk groups should all be strapped so it cannot be turned off.

We agree with the recommendations of not encrypting talkgroups used for interoperability. This should apply to Main dispatch talkgroups of P911, E911, F911 and County COM's and SPEV's.

For the 3 types of encryption algorithms, we agree that AES-256 should be a goal for all agencies but all 3 should be loaded into radios, this will be a cost issue for most if not all agencies. Motorola is giving ADP encryption for free but there is a big cost for adding the other 2 types and also Multi key is required at an additional costs we are told.

Another note for AES-256 that it be the standard base for MPSCS shall be P25 compliant. This will be a big change especially for MSP since their primary encryption type is DES-OFB.

OTAR: We have that feature in our contract and it should be very useful.

Key Sharing: We think this is a requirement as we will need interoperability with MSP and all surrounding counties.

Common Key Reference(CKR): We agree that we work with the MPSCS to assign unique CKR's to avoid duplicates and the same for KEY ID.

Thanks Bryce

Bryce C. Alford
911 Radio Systems Administrator
Ingham County Public Safety Radio System
balford@ingham.org
517 285-5330-cell

19 February 2020

Michigan's Public Safety Communications Interoperability Governing Board
7150 Harris Road
Dimondale, MI 48821

Esteemed Board Members,

I applaud the efforts of the State Interoperability Governance Board over the encryption conundrum. It is gratifying to see the Board is willing to tell people what to do, or rather, what not to do regarding MPSCS. For many users across the state, MPSCS delivers the highest level of interoperability per DHS guidelines as presented in the Interoperability Continuum as a "common system in daily use". Yet encryption, by its very nature, does nothing to further interoperability- just the opposite. A common encryption algorithm with a common encryption key is the only way I can see to bring about interoperable encrypted communications across the MPSCS, without the interaction of suitably equipped dispatch centers.

There seems to me two viable options: a short-term solution where encryption algorithms are standardized within some set time frame, and a longer-term solution which relies on normal equipment replacement cycles. Either choice may prove expensive, but a longer-term solution will perpetuate the inability of encrypted agencies to communicate. A short-term solution that involves the immediate upgrade of encryption to the AES-256 algorithm across the MPSCS would require State government funding. On the other hand, a much less costly short-term approach may be taken.

I suggest deploying ADP across all encryption capable units. ADP is already in use by many MPSCS agencies. ADP is offered by Motorola, in some case for free. While this solution would not be cost free, it will be significantly less expensive than purchasing AES or DES upgrades for all radios that do not currently have it. In this manner, a common encryption algorithm would be available to everyone for interoperable communications. I do not suggest that ADP be mandated for use. Agencies should be free to use the encryption means they wish. Rather, that ADP be a common

encryption means, at least temporarily, until it can be decided upon how to proceed with a more secure encryption standard.

Regardless of whether the above suggestion is adopted, the encryption effort will require a good deal of planning, efficient execution and knowledgeable management. I believe MPSCS is perfectly positioned to manage the effort to normalize encryption. Once a plan has been established, a mechanism to ensure compliance should be utilized. Perhaps the MPSCS "Go-Live" procedure can be modified to accommodate interoperability whether agencies utilize encryption or not, as a matter of initial system "turn-up".

In my opinion, to be successful across the state and across disciplines, elected officials must be made aware that these interoperability issues are important enough to codify, at the local and perhaps at the state level. First responder command staff must engage in interactions with their peers to develop the relationships necessary to interoperate successfully. These relationships should result in standard operating procedures (SOPs) that are reduced to writing and disseminated appropriately. Then, SOPs must be adopted and personnel trained in their requirements and exercised regularly in their use. Or whatever combination of the above gets the job done. Otherwise, though we may have a common encryption algorithm and common encryption keys, we will still have communications issues across agencies and disciplines.

It is clearly the intent of the Board to "tell people what to do" by way of the encryption moratorium. I believe the moratorium to be a good first step. I also believe it is time to "tell people what to do" vis-a-vis MPSCS regarding interoperability whether encryption is used or not. It is also my opinion that taxpayers have a right to expect equipment purchased for use of public safety first responders will be used in the public's best interest. For example, I believe taxpayers expect fire trucks will be used to put out fires and firearms will be used to protect the lives of sworn police officers and the public they protect. And they are. I also believe the public expects that personnel furnished with these tools will become proficient in their use and the tools provided will be maintained in top operating condition. And they are. I believe taxpayers have a

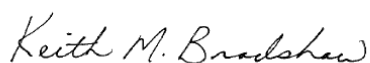
right to expect these things and that local governments have a fiduciary responsibility to ensure these taxpayer expectations are met to the best of their ability. I am convinced public safety officials wouldn't have it any other way. In fact, to meet taxpayer expectations and to provide for the safety of first responders, fire and police agencies devote much time and resources to train their personnel on the use of the tools provided. These training efforts are in some cases, immediately graded by the public as they watch response efforts courtesy of local media.

In this day and age, the taxpaying public has a right to expect that no matter how many MPSCS agencies show up at a common incident scene they will be able to talk to each other. With or without encryption.

