U.S. Department of Homeland Security

Prepared for State of North Carolina

CISA/ICTAP

Cybersecurity and Infrastructure Security Agency / Interoperable Communications Technical Assistance Program

CISA/ICTAP-NC-ENG-ENCRYPT
WO19-148

North Carolina SOG Report
2020

State of North Carolina Interoperable Radio Encryption Standard Operating Guideline (SOG)

Signature Page

Approved by:

Jamie Barrier, Battalion Chief – Mooresville Fire Rescue Date
SIEC Chair

Charles Laird, Program Specialist – NC DIT/FirstTech Date
SIEC Vice-Chair

Matt McMahon, Communications Specialist – Vidant Health Date
SIEC Encryption Working Group Chair

Michael Hodgson, Network Manager – NCSHP/TSU Date

Greg Hauser, Statewide Interop Coordinator – NCEM Date

Record of Changes

Change No.	Date	Description	Signature
001	5/28/20	Document approved by SIEC	G. Hauser
002	6/3/20	Document signed (DocuSign)	G. Hauser
003	6/8/20	Addition of SHP technical lead	G. Hauser
004	2/15/21	Edited NCSHP Email suffixes	G. Hauser

This Standard Operating Guideline (SOG) is subject to information updates and changes. The use of this Record of Change helps manage SOG modifications throughout the life of this document. All attempts have been made to ensure the accuracy of the information within this SOG.

Table of Contents

List of Tables

List of Figures

INTRODUCTION

This document is intended to provide guidance for public safety entities considering encryption in North Carolina. This document does NOT require the use of encryption by any agency, but rather it sets forth a process to follow if an agency chooses to implement encryption. As the public safety user community continues to implement digital technology to support mission-critical voice communications, they have recognized an increasing need to protect sensitive information transmitted over the air and within the network. The North Carolina Voice Interoperability Plan for First Responders (VIPER) system recognizes the need for interoperable, and secure communications. Successful interoperable encryption can be as simple as ensuring common keys are loaded on the national 700MHz conventional tactical channels. Agencies considering encryption should carefully weigh the increased security of the communication against the impacts on personnel and interoperability. This document outlines common interoperability encryptions keys used in the State of North Carolina. The document does not address individual agency generated encryption keys with the exception of a recommendation that agencies take steps to avoid conflicts with Common Key Reference (SLN), generically known as Storage Location Numbers (SLN). Radio encryption can be divided into two areas: internal agency encryption and interoperable encryption. This plan is meant to work in conjunction with the existing policies and Guidelines for local radio systems along with VIPER.

Encryption Algorithms

VIPER is built on the Project 25 (P25) standard; therefore, this policy recommends the use of P25 encryption, standards-based security solution using NIST FIPS 140-2/197 compliant Advanced Encryption Standard (AES) 256bit to ensure the highest level of secure communication and interoperable communications. AES, Data Encryption Standard (DES) and Motorola Advanced Digital Privacy (ADP) are the most common algorithms used today. Agencies are encouraged to load the State of North Carolina and National interoperability keys in addition to their private key requirements. While other encryption types are used daily, it is recommended that all future equipment features work toward the AES256 algorithm. Agencies that continue use of RC4/ADP, AES128 ~~o~~r DES algorithms should consider a plan on transitioning to AES256 in the future. National Interoperability keys continue to operate with both AES256 and DES algorithms.

It is important to note that AES256 is the only algorithm that is recognized by the Department of Homeland Security's P25 Compliance Assessment Program (P25 CAP), which sets the requirements for grant eligible equipment. This means that to be compliant with P25 CAP requirements means radios must:

1. Have no encryption;
2. Have AES 256 (for U.S. agencies only); or
3. Have AES 256 along with any other non-standard encryption algorithms.

Additional information can be found at https://www.dhs.gov/science-and-technology/approved-grant-eligible-equipment

Encryption Challenges

Failure to coordinate encryption parameters such as SLN and Key IDs (KID) can hamper operability and interoperability and may even result in loss of communications.

Migration to AES256 Algorithm

Public safety agencies who choose to implement encryption should implement AES256 encryption to ensure multivendor compatibility and information security. Deployments of older or proprietary encryption types/algorithms should be avoided if possible. Agencies receiving grant funds must ensure compliance with relevant grant requirements. Agencies purchasing radios capable of encryption are strongly encouraged to procure radios with support for multiple encryption keys (sometimes known as “multikey”).

Encryption Key Assignment and Distribution

Once an agency has decided to implement P25 digital encryption, consideration needs to be given to prevent encryption key conflicts. If an agency desires internal encryption only, the SLN assignment can be handled by the Viper Point of Contact (POC) for the County/Discipline. It will be the responsibility of the Viper POC to maintain a list of the current SLN agency assignment in their respected county/discipline. Each SLN will be assigned to an agency for their encryption use. Each County is allocated (20) unique SLNs for agencies wishing to implement their private encryption. If the Viper POC exhausts all (20) SLNs assigned, please contact the VIPER TSU for further direction. Agencies wishing to load NC or National interoperable keys will be required to contact VIPER for SLN and Key loading instructions.

