Public Comment Feedback Matrix for Non-Standard Encryption CAB
February 28, 2017

#	Received Comment	P25 CAP/OIC Response
1	DES should be considered the Project 25 Compliance Assessment Program (P25 CAP) compliant encryption.	AES 256 is the only recognized encryption standard for P25 CAP testing.
2	AES will cause a price increase. AES is an option, how can you force a grantee to purchase AES?	The P25 CAP/Office for Interoperability and Compatibility (OIC) does not require P25 CAP compliant equipment to include AES 256 encryption. Any equipment on DHS's website that can be acquired without any installed voice privacy or encryption algorithms (i.e., clear voice) are also considered P25 CAP compliant.
3	Needs to see finalized Common Area Interface (CAI) requirement test CABs and P25 CAP Suppliers' Declaration of Compliance (SDoC)/Summary Test Report (STR) template documents.	The updated P25-CAB-CAI_TEST-REQ document and updated SDoC/STR templates are works in progress. Please do continue to visit the website for program updates.
4	Compliance Assessment Bulletin (CAB) should not be referring to 'shipments.'	The updated CAB language will not refer to 'shipments.' (The intent was to define how the users can acquire these radios.)
5	Update Telecommunications Industry Association (TIA) reference document to latest version.	References to the latest TIA documents will be included in the updates.
6	Has public safety considered asking the Federal Communications Commission (FCC) to specify AES 256 for the other FCC public safety interoperability channels?	DHS OIC has not considered asking the FCC to specify the P25 encryption standard to bands other than 700MHz. The P25 CAP requires the P25 standard encryption (AES 256) be used for the CAP encryption test cases. The AES 256 requirement extends to equipment in all the public safety frequency bands. If the FCC allows the use of P25 digital encryption in the future on the non-700MHz mutual aid channels, P25 CAP compliant equipment will be able to support that capability.
7	Is P25 CAP compliant equipment required when non-federal funds are used to acquire the equipment?	If the funds are not federal grant funds and the RFP does not specify P25 CAP compliant equipment, any equipment can be acquired. However, DHS OIC recommends and promotes through outreach that all users (federal, state and local) use P25 CAP as a criteria for acquisition (including meeting requirements within the Non-Standard Encryption CAB).
8	Estimated completion times.	DHS OIC considers this a priority task and is targeting a 30-day timeframe.
9	How will AES be provided to fielded equipment?	The P25 CAP/OIC is not stipulating how the AES will be provided. This is an action for users and manufacturers to agree upon. DHS OIC is requiring that manufacturers provide users with the means to obtain AES for radios that do not have it. (DHS OIC is also seeking that vendors document how a user can request and receive AES for fielded P25 equipment.)
10	My organization requires AES when encryption is requested.	It is reassuring to hear about organizations requiring AES as the encryption option when encryption is requested. OIC would make note that reviewing the capabilities of the equipment to be acquired **when encryption is not requested** is just as important. Many P25 subscribers are provided with non-P25 standard encryption, at no cost, when AES encryption is not ordered. This effort is to stop the proliferation of P25 equipment with non-standard features when a standard equivalent feature is available.

#	Received Comment	P25 CAP/OIC Response
11	Develop white paper pros and cons for non-standard encryption.	The Land Mobile Radio (LMR) encryption topic is addressed by many articles. SAFECOM and NCSWIC have published a paper *"Guidelines for Encryption in Land Mobile Radio Systems"* that discusses many of the issues related to LMR encryption.
12	Should AES encryption be required for all P25 CAP approved equipment?	P25 CAP/OIC will not be requiring AES 256 encryption for all equipment that is posted on the DHS Approved Equipment list. Clear voice equipment with no encryption capability is also allowed to be posted. Requiring the standards based equivalent for all equipment may increase the price point of devices for users that just want P25 CAP compliant equipment without encryption.