Please understand that the views and opinions stated herein are strictly my own and do not reflect the position of Oakland County or any of my previous employers or any of the committees on which I have the honor to serve.

Please do not hesitate to contact me if you have any questions regarding these comments.

Respectfully,

A handwritten signature in cursive script that reads "Keith M. Bradshaw".

Keith M. Bradshaw
Supervisor, Radio Communications Oakland County CLEMIS
Chair, Michigan Public Safety Frequency Advisory Committee
Chair, Detroit South East Michigan Urban Area Security Initiative Interoperable Communication Committee
59991 Havenridge
New Haven, MI 48048
586-749-9356
Kbrads48310@gmail.com

From: [Jarvis, James](#)
To: [Jannereth, Kate \(DTMB\)](#)
Subject: RE: Encryption Interoperability on Michigan's Public Safety Communications System
Date: Tuesday, January 21, 2020 9:52:48 AM

Kate,

Glad to see that ADP from the original draft policy has been replaced with the standard being P25 compliant!

As stated at the MPSCIB meeting, this is a great first start toward encrypted interoperability. In addition to a policy, there should be a full encryption management plan that includes key management and statewide SLN management.

My thoughts on the draft:

Subject and Purpose: Should be straight forward.....The purpose of this policy is to establish a procedure for implementing encrypted voice communications on the MPSCS that will allow for interoperability among system users.

The Policy section should be more prescriptive.All MPSCS member agencies will obtain written approval from the MPSCS Director through the RPU prior to implementing encryption. Member agencies will submit an encryption strategy that includes an implementation plan, key management plan, and impact to interoperable communications with other agencies.

All of the extra's on position of MPSCS and before purchasing can be removed.

Also, instead of referring to the best practices document, consider placing snippets of information on the policy document as Technical Background that identify encryption capabilities and concerns as they apply in Michigan. And – the policy does not include how SLN's and KID's are identified and managed.

Here is one example on possible language from another State:

Capabilities

Encryption keys are used in end user equipment where encrypted voice communications are utilized. This includes, but may not be limited to, subscriber radios, dispatch consoles and radio voice logging equipment. Encryption utilizes an encryption key (a string of hex characters of varying length depending on the encryption protocol utilized) and a Common Key Reference (CKR) used to select or index the desired key. Because many different encryption keys may be active on the system at any time, the CKR is transmitted with the encrypted transmission, so that the receiving equipment will know which encryption key to use to decode the transmission.

Constraints

If a radio user or dispatch console utilizes encryption and other users on that talkgroup do not have the correct encryption key in their equipment, they will not receive the message. Any radio voice logging equipment that does not have the appropriate encryption keys will not log the voice traffic.

CKRs must be unique across the system.

While it is possible for more than one key to be identical, no two encryption keys should use the same CKR. E.g. If a region has CKR "1" with a key of "12345678" and there is a statewide key with CKR of "1" with a key of "00000000", this would cause the receiving unit (radio/console or voice logging equipment), to not accept one of the keys, or the unit would not know which key is appropriate for receiving an encrypted transmission with "CKR 1."

Thanks for the opportunity to comment.

I also recommend a request for CISA technical assistance for an encryption workshop. This will include assistance with developing a statewide encryption plan vs a policy that is requiring each agency desiring to use encryption to come up with their own plan.

Jim

From: [Lisa Hall](#)
To: [Jannereth, Kate \(DTMB\)](#)
Cc: [Bryce Tracy](#)
Subject: Fwd: Encryption Interoperability on Michigan's Public Safety Communications System
Date: Tuesday, February 18, 2020 7:39:00 AM
Attachments: [MPSCIB Encryption Recommendations and Best Practices.docx](#)

Kate,

Here are some of my questions/comments.

First, please understand I come from a place of good. I understand the problem and get we need a good long term plan to avoid a bigger mess. I'm not against a plan or policy. I do want to make sure that you all preserve the hard work done to establish trust and relationships with non MSP users. Approach and language to subjects like this are important. I don't want to see things go backwards. Some of my comments are directed toward that.. ensuring positive working relationships and maintaining the trust levels.

I spoke with Bryce and he explained the group is not really looking for feedback on the guidelines since those have been approved already. However, for me because the policy refers to the guidelines, it's important that what's laid out in the guidelines is in line with the policy and vice versa. Currently, these two documents together don't really compliment each other. OR, the policy needs more guidance and information in it.

The policy states, before a solution can be purchased, notification must be made and approval must be given. Approval of what? The solution and a plan? Just the solution? Just the plan? Policy really doesn't say. It should be clear what needs to be approved and how to get there.

An observation - this policy is attempting to define an agencies purchasing policy. MPSCS can't dictate what I can and cannot purchase. (I do realize that is not the intent.) I believe the intent is to clearly define that radios and consoles will not be approved to be connected to the MPSCS without an approved encryption solution and plan.

