Project 25 Compliance Assessment Program Advisory Panel (P25 CAP AP)
Open Meeting
March 29, 2017
Meeting Summary

P25 CAP Webpage Updates

The encryption requirements Compliance Assessment Bulletin (CAB) has been updated and posted on DHS's website. The update to the CAB was needed to clarify P25 CAP standard encryption and, more specifically, the Advanced Encryption Standard (AES) 256 standard encryption algorithm. Numerous large events can be cited where there have been issues with encryption. Encryption is becoming more useful and it is becoming necessary post-event. Currently, it is difficult to be interoperable when not everyone has encryption. Secure compatibility between agencies in an emergency needs to be improved, so the requirement for encrypted radios to have AES 256 was clarified. Other encryptions can be added, but you must have AES256 to be compliant.

The 'Approved Equipment' page now provides two lists of radios. There is a fully compliant list and non-compliant list. The compliant list is for subscribers that are offered without any encryption or with optional encryption that includes AES 256. The non-compliant list is for subscribers that are offered with non-standard encryption as a baseline feature. These products can be made compliant if they are provided with optional AES 256 encryption.

P25 Test Lab recognition defines the eight laboratories that have been approved for P25 testing based on the 2010 CABs. The test labs are going through the new accreditation process, which is required for the 2016 CABs. As of this meeting, there are only two labs that have completed the reaccreditation.

Question: Is there is a way to add the non-compliant radios, which have a note on what needs to be done to become compliant, to the compliant list?

Answer: The P25 CAP AP is trying to keep the compliant list as upfront as possible to eliminate confusion to the end user as grant guidance can be difficult to understand, and we do not want to make it any harder for users to interpret. If manufacturers want to be on the compliant list, they need to become fully compliant. The P25 CAP AP is happy to work with the manufacturers to become compliant, and the manufacturers will have to answer the following questions:

- How will you become compliant so users can order radios in the configuration they desire, encryption/non-encryption?
- How will you help address people in the field that have interoperability issues with non-standard encryption?
- What is your timeline to become compliant?

Question: We have multiple air interface protocols in our radios. If we disable all encryption, will that make them P25 CAP compliant?

Answer: If the non-standard encryption was disabled at the factory and not in a manner where the customer can re-enable the non-standard encryption in the field, then the procedure would comply with the CAB criteria for a product without encryption. However, manufacturers are still encouraged to provide a resolution for those agencies that do want encryption that meets the CAB requirements.

Question: If we release a new version of firmware for radios that disables ADP encryption to become compliant, would you consider that acceptable as long as the end user cannot go back in and reactivate the 40-bit encryption?

Answer: The firmware update as described would comply with the CAB criteria for a product without encryption. However, manufacturers are still encouraged to provide firmware updates for those agencies that do want encryption that meets the CAB requirements.

Question: What about the customers that have older versions of firmware and get radios, then downgrade it to the previous version of firmware with the 40-bit encryption, is that radio compliant?

Answer: We understand the limitation, but it is better to have the ability to add standard encryption AES 256. The idea is the more radios that have AES 256 in their radios, the easier it will be when older radios get upgraded.

Question: In order to resolve this issue, most manufactures will have to do a firmware update and in turn update our Suppliers' Declaration of Compliance (SDoC)s and Summary Test Reports (STR)s. What will the turnaround be?

Answer: DHS has been posting a message on the website as soon as we verify new SDoCs/STRs. The message states the equipment is compliant and that the SDOCs/STRs are going through the DHS review process before they can be posted on the web site. DHS has been trying to reduce the amount of testing needed for firmware updates, and we are leaving it up to the manufacturer to be honest and decide if the firmware needs to be retested. When a vendor signs the SDOC, they are saying they have done the required testing.

OIC Updates

Time Division Multiple Access (TDMA) is being added to the CAI test requirement CAB for performance and trunked interoperability. Updated SDoCs and STRs templates will be required.

Inter Sub-system Interface (ISSI)/Console Sub-system Interface (CSSI) test requirement CAB is being updated to include FDMA interoperability test cases and supplementary data test, and TDMA over ISSI/CSSI. Timeline is hopefully going to be around May.

P25 CAP AP is asking industry for any suggestions for ISSI/CSSI testing issues. It cannot be done without the input of users and vendors. One of the challenges is the rule of three. There are not three labs that do ISSI/CSSI testing. OIC welcomes any ideas towards streamlining the testing.

