SOP 12

Use of Third-Party Communications Interconnection Technologies with Maryland FiRST

1 Purpose

To establish the process for user agencies to request and gain approval for the use of third-party communications interconnection technologies connecting to the Maryland FiRST statewide radio public safety network. Additionally, to assure that any proposed third-party communications interconnection technologies are evaluated to ensure they are secure, controlled, reliable, and adequately protect the quality and integrity of the Maryland FiRST system for all users.

2 Scope

This policy applies to all primary, limited-primary, and interoperability users of the Maryland FiRST statewide public safety communications system desiring to employ or employing third party communications interconnection technologies.

3 Authority

The Statewide Interoperability Radio Control Board ("Board") has the authority to establish Standard Operating Procedures, Quality of Service Standards and Maintenance Guidelines for the Maryland FiRST Radio System in accordance with the Annotated Code of Maryland, Public Safety Article, § 1-501-1-503.

4 Policy Statement

No third-party communications interconnection technology equipment or systems, with the exception outlined in paragraph 5B, may be connected to, or otherwise configured to operate with the Maryland FiRST public safety radio system until approved by the Radio Control Board per the process outlined in this Standard Operating Policy.

5 Supporting Rules

A. The use of third-party communications interconnection technology systems may not have a disproportionate impact to the capacity of the Maryland FiRST system.

B. The Director of the Radio Control Board may authorize the limited/temporary testing or piloting of third-party communications interconnection technology systems, provided the Radio Control Board is informed at the next meeting. In the event of an emergency, the Director of the Radio Control Board may authorize the temporary operation of interconnecting technology. The Radio Control Board will be informed at the next meeting of any permitted temporary emergency operation. Without approval by the Radio Control Board to continue, the interconnection technology must be disabled following the emergency event.

C. All permitted communications through third party interconnection technologies to Maryland FiRST licensed frequencies shall be for the sole or principal purpose of protecting the safety of life, health, or property.[1]

D. All use of Maryland FiRST radio frequency ("RF") resources through third party communications interconnection technologies shall only be made by those meeting the eligibility requirements established by the Federal Communications Commission ("FCC").[2]

E. Any approved third-party communications interconnection technology systems shall include as essential features, a robust security system designed to prevent unauthorized access as well as the ability of Maryland FiRST staff to disable access to an individual user or users promptly through a methodology approved by the Director of the Radio Control Board.

F. Any funding required for the purchase of hardware or software and for the installation/setup of the interconnection technology, and any cost associated with the operation and maintenance of the interconnection technology, including any subscription costs shall be borne by the agency/agencies using the interconnection technology.

G. Maryland FiRST shall not be responsible for future configuration, operational updates, or any other changes that affect the Third-Party communications technology. The user agency requesting the third-party interconnection device

[1] *See* 47 USC §337(f)(1)(a)
[2] *See* 47 CFR §90.523

will hold Maryland FiRST harmless for system maintenance, configuration changes, version upgrades, or other system enhancements which may render the user's interconnection technology obsolete or otherwise impede its continued use.

6 Procedures and Technical Issues

An agency or agencies desiring to use a third-party communications interconnection technology shall submit a proposal to the Director of the Radio Control Board to start the review and evaluation process. The proposal shall consist of a comprehensive Interconnection Plan ("Plan"). This Plan[3], in part, will describe how the proposed technology will provide for robust security and the management of access by authorized users. The Plan will include, but may not be limited to the following:

A. Statement of compliance indicating that all transmissions from the proposed technology will operate appropriately with Maryland FiRST which uses the nationwide P-25 suite of standards as applicable and incorporated by the United States Department of Homeland Security[4] as its fundamental operating architecture.

B. Describe with specificity in the Plan how the proposed system will be connected to the Maryland FiRST system as well as the capabilities of the proposed interconnection system to provide redundancy before connecting to Maryland FiRST. Documentation should include physical locations and contact information for where the interconnection devices will be located, as well as considerations required for isolating offending devices during emergency situations.

C. The Plan should discuss the technology adoption and the anticipated and potential capacity impacts to Maryland FiRST. To the extent practical, the Plan should identify talkgroups to be used, interoperability impacts, and geographical areas where the technology would most often be used. *Donor radios should only be programmed with the user-agency's talkgroups to avoid potential of inadvertent impact to allied agencies.*

[3] Plans are specific to an agency's requirements and a specific device technology. If a technology has been previously reviewed and approved by the Radio Control Board, a subsequent agency request to also utilize the technology may reference an existing approved Plan and identify only proposed changes, if any.