Policy

Before purchasing an encryption solution (As stated above... is the intent to dictate a purchasing policy? I believe guidance should say BEFORE purchasing, make sure the encryption solution is one that would be approved for connection and list the available solutions. Policy should say in order for a device (radio, console, pager, etc.) with encryption to be connected to MPSCS, it must have a MPSCS approved encryption solution and list the solutions. I appreciate these may change, wording can indicate other solutions can be submitted for review) on any MPSCS connected radio, pager and/or dispatch console, members must notify and obtain the MPSCS Director's signature approval (as mentioned above, approval of what - the solution selected, a plan, both??) through the MPSCS Radio Programming Unit. The documentation (what documentation? This should be something like: In order to receive approval, an encryption plan must be submitted for approval that must include...) must include the (add in type of encryption solution), member's encryption strategy, implementation plan, impact to interoperability and communications approach (what does this mean? Is this a notification plan or MOUs or??) to public safety partners.

This allows the MPSCS to ensure the impact (ensure the impact? would be better worded ensure the impact of the encryption solution is understood and communicated to all users) of implementing encryption by

each member, has the appropriate level of awareness to all other impacted members. While it is not the position of the MPSCS to mandate public safety communications encryption practices (you aren't mandating but if this needs 'approval' there are things that you are mandating. I don't like this wording. Doesn't seem appropriate for a policy.) , it is the position of the MPSCS to preserve interoperability (interoperability with WHO? MPSCS provides interoperability with statewide talkgroups. What if an agency doesn't want interoperability on their main dispatch talkgroup with any agency outside of theirs to include MSP? Are you going to dictate that they MUST allow MSP access to their local dispatch talkgroup? And if so under what authority? Can't use MPSCS unless MSP has access? Hate to see you go backwards with this. But if this is really what is wanted, that needs to be clear here.) across emergency response in Michigan. These steps (what steps? It would be better to say approval must be sought when changing an existing encryption solution) should be taken any time an MPSCS member is changing encryption on any talkgroups.

The standard base encryption for the MPSCS shall be P25 compliant. The Michigan Public Safety Communications Interoperability Board (MPSCIB) will review all changes to recommended guidelines. (This seems out of place. Either you need to list the must haves and must nots or you need to refer to a recommended guidelines document for a list of must haves and must nots and then say they will be reviewed and updated by MPSCIB.)

Refer to the Encryption Recommendations and Best Practices guidance document as approved by the MPSCIB. (In my opinion, this document needs reworked if it is going to the guide for approval or not. I should not have to guess on what will be approved and not be approved. It needs more information on what encryption is and what the impacts are and what needs to be taken into consideration. You need someone to look at it that isn't familiar with what it is and why you would care about if I encrypt something. And all the pieces it affects to include dispatch. While you say you shouldn't encrypt a main channel, it should be included that consoles are a part of that consideration - if you ever want dispatch to hear you or have the capability of hearing you... that has to match too. I know that's something YOU all know but that isn't obvious to others.)

Again as stated before, as a user, I understand what you are trying to get to and why. But I do not like unclear expectations and an unknown. This is a policy that just says the Director has to approve. It doesn't tell me what needs to be considered and how to get there. This just leaves it up to him and if I'm an untrusting person of 'the State'.. this is an added reason to not participate. MPSCS has worked hard to gain the trust and respect of 'the local users'... I don't want this to take that backwards. This needs more information on the how/why for those that aren't knee deep in it so an understanding can be gained before wrong opinions are formed. I don't disagree with the intention or direction but I also want to maintain some local control over the decisions we make and how we want to operate. That is mostly about education and impact which I know you all know but that needs to be portrayed in here too. And I do worry that a part of this about MSP interfacing if an agency says.. if we have MSP involved in something we will move to an event channel otherwise we don't care that MSP doesn't have this solution and we are giving them our P911 talkgroup anyway... what's the answer?

I've attached what I started on the guidelines but I did stop after I spoke with Bryce. I have more notes on them but I'll save them.

----- Forwarded message -----

From: MPSCS <dtmb@govsubscriptions.michigan.gov>

Date: Wed, Jan 15, 2020 at 2:25 PM



From Lisa Hall: Encryption Recommendations and Best Practices

Talkgroup needs to be consistent throughout the document.. talkgoup or talk-group?

Purpose:

Provide education and guidance to police, fire, emergency medical, emergency management, transportation, public works and critical infrastructure governmental agencies regarding the programming, keyloading and use of encryption features on 700/800 MHz radios. (Forgot your good friends in dispatch.)

Background:

The Michigan Public Safety Interoperable Communications Board (MIPSCIB) has been charged with the responsibility of coordinating interoperable public safety communications in Michigan. Numerous public safety agencies and governmental disciplines use 700/800 MHz trunked and conventional radios intended to provide interoperable communications between all public safety and governmental disciplines. Radios on the Michigan Public Safety Communications System (MPSCS) are programmed with a basic radio interoperability template that includes statewide interoperable talkgroups as well as 700/800 MHz analog and digital channels and talkgroups that are part of the non-Federal national interoperability plan.

At the request of public safety members, and by the growing demand for a solution to provide more secure public safety radio communications, the MPSCIB has drafted this document to provide education, give and guidance, and set a path/process for MPSCS users and the MPSCS Radio Programming Unit (RPU) to add encryption features to radio templates for use during day-to-day operations, or at during significant events where transmission of sensitive information over non-encrypted radio channels may put the safety of personnel or the public at risk.

