ATTACHMENT 6: Encryption Verification Standard Mapping List

06-Jan-25

Version: 0.1

System Test Platform to be a System

As NEW DESIGN CHANGE REQUEST,

TO DISCUSS!!

This Attachment is for new design change discussion, out of Scope

This Attachment takes reference to:

1. NCSIST SC12060P-CS移動臺等10項 工作說明書 (hereafter refers as SOW).
2. SOW Attachment 7 Encryption Verification Qualification Standard Table密式驗證合格標準表.

The purpose of this attachment is to provide the mapping table between

1) Attachments in this documents, and

2) SOW Attachment 7 Encryption Verification Qualification Standard Table密式驗證合格標準表.

| **一、密式驗證合格標準表** | | **項目 ：密式置換** | | | |
| --- | --- | --- | --- | --- | --- |
| 編號 | SOW 檢測項目 | | SOW Description | Mapping to this document |
| 1 | 於網管中心、派遣臺等兩種次系統之密碼模組，須與移動臺加密互通。 | | The crypto modules of Network Management Center and Dispatch Console must interoperate with Mobile radio over encryption communiaction. | Attachment 3, Test Case  2.2 Radio Feature  2.3 VPM (Console) Feature  2.5 Key Management Facility (KMF) |
| 2 | 「保密裝備」內含標準AES演算法，具備密鑰長度至少256位元(含)以上供置換之研改範本(可正常運作之範本) 。 | | Crypto module contains the standard AES algorithm and has a key length of at least 256 bits (inclusive) for replacing with CFX modification template. | Attachment 3, Test Case  2.2 Radio Feature  2.3 VPM (Console) Feature |
| 3 | 標準型AES演算法中Sbox、Mixcolumns兩個元件須能被置換， 廠商須提供一組Sbox、Mixcolumns作為參數，供執行研改。 | | The two components Sbox and Mixcolumns in the standard AES algorithm must be replaceable. The manufacturer must provide a set of Sbox and Mixcolumns as parameters for implementation research and modification. | Attachment 2, Section 3.4 Configurable Parameters Modification. |
| 4 | 廠商提供本案「密碼模組」AES演算法之相關Source Code及弱點掃描報告(經源碼弱掃須無高、中風險項目)。 | | The manufacturer to provide the relevant source code (Source Code) and vulnerability scanning report of the AES algorithm of crypto module. The result of source code vulnerability scanning must be that there are no high or medium risk items. | Motorola will separately provide report from independent laboratory subjected to the laboratory approval as part of the verifications. |
| 5 | 廠商提供「密式置換相關附屬軟硬體及工具」供本院執行密式置換，並可將研改後之「AES演算法參數/燒錄檔」，燒錄至網管中心、派遣臺及移動臺之「密碼模組」。 | | The manufacturer provides "accessory software, hardware and tools related to encryption replacement" for NCSIST to perform encryption replacement, and can burn the modified "AES algorithm parameters/burning file" to the crypto module of Network Management Center, Dispatch Console and Mobile Radios. | Attachment 2, Section 5 Programming the Configurable Parameters into the Target Devices.  Attachment 4, List of Equipment for System Test Platform and Accessories. |
| 6 | 廠商提供「密式置換相關附屬軟硬體及工具」供本院執行密式置換，須由本院「自主」掌控且可以「無限制次數」密式置換及燒錄。 | | The "key replacement related ancillary software, hardware and tools" provided by the manufacturer must be "independently" controlled by our institute and can be used for "unlimited times" of key replacement and burning. | Attachment 2, Section 3.4 Configurable Parameters Modification. |
| 7 | 廠商提供「系統測試平臺」供本案網管中心、派遣臺及移動臺「密碼模組」密式置換測試，於系統採用原標準AES演算法下，系統成功進行「加/解密」通聯驗證。 | | The "system test platform" is capable of performing mutual AES encryption/decryption tests on Mobile Radios, Dispatch Consoles and Network Management Center for full-system connectivity encryption verification. | Attachment 3, Test Case  2.2 Radio Feature 2.3 VPM (Console) Feature |
| 8 | 廠商提供「系統測試平臺」供本案網管中心、派遣臺及移動臺「密碼模組」密式置換測試，於系統採用密式置換(參數置換)後之AES演算法下，系統成功進行「加/解密」通聯驗證。 | | The "system test platform" is capable of performing mutual CFX encryption/decryption tests on Mobile Radios, Dispatch Consoles and Network Management Center for full-system connectivity encryption verification. | Attachment 3, Test Case  2.2 Radio Feature 2.3 VPM (Console) Feature |
| 9 | 廠商提供「保密裝備安全鑑測驗證技術說明文件」，須提供以繁體中文製作，符合本院審查要求，並以紙本裝訂成冊3份及光碟電子檔(可供編輯OFFICE WORD檔) 2份。 | | When delivering document " Encrypted Equipment Security Test Validation - Description" in this case, the manufacturer must provide it in Traditional Chinese. The document must provide an OFFICE WORD file, and please bind it in 3 copies on paper and an electronic file on a CD (available for editing) )2 servings. | This is the way of document delivery, not to be discussed in this document. |