[4] *See* https://www.dhs.gov/publication/p25

D. If providing interconnection with a Maryland FiRST encrypted talkgroup, the technology providing intersystem connection, or the user shall not decrypt the talkgroup. Encrypted talkgroups shall remain secure on Maryland FiRST and the connected system.

E. Interconnection documentation provided in the Plan shall identify how a user will know if a communications failure occurs before the intended communications reach Maryland FiRST. The objective of this requirement is to prevent confusion in the identification of technical failures occurring outside of the control of Maryland FiRST.

F. The Plan shall describe in specificity the security systems included in the proposed third-party communications interconnection technology at the system level. How does the manufacturer of the proposed system prevent hacking and other forms of unauthorized access?

G. At the device level, the Plan shall describe the security protocols employed. Reference should be made to the State of Maryland's "Mobile Device Management Policy."[5] Each Plan should address how systems will comply with applicable parts of this policy.

H. The Plan shall also describe in detail how the staff of the Maryland FiRST system can access and interrogate the proposed third-party communications interconnection technology to disable discrete or individual users. The Plan should focus on the critical issues of Maryland FiRST staff access, timeliness of access, and method(s) of access. The expectation is that a member of the Maryland FiRST staff can access the proposed system through a remote access device, e.g., personal computer or telecommunications device such as a tablet or smartphone and have the ability to monitor the technology's activity with Maryland FiRST and disable individual users as needed to preserve capacity of the system or maintain compliance with Federal laws and the rules of the FCC.

The submitted plan will be reviewed for completeness (did it meet the checklist requirements?) by the Maryland FiRST staff. Should there be an issue with the plan, it will be returned to the submitting agency/agencies to address the issue(s). When the plan meets the checklist requirements, it will be forwarded to DoIT's Office of Security Management (OSM) for a recommendation from an information security perspective and it will be forwarded to the Radio Control Board System Managers Committee for their advisory review and recommendation. The

[5] *See* https://doit.maryland.gov/policies/Documents/Policies/20-12-Mobile-Device-Management.pdf.

Radio Control Board System Managers Committee will convene a technical review panel composed of knowledgeable representatives from the counties and State agencies to conduct their review and evaluation. Concurrent evaluations will be conducted by the Maryland FiRST staff, DoIT OSM, and System Managers Committee technical review panel. When the evaluations have been completed and recommendations prepared, the Director of the Radio Control Board will add the request to the Radio Control agenda and submit the plan for the Board's review and approval. Should there be a delay in the review process, the Director of the Radio Control Board will inform the Board of the delay.

7 Definitions

Third-party interconnection technology: A product whose purpose is to allow connections to Maryland FiRST RF or network resources; originating outside of the MD FiRST network, or otherwise not originating from a subscriber radio. Examples include but are not limited to: FirstNet's "Mission Critical Push to Talk", Verizon's "Push to Talk Plus", Motorola's "Critical Connect", "Wave", and "Smart Connect", Cisco Instant Connect, Tango-Tango, ESChat, etc. as well as the Inter RF Support System Interface ("ISSI").

Project 25 Inter RF Subsystem Interface (P25 ISSI): The P25 ISSI is a non-proprietary interface that enables RF subsystems (RFSSs) to be connected together into wide area networks so that users on different networks can talk with each other. It allows the user to roam onto a different network(s) while maintaining contact with their dispatcher.

8 Responsibilities

A. Applying Agencies: Agencies desiring to use a third-party communications interconnection technology must follow the process delineated in this SOP. Using agencies will be responsible for all costs related to acquisition, installation, subscription, maintenance, technology upgrades and other expenses. Any device with connection capability to Maryland FiRST that becomes lost, stolen, or otherwise compromised shall be reported to the System's staff as soon as practical for disablement per the Lost or Compromised Radio Policy.[6] This notification must be made at the earliest practical opportunity, not when a replacement device is to be added. The address to be used when making such notification is MDFirstSystem.Manager@maryland.gov.

[6] *See* https://doit.maryland.gov/support/Radio%20Control%20Board%20Minutes/MD%20First%20Lost%20or%20Compromised%20Radio%20SOG%200.02.pdf

B. Maryland FiRST staff: Will review and evaluate submitted plans, ensuring they meet all the requirements of this SOP and make a recommendation.

C. DoIT's Office of Security Management (OSM): Will recommend approval or disapproval of the submitted plan from an information security perspective.

D. Radio Control Board System Managers Committee: Will review and evaluate submitted plans and make an advisory recommendation to the Radio Control Board.

E. The Director of the Radio Control Board: May approve temporary changes or modifications to this policy to ensure the security of the system or to accommodate an emergency condition. Any temporary changes or modifications must be reported at the next Radio Control Board meeting. Any permanent changes to this policy require the approval of the Radio Control Board.