As a result, the MPSCIB has adopted these encryption recommendations and best practices to ensure and maintain help promote the education and guidance for all users, while maintaining a high level of interoperability. for mutual aid clear/open and encrypted/secured communications.

Definitions:

Types of Encryption Algorithms

- **ADP (Advanced Digital Privacy)/ARC4** Low security encryption. Usually loaded in template but can be loaded with keyloader.
- **DES-OFB (Digital Encryption Standard Output Feed Back)** Medium security encryption that is usually loaded with keyloader but can be loaded with software.



- **AES256 (Advanced Encryption Standard)** High security (Federal Grade) encryption that can be loaded with keyloader or software (in some radios).

Types of Encryption Activation Settings

There are three different states for encryption: Clear, Selectable and Strapped (secure).

- **Clear** is ~~used a state of~~ ~~when there is~~ no encryption on the talk-group and ~~the~~ encryption cannot be turned on.
- **Selectable** ~~can be used~~ is a state ~~allowing to turn~~ encryption ~~to be turned~~ on or off using a switch or button or other radio feature selectable setting.
- **Strapped** is ~~used a state of encryption on the talkgroup always on~~ ~~when the talk group is always encrypted~~ and cannot be turned off.
- **Infinite Key Retention:** ~~Selected in the radio template/programming to retain the keys if power is removed from the radio. If unchecked the radio will lose all keys if power is removed and that talkgroup may lose the ability to transmit on encrypted talkgroups on the system.~~

Talkgroup Encryption

(I would define encryption here. What does it mean? You are taking for granted that people know what it is or have a broad understanding of it. I did not when we first came on the system which caused a big programming issue which is exactly what you are trying to avoid by having standards.)

Talkgroups can have different levels of encryption depending on how they are used. Any talkgroups that are used for interoperability with ~~different~~ multiple agencies or have the possibility of ~~someone~~ a critical interfacing agency not having a specific encryption level, type or key ~~should not use the~~ must use caution in selecting an encryption type or level ~~feature~~.

Talkgroup Encryption Recommendations:

Talkgroup encryption is not recommended for main (should not use 'county') dispatch talkgroups, statewide common talkgroups, special event talkgroups or any talkgroups used for multiple agency interoperability. Radio traffic over encrypted talkgroups is limited to users with radio that contain the exact agency encryption key, type and level. This would include mutual aid agencies from different jurisdictions and the Michigan State Police. An agency encrypting a main dispatch talkgroup would need to ensure that all users that require access to that talkgroup had hardware capable of the encryption and encryption keys. This could lead to equipment replacement and programming costs.



An agency could implement both clear and strapped talkgroups to allow for communication options based on secure transmission needs for traffic and events. It is recommended that designated encrypted talkgroups use the strapped setting to avoid accidental clear transmissions.

~~This would include but not be limited to county main dispatch, common, special event and interop channels/talkgroups. If there is a need for encryption on county interop channels/talkgroups, you should split them over several channels with talkgroups that are designated with some being clear and some being strapped.~~

If the talkgroup needs to be both encrypted or clear depending on how it is used and who has access to encryption then it should be set to selectable. This should mainly be used for talkgroups that cover a large area and are in a large number of radios. The MPCSC Zone I and J event talkgroups use this selectable encryption feature and only use the MPSCS DES-OFB encryption key.

For talkgroups that are encrypted and everyone using them has encryption then they should be set as strapped. This gives the radio user the defined knowledge that the talkgroups will always be encrypted and not be set to clear by mistake.

1. Leave your dispatch/common shared talkgroups (P911, E911, F911, FE911, County COM1-83, and SPEV) free from encryption features for interoperability with your surrounding agencies. Other talkgroups can have encryption enabled to maintain secure communications.
2. If any agency/county/dispatch wishes to encrypt their P911s, or talkgroups corresponding to P911s whereby day-to-day law enforcement calls for service, etc. are transmitted/received, they use the standard MPSCS encryption key, whether it is ADP or DES.
3. If any agency/county/dispatch wishes to encrypt a P911 or other talkgroup, they should immediately notify MPSCS and local and surrounding stakeholders so plans can be made in advance to rewrite codeplugs to support the encryption, update Memorandums of Understanding (MOUs) if needed, purchase encryption boards if the radios are not capable of it, and determine pathways for unencrypted communications in the interim.
4. It is recommended that the MPSCS key be used for CKR1 which is used in the consoles during a multiselect usage.
5. It is recommended that the MPSCS key be used for the Private Call, Failsoft, and Dynamic Regrouping features in the radio programming.

MPSCS uses all three types of encryption algorithms, however both the ADP and DES-OFB algorithms are not P25 standard compliant. Because the lower security algorithms are still used in many radios across the State, it is recommended that all three different algorithms be loaded into a radio if using encryption to ensure interoperability with all other agencies.