In August 2016, there was a new CAB issued with added tests and reaccreditation of test labs. The deadline for accreditation is August 2017. So far, only two labs have gone through the reaccreditation process. If a manufacturer cannot meet the deadlines for retesting their P25 equipment, the manufacturer will need to contact DHS with a request for extension.

Question: If the manufacture is not able to get lab accreditation or testing completed by the deadline and a waiver is granted, what does that mean?

Answer: The waiver will give you an allotted amount of time to get the testing completed. In the waiver request, the manufacturer will need to specify why the extension is needed and the estimated test completion date.

Question: The labs are starting to get reaccredited and ready to perform testing. When will the current CAI CABs/SDoCs and STRS freeze?

Answer: The 2016 CABs added new tests. The new changes will not require new testing; it is clarifying what is required for encryption test cases. The STRs have notes that were added about encryption and the tests stayed the same. SDoCs added a table asking the manufacturer to categorize the encryption provided on radios.

Question: How often will a new CAB be released?

Answer: When a new CAB is released, manufacturers will have one year to complete testing. New CABs should not be released less than one year from each other. The next CAB released will be for TDMA.

Question: Will the ISSI/CSSI CAB be released after the TDMA CAB is complete?

Answer: We are still working on the testing for CSSI/ISSI. If we do not give you the tools for testing, then we cannot release the CABs.

P25 CAP AP Priorities:

The TDMA CAB update will come out first, with CSSI testing being more important than ISSI testing. The P25 test labs need to be accredited for these tests as soon as possible.

There is interest in better understanding whether the proper amount of conformance testing could relieve the 'rule of three' interoperability testing requirement. It is understood that the rule of three testing presents testing challenges.

Grant guidance from SAFECOM is important as it defines what is required when using grant funding for P25 CAP compliant radios. End users need guidance on what is required, and the P25 CAP AP is trying to help with outreach in forms of 100 second videos, white papers and simplifying grant language.

Two customer issues were brought to the P25 CAP AP

Single key, multi-key SU secure interoperability: The original question relates to single key and multi-key radios sharing the same key material on a common talk group. This issue was brought up during the Orlando P25/Telecommunications Industry Association (TIA) meetings. Members of the AP have stated that interoperable keys can be loaded into a single key radio as well as a multi-key radio when using a Key Variable Loader (KVL). The only time you run into an issue is when the keys are loaded into some multi-key radios using Over the Air Rekeying (OTAR). Then there is a possibility the multi-key radio will not be able to communicate with the single key radio in the encrypted mode.

The AP will send a request to the Compliance Assessment Processes and Procedures Task Group (CAPPTG) to get clarification for the secure interoperability expectations between single key and multi-key radios when keys are loaded with a Key Fill Device (KFD)/KVL for both the single key and multi-key radio, and for an explanation on secure interoperability expectations when keys are loaded with a KVL/KFD for the single key radio and loading via OTAR for the multi-key radio.

Spotsylvania, VA: This county recently updated to a P25 trunked system and wants to securely interoperate with other P25 systems and radios in the DC area. Even though Spotsylvania has been authorized to receive key material from the National Law Enforcement Communications Center (NLECC), Spotsylvania has not been able to load NLECC-generated interoperability keys into the Spotsylvania KMF. Spotsylvania has a particular vendor's KMF and NLECC has another vendor's KMF. Systems that have the NLECC vendor KMF have been able to download keys for the NLECC KMF. However, the Spotsylvania vendor's KMF customers have not been able to download keys as the downloaded procedures supported by the NLECC KMF are not supported by the P25/TIA standards, nor by the Spotsylvania vendor.

Question: Why did Spotsylvania go to P25 CAP AP?

Answer: They went to their manufacturer, but the resolution required a response from another manufacturer. P25 CAP AP has always made their email address available for any P25 user that has problems or issues with a P25 system. The P25 Steering Committee, the CAPPTG and the TIA-TR8 have

not advertised any email address where P25 users can express an issue or input a problem they are experiencing.

A TIA TR-8 representative volunteered to help with both of these problems. Further, a P25 Steering Committee representative felt this is a process issue and not a standards issue, so should be addressed through CAPPTG. The P25 Steering Committee representative said he would investigate the issue as the current chair of CAPPTG.