9 Contact Information

The Maryland FiRST Agency Coordinator/Customer Liaison may be contacted at:
md-first.radio@maryland.gov

The Maryland FiRST System Manager may be contacted at:
MDFirstSystem.Manager@maryland.gov

10 Approval

This SOP was reviewed by the Maryland FiRST Radio Control Board System Managers Committee on November 29, 2023, and was approved by the Statewide Interoperability Radio Control Board, by majority vote on December 13, 2023.

Norman Farley

Norman J. Farley
Director of the Board

Katie Savage

Katie Savage
Chairwoman of the Board

Third-party Communications Interconnection Technologies
Checklist – Compliance with SOP Process Steps

Agency/County: _____

Technology: _____

□ Requestor submitted to the Director of the Radio Control Board a comprehensive Interconnection Plan.

_____ _____
Date Initial

□ Plan reviewed and evaluated by the Maryland FiRST staff to assess compliance with the requirements of the SOP followed by applicable recommendation(s).

_____ _____
Date Initial

□ Plan reviewed and recommendation made by DoIT's Office of Security Management.

_____ _____
Date Initial

□ Radio Control Board System Managers Committee convened a technical review panel which reviewed and evaluated the submitted Plan and made an advisory recommendation to the Radio Control Board.

_____ _____
Date Initial

□ Director of the Radio Control Board added the request to the Radio Control agenda and submitted the Plan for the Board's review and approval.

_____ _____
Date Initial

Third-party Communications Interconnection Technologies
Agency Checklist – Essential Elements of the Plan

- □ Explains how the proposed technology does not have a disproportionate impact to system capacity.
- □ Confirms that the system is for the sole or principal purpose of protecting the safety of life, health, or property and users meet the eligibility requirements established of the FCC.
- □ Describes in detail all essential features of a robust security system designed to prevent unauthorized access as well as the ability of Maryland FiRST staff to access and interrogate the technology to disable access to an individual user or users promptly. Explains how the manufacturer of the proposed system prevents hacking and other forms of unauthorized access at both the device and system levels? Also explains how the technology complies with the State of Maryland's "Mobile Devices and Services Statewide Policy."
- □ Describes how the proposed system will be connected to Maryland FiRST system as well as the capabilities of the proposed technology to provide redundancy before connecting to Maryland FiRST.
- □ Identifies all talkgroups to be used, interoperability impacts, and geographical areas where the technology would most often be used. Affirms that inter-agency talkgroup sharing agreements have been properly coordinated, if applicable.
- □ Explains how a user will know if a communications failure occurs before the intended communications reach Maryland FiRST.
- □ Affirms that funding for the purchase of hardware or software and for the installation/setup of the interconnection technology, and any cost associated with the operation and maintenance of the interconnection technology, including any subscription costs, shall be borne by the agency/agencies using the interconnection technology.
- □ Confirms that Maryland FiRST is not responsible for future configuration, operational impacts, or any other changes that affect the Third-Party communications technology.
- □ Affirms that the user agency will hold Maryland FiRST harmless for system maintenance, configuration changes, version upgrades, or other system enhancements which may render the user's interconnection technology obsolete or otherwise impede its continued use.

SOP 12 - Third Party Connection Technologies 12-5-2023 Final

Final Audit Report 2023-12-18

Created:	2023-12-14
By:	maria fisher (maria.fisher2@maryland.gov)
Status:	Signed
Transaction ID:	CBJCHBCAABAAsmQLWJcm6WGiGem60R2i-kKhfDHNBxfS

"SOP 12 - Third Party Connection Technologies 12-5-2023 Final " History

Document created by maria fisher (maria.fisher2@maryland.gov)
2023-12-14 - 8:37:01 PM GMT

Document emailed to Norman Farley (Norman.Farley@maryland.gov) for signature
2023-12-14 - 8:37:48 PM GMT

Email viewed by Norman Farley (Norman.Farley@maryland.gov)
2023-12-14 - 9:01:42 PM GMT

Document e-signed by Norman Farley (Norman.Farley@maryland.gov)
Signature Date: 2023-12-14 - 9:02:10 PM GMT - Time Source: server

Document emailed to Katie Savage -DoIT- (katie.savage@maryland.gov) for signature
2023-12-14 - 9:02:12 PM GMT

Email viewed by Katie Savage -DoIT- (katie.savage@maryland.gov)
2023-12-18 - 2:19:51 PM GMT

Document e-signed by Katie Savage -DoIT- (katie.savage@maryland.gov)
Signature Date: 2023-12-18 - 2:20:07 PM GMT - Time Source: server

Agreement completed.
2023-12-18 - 2:20:07 PM GMT