Encryption Feature Setting Recommendations:

1. Use **strapped** when using talkgroups that are always going to be encrypted. (Examples = Drug Team, Tactical or Agency Specific “Proprietary” talkgroups).
2. Use **selectable** for Zone I and J Event talkgroups. (Is the recommendation that selectable be used ONLY for Zone I or J or is selectable to be used for talkgroups that allows an option for encrypted communications for specific traffic or events such as talkgroups in MPSCS established zones I and J?)
3. **Select Infinite Key Retention** ~~Recommended that it is checked~~ in the radio and template programming ~~to be selected to~~ retain the keys if power is removed from the radio. If unchecked the radio will lose all keys if power is removed and that talkgroup may lose the ability to transmit on encrypted talkgroups on the system.
4. **Ensure Encryption Interoperability** ~~Recommends that by sharing certain encryption keys be shared~~ between agencies to allow ~~interoperability access and communication on encrypted across different~~ talkgroups.

Algorithm Type Recommendations:

1. Use the current P25 compliant algorithm (currently AES256) in your radios.
2. Use older, non P25 compliant algorithms, when communicating with other agencies using older standards. (Install all versions that are available to maintain interoperability including encryption security with other agencies.)

Multi key

Radios come with either a single key or multi key option in them.

- Single key allows only using a single key between multiple algorithms. This will limit interoperability between agencies.
- Multi key allows multiple encryption keys to be used in the radio.

Recommendations:

1. Purchase multi key option when using encryption in your radios.



Common Key Reference (CKR) Systemwide Reference Number

The CKR is used as a reference number between a keyloader and a radio when adding encryption to the radio. It is recommended that each agency have a unique CKR number to avoid confusion between different radios and agencies. An agency is not required to give their encryption key to the MPSCS Radio Programming Unit but it is required that they coordinate their encryption CKRs with them to avoid any confusion.

CKR Recommendations:

1. Work with the MPSCS to assign unique CKRs and to avoid duplicates.
2. Reference the CKR when requesting encryption for updates in the software.

Key ID (KID)

The key is a number that is specific to the encryption key and must be unique across the system or it can lead to conflict. Duplicate KIDs are not allowed in the software or keyloaders because of software limitations.

KID Recommendations:

1. Work with the MPSCS Radio Programming Unit to assign unique KIDs and to avoid duplicates.

Over the Air Rekeying (OTAR)

OTAR is the ability to rekey the radio over the system without the use of a keyloader. This provides the ability to issue a new key quickly and without the possibility of missing radios or having older keys that don't work. This should be used to eliminate the possibility of a lost or stolen key or if constant key updates are needed for secure communication.

OTAR Recommendations:

1. Use OTAR for constant key updates and to avoid the use of multiple keys per agency for key security.
2. Use one key that is changed on a regular basis instead of several keys that are never changed.

Key Sharing

To use or have access to another agency's talkgroup you must have a MOU stating that you can have it programmed in your radios. You must also obtain any encryption keys that are used for the talkgroup. The MPSCS does not share any DES-OFB or AES keys that are in possession of the State (State or Local keys) with another keyloader but they can be loaded into any radio or console that has encrypted



talkgroups in them. MPSCS radio techs (through coordination with the MPSCS Radio Programming Unit) will load any State keys that are needed into a radio upon request to ensure secure communication in that radio.

The ADP software keys can be viewed in the software without a system key and can be shared in both radios and keyloaders.

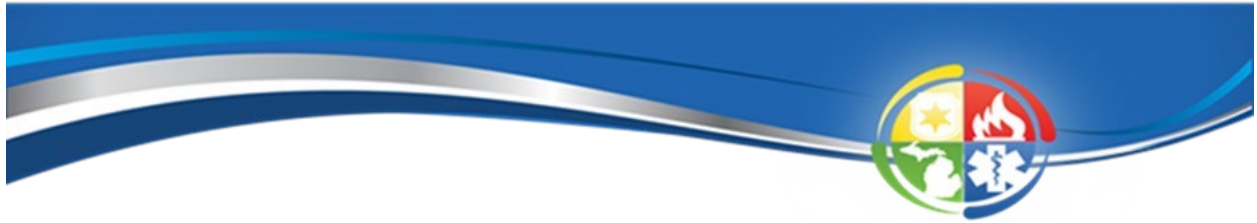
Reference the MPSCS policy that all radios being removed from the system have all keys erased before transferred to another agency or removed from the system.

Key Sharing Recommendations:

1. Load encryption keys in the radios of other agencies that are going to use your encrypted talkgroups so secure communications and interoperability can be maintained.
2. It is recommended that accurate records be kept by the authority having jurisdiction to maintain accountability and tracking of shared encryption keys, in coordination with radio inventory list.

Best Practices for Encryption Security

1. Keyloader security
 - a. Password protection: keyloader must be password protected.
 - b. Physical security: Must be stored in a secure location and maintaining a strict chain of custody.
 - c. Accountability: Shared authorization of keyloader use and access from multiple consenting authorities.
 - d. Sharing of keys between keyloaders: Keys should only be shared with a MOU agreement between authorized parties. Once that key is shared it cannot be recalled unless of a compromised security breach. Should be supervised by the owner of the key being shared.
2. Key rotation
 - a. Use OTAR for key rotation in a large number of radios.
3. Compromised keys
 - a. There should be timely notification when keys are compromised (within 24 hours).
 - b. Develop a key replacement plan.
4. Compromised radios with loaded keys



- a. There should be timely notification when radios are lost or stolen (within 24 hours).
 - i. Compromised radios can be used to monitor encrypted traffic.
 - b. Radios removed from service, transferred or sold should have all keys erased.
 - i. Keys must be erased manually or with keyloader separate from programming software.
5. Key documentation and security
- a. Document hard copy key strings and store in a secure location.
 - b. Maintain a list of radios that have that key installed.

From: [Petres, Christopher](#)
To: [Jannereth, Kate \(DTMB\)](#)
Subject: Comment on MPSCS Encryption Management Policy
Date: Wednesday, February 19, 2020 10:49:40 AM

Please accept my response to the request received in a letter dated January 9, 2020 from the Michigan Public Safety Communications Interoperability Board, seeking comments on new drafted policies.

I have a few comments regarding the MPSCS Member Encryption Management Policy.

I am opposed to all encryption used for routine communications. This includes dispatch, secondary dispatch, fireground, and any sidebar channels. This is a similar stance to the recommendations as listed in the MPSCS Encryption Recommendations and Best Practices document.

I understand there are times encryption is needed to ensure security of sensitive operations such as CID, protection details, SWAT and similar. These potentially sensitive operations are the exception, not the rule.

In my experience, encryption breaks interoperability. Talkgroups once shared with other agencies may no longer be functional once the owner turns on encryption. This may not be known to all users with access to the talkgroup, therefore they may still expect it to work. All this was noted in the memo, and I concur.

Encryption adds layers of complexity for technicians and users. Users often do not have the knowledge or patience to understand the "why" or "how" to operate and apply advanced functions properly and effectively. More options, such as unnecessary encryption, adds layers and "just something else to go wrong." This is especially true when settings are not strapped and user-selectable. When user selectable, all the efforts spent in creating secure communications can be easily defeated by accidental or uninformed user action.

Many times encryption requires a higher tier radios or upgraded models at significant cost. This would be necessary for all users with that talkgroup. Not all agencies have the financial resources to upgrade their radios just because a neighbor uses encryption. In this example, neighboring jurisdiction may now have to scramble to shoulder the burden of replacing their perfectly good radios just to talk to their neighbors once again. Higher-grade encryption is often an additional cost over standard encryption as well. P25 standards do not include these lower grade (often lower cost or free) encryption options.

Encryption can greatly limit options regarding equipment selection. There are times consumer-grade receivers would easily satisfy operational needs, and at great cost savings. As consumer equipment lacks encryption ability, this option is removed. Overhead speakers within a fire station could be served by a moderately priced scanner, rather than a high-tier and cost radio. Many legitimate public safety users also rely on scanners. A few examples may be to listen to neighboring agencies when a formal talkgroup sharing MOU does not yet exist, a volunteer firefighter only issued a VHF pager but all further communications are only on 800, a user who wishes to keep a subscriber unit on a main talkgroup but would still like to scan without altering scanlist in the subscriber unit. I have personally installed scanners into dispatch consoles and voice logging

equipment for economical monitoring of non-primary talkgroups.

Many will argue HIPAA as a reason for encryption. Many professional publications disagree. "HIPAA does not apply to *communications required to treat patients or to information shared for operations purposes*. 45 C.F.R. § 164.501 Since information shared by a dispatch agency is shared to treat patients and to operate effectively as a dispatch service, HIPAA most often does not apply to the communication. These are considered incidental disclosures, which HIPAA's provisions specifically permit. However, if it is not necessary to transmit a patient's name or certain information for the purpose of treatment or service, it is best to omit that information from the unencrypted transmission. In large part, though, these communications pose no concern under HIPAA." -

<https://urgentcomm.com/2014/07/23/emergency-medical-dispatches-and-hipaa-are-you-hipaa-compliant/>

Furthermore, hiding information from our citizens does nothing for government transparency. Public safety needs as much public support as it can get.

Lastly, obscuring communications becomes moot when authorized users of the radio system publish their content in real-time across numerous social media outlets, forums, and incident information sharing services. These appear to be rouge actors not acting in any official or Public Information Officer capacity. The best implemented plans and technology can all be for nothing when these actors divulge the contents of secure communications.

In conclusion, I support encryption only in select cases and never as a widespread or blanket application. I agree with the contents of the Best Practices document and draft policy. While the policy states it is not the position of MPSCS to mandate encryption practices, I believe it should encourage the easiest and most reliable method of interoperable communications, which is clear voice.

Chris Petres
Driver/Engineer/Paramedic
Radio Maintenance
Waterford Regional Fire Department

From: [Chris Petres](#)
To: [Jannereth, Kate \(DTMB\)](#)
Subject: Comment on MPSCS Member Device Management Policy
Date: Wednesday, February 19, 2020 12:02:44 AM

Please accept my response to the request received in a letter dated January 9, 2020 from the Michigan Public Safety Communications Interoperability Board, seeking comments on new drafted policies.

I have a few concerns regarding pagers within the MPSCS Member Device Management Policy.

It is my understanding MPSCS does not account for pagers with IDs or serials. As there is not really any way to track these devices, requesting notification of disposal via the Device Enable / Disable Form seems like an unnecessary paperwork burden. To my knowledge, pagers are currently unable to be remotely disabled or inhibited like typical subscriber units.

Pagers are a receive-only device. If an individual were to obtain one and even modify programming, there would be no impact on system performance or security.

As they do not transmit, system keys and similar sensitive information is not needed nor contained in these devices. As this information is not there, it cannot be read.

Pager programming does not contain any RF information not already publicly available by various means. The *existence* of a talkgroup / pagegroup is easily obtained by a scanner, although exact use or name may be *confirmed* with PPS data. I feel this is very low risk and sensitivity. This information can also be easily protected with passwords within programming.

Pagers are basically fancy scanning receivers with no impact on the system. There are many personally-owned pagers on the system by both hobbyists and public safety users. Likely some have been cloned from official use devices. It would be impossible to establish how many of these exist. As privately owned, there is no control or tracking. Without this knowledge, it is impossible to keep this information out of circulation, a perceived goal of this policy.

For pager units utilizing clear voice, I feel little or no action is needed prior to disposal. It can monitor nothing a scanner can't and likely contains no data not already factory programmed into most modern scanners.

I do not have much experience with encryption related to pagers. Obviously encryption keys require more controls. While I assume keys cannot be read from a device and are safe, it does little to protect eavesdropping using a disposed, lost or stolen device that can still decode secure voice. When possible, these should probably be erased prior to disposal to prevent undesired monitoring as listed in the draft policy. However, without an

inventory database available, no one can be assured this is done.

Beyond transferring or disposing of assets, when it comes to securing agency data and programming contained within pagers, passwords have not been used everywhere. This leaves data vulnerable to anyone with a USB and downloaded PPS. When used, password protected programming is also only as secure as the password. I can testify some of these passwords have been shared with unauthorized persons. This has had the detrimental effect of degraded performance on some units and lack of standardized programming within the agency. These compromised passwords also create the potential for the password and pager-contained information to leak beyond the agency. It seems pager management and security has been lax thus far. Passwords are not mandated and have not always been an option. Additional policies or steps should be taken to re-enforce pager data security, when chosen to be used.

Chris Petres
Firefighter / Paramedic
Explorer Advisor - Post 1717
Radio Maintenance
City of Northville Fire Department
248-974-3943

From: [Al Young](#)
To: [Jannereth, Kate \(DTMB\)](#)
Subject: MPSCIB Encryption Recommendations for MPSCS
Date: Friday, January 31, 2020 8:59:18 PM

After reading both documents, I am in agreement with both. They spell out "common" functionality and security which will be easy to follow for all agencies.

--

Capt. Al Young
B-Shift Shift Commander
Taylor Fire Department
23345 Goddard Rd
Taylor, MI 48180
w(734) 374-1318 c(734) 231-6022
email: ayoung@ci.taylor.mi.us

Downriver Haz-Mat (DERT) Technician - Training Coordinator



STATE OF MICHIGAN
MICHIGAN PUBLIC SAFETY COMMUNICATIONS INTEROPERABILITY BOARD
LANSING

January 9, 2020

Attn: Michigan Public Safety Agencies
Michigan Public Safety Fraternal Organizations
Michigan 9-1-1 Community
Michigan Emergency Managers

Re: Encryption Interoperability on Michigan's Public Safety Communications System

To All Those Concerned and/or Affected,

The Michigan Public Safety Communications Interoperability Board (MPSCIB) in conjunction with the Office of Michigan's Public Safety Communications System (MPSCS) collaborates with Michigan's public safety partners, to provide and promote statewide communications and interoperability across all platforms. It also adopts procedures and best practices to oversee the organization and operations of public safety communications and interoperability throughout Michigan. The Board is responsible for advising the Governor on all interoperability aspects within the emergency communications ecosystem to ensure the public safety community is leveraging available technology both today and in the future.

As most of you may be aware, encryption has been implemented in various communities across the State of Michigan in multiple configurations with varying degrees of success. Through this adoption, it has become clear to the MPSCIB that greater planning and oversight is necessary to ensure the integrity of public safety interoperable communications across disciplines and geographical coverage areas for mutual aid efforts. **The non-standardized implementation of encryption across Michigan has demonstrated the risk to public safety due to the loss of interoperability between responding agencies. The MPSCIB cannot stand by actionless and thus issued a moratorium on December 10, 2019 on all new encryption programming on the MPSCS until further notice.**

The MPSCIB is requesting comment on the two attached policies by February 19, 2020 for discussion at either the March 10, 2020 or a specially called MPSCIB meeting for the purpose of this continued discussion. Comments can be sent to JannerethK@michigan.gov. Please reference the board approved [Encryption Recommendations and Best Practices document](#) prior to responding. To read current encryption discussion by the MPSCIB, please see the [Board's minutes](#) dating back to February 19, 2019.



STATE OF MICHIGAN
MICHIGAN PUBLIC SAFETY COMMUNICATIONS INTEROPERABILITY BOARD
LANSING

For your further consideration, AES 256 encryption is the P25 Standard and to qualify for federal grants, a device must be P25 compliant.

Sincerely,

Lieutenant Colonel W. Thomas Sands, Chair
Deputy Director
Michigan State Police



Mr. Bradley A. Stoddard, Vice-Chair
Statewide Interoperability Coordinator
Michigan's Public Safety Communications System
Department of Technology, Management & Budget

Attached:

Draft MPSCS Member Device Management Policy

Draft MPSCS Member Encryption Policy

[MPSCIB Encryption Recommendations and Best Practices](#)

	MICHIGAN'S PUBLIC SAFETY COMMUNICATIONS SYSTEM		
Effective Date: TBD Revised Date: Reviewed Date:	Program Name:		Category: <input type="checkbox"/> Internal <input checked="" type="checkbox"/> External Type: <input checked="" type="checkbox"/> Policy <input type="checkbox"/> Procedure <input type="checkbox"/> Policy and Procedure
	Subject: Member Device Management Policy Applies to: All MPSCS Members and MPSCS connected devices.		
	Number: X.X.X	Page: 1 of 1	

X.X.X MPSCS Member Device Management Policy

I. Subject and Purpose

To manage the security of the Michigan's Public Safety Communications System connected devices in a secure and consistent manner across all member agencies. This policy must be adhered to whenever a device is transferred to another entity, sold, recycled, donated, lost, stolen, destroyed or otherwise removed from service on the MPSCS.

II. Policy

Before transferring ownership of a MPSCS connected radio, pager or dispatch console, members must notify the MPSCS of the action via the Device Enable/Disable form and clear their devices of all programming and data in compliance with CJIS Security Policy. This allows the MPSCS to disable the device and be aware that the device is no longer owned by that member. While it is not the MPSCS's responsibility to track member devices, it is important to mitigate risk to the system by identifying accessible assets. In addition, it protects the member's programming and data, and prevents the new owner of the asset to access that programming and data. These steps should be taken any time an MPSCS connected device is transferred, donated, sold, recycled, lost, stolen, destroyed or otherwise removed from service on the MPSCS.

Refer to CJIS Security Policy regarding Media Protection, Sanitization and Disposal for further guidance.

MPSCS provided CAD solutions are required to follow CJIS Security Policy per the MPSCS integration agreement.

III. Definitions

IV. Other Applicable Documents



MPSCS Disable/Enable Request Form

V. Contacts

NCC Manager
Josh Draskowski
xxx@Michigan.gov
517-284-XXXX

VI. Termination or Review Responsibility

The MPSCS Director is responsible for the review and update of this policy. All areas impacted by this policy have 6 months to be in compliance following any changes.

	MICHIGAN'S PUBLIC SAFETY COMMUNICATIONS SYSTEM		
Effective Date: TBD Revised Date: Reviewed Date:	Program Name: Subject: Member Encryption Management Policy Applies to: All MPSCS Members and MPSCS connected devices. Number: TBD		Category: <input type="checkbox"/> Internal <input checked="" type="checkbox"/> External Type: <input checked="" type="checkbox"/> Policy <input type="checkbox"/> Procedure <input type="checkbox"/> Policy and Procedure
	Page: 1 of 1		

MPSCS Member Encryption Management Policy

I. Subject and Purpose

The Michigan's Public Safety Communications System must approve all integrated plans involving encryption, prior to a member purchasing a solution in order to manage the interoperability of the MPSCS connected devices in a secure and consistent manner across all member agencies. This policy must be adhered to whenever a member purchases or changes encryption types or keys that will be used for talkgroups that could be patched for interoperability or used by another member of the MPSCS.

II. Policy

Before purchasing an encryption solution on any MPSCS connected radio, pager and/or dispatch console, members must notify and obtain the MPSCS Director's signature approval through the MPSCS Radio Programming Unit. The documentation must include the member's encryption strategy, implementation plan, impact to interoperability and communications approach to public safety partners. This allows the MPSCS to ensure the impact of implementing encryption by each member, has the appropriate level of awareness to all other impacted members. While it is not the position of the MPSCS to mandate public safety communications encryption practices, it is the position of the MPSCS to preserve interoperability across emergency response in Michigan. These steps should be taken any time an MPSCS member is changing encryption on any talkgroups.

The standard base encryption for the MPSCS shall be P25 compliant. The Michigan Public Safety Communications Interoperability Board (MPSCIB) will review all changes to recommended guidelines.

Refer to the [Encryption Recommendations and Best Practices guidance document](#) as approved by the MPSCIB.

III. Other Applicable Documents

Encryption Recommendations and Best Practices

IV. Contacts

RPU Manager

V. Termination or Review Responsibility

The MPSCS Director is responsible for the review and update of this policy with secondary review by the Michigan Public Safety Communications Interoperability Board as needed.