The administrative (general encryption inquiries, local POC questions) contact for North Carolina will be:

Joseph Allison
North Carolina State Highway Patrol
Technical Services Unit
Joseph.allison@ncshp.org

The technical (encryption key assignments, equipment capabilities, key loading inquiries) contact for North Carolina will be:

David T. Sizemore
North Carolina State Highway Patrol
Technical Services Unit
Tucker.sizemore@ncshp.org

VIPER, in coordination with the NLECC (National Law Enforcement Communications Center) and VIPER Points of Contact (POC), will maintain a database of statewide and national assigned SLN/KIDs in an effort to prevent overlap among public safety agencies. Requesting access to NC County SLN/KIDs should go through their assigned VIPER POC. Member Agencies using statewide or national keys must submit the encryption key request, Non-disclosure form and programming security agreement to the VIPER TSU for review and assignment. Agencies that are already utilizing encryption should also contact VIPER to determine if their existing SLN/KID is unassigned. If there is already a conflict, the agency should evaluate a change at the next reasonable opportunity.

It must be noted that this process only applies to the SLN and KID. The Traffic Encryption Key (TEK), is left entirely to the agency to create with the exception of VIPER and NLECC issued Keys. The TEK is the actual encryption string, or the unique values that secure the communication. Only the agency will know those parameters and have access to the secured communication, unless they chose to share their encryption key(s). No part of this guideline's process reveals your secured communications or TEK to NLECC or VIPER.

The default crypto period is static; in other words, the interoperable encryption key is not subject to scheduled periodic reprogramming (barring any exigent circumstances) VIPER TSU administration will notify and provide guidance if they find or are made aware that interoperable encryption keys are compromised and re-keying is required.

Table 1 – North Carolina County SLN Assignments

Entity / County	FED FIPS	Local FIPS	SLN Begin R1$_{10}$	SLN End R1$_{10}$	SLN Begin R2	SLN End R2	KID Begin R1	KID End R1	KID Begin R2	KID End R2
Federal I/O			0001	0020						
Alamance	37001	1	0021	0029			$0020	$002F	$A020	$A02F
Alexander	37003	3	0030	0039	0040	0049	$0030	$004F	$A030	$A04F
Alleghany	37005	5	0050	0059	0060	0069	$0050	$006F	$A050	$A06F
Anson	37007	7	0070	0079	0080	0089	$0070	$008F	$A070	$A08F
Ashe	37009	9	0090	0099	0100	0109	$0090	$00AF	$A090	$A0AF
Avery	37011	11	0110	0119	0120	0129	$0110	$012F	$A110	$A12F
Beaufort	37013	13	0130	0139	0140	0149	$0130	$014F	$A130	$A14F
Bertie	37015	15	0150	0159	0160	0169	$0150	$016F	$A150	$A16F
Bladen	37017	17	0170	0179	0180	0189	$0170	$018F	$A170	$A18F
Brunswick	37019	19	0190	0199	0200	0209	$0190	$01AF	$A190	$A1AF
Buncombe	37021	21	0210	0219	0220	0229	$0210	$022F	$A210	$A22F
Burke	37023	23	0230	0239	0240	0249	$0230	$024F	$A230	$A24F
Cabarrus	37025	25	0250	0259	0260	0269	$0250	$026F	$A250	$A26F
Caldwell	37027	27	0270	0279	0280	0289	$0270	$028F	$A270	$A28F
Camden	37029	29	0290	0299	0300	0309	$0290	$02AF	$A290	$A2AF
Carteret	37031	31	0310	0319	0320	0329	$0310	$032F	$A310	$A32F
Caswell	37033	33	0330	0339	0340	0349	$0330	$034F	$A330	$A34F
Catawba	37035	35	0350	0359	0360	0369	$0350	$036F	$A350	$A36F
Chatham	37037	37	0370	0379	0380	0389	$0370	$038F	$A370	$A38F
Cherokee	37039	39	0390	0399	0400	0409	$0390	$03AF	$A390	$A3AF
Chowan	37041	41	0410	0419	0420	0429	$0410	$042F	$A410	$A42F
Clay	37043	43	0430	0439	0440	0449	$0430	$044F	$A430	$A44F
Cleveland	37045	45	0450	0459	0460	0469	$0450	$046F	$A450	$A46F
Columbus	37047	47	0470	0479	0480	0489	$0470	$048F	$A470	$A48F

Entity / County	FED FIPS	Local FIPS	SLN Begin R1$_{10}$	SLN End R1$_{10}$	SLN Begin R2	SLN End R2	KID Begin R1	KID End R1	KID Begin R2	KID End R2
Craven	37049	49	0490	0499	0500	0509	$0490	$04AF	$A490	$A4AF
Cumberland	37051	51	0510	0519	0520	0529	$0510	$052F	$A510	$A52F
Currituck	37053	53	0530	0539	0540	0549	$0530	$054F	$A530	$A54F
Dare	37055	55	0550	0559	0560	0569	$0550	$056F	$A550	$A56F
Davidson	37057	57	0570	0579	0580	0589	$0570	$058F	$A570	$A58F
Davie	37059	59	0590	0599	0600	0609	$0590	$05AF	$A590	$A5AF
Duplin	37061	61	0610	0619	0620	0629	$0610	$062F	$A610	$A62F
Durham	37063	63	0630	0639	0640	0649	$0630	$064F	$A630	$A64F
Edgecombe	37065	65	0650	0659	0660	0669	$0650	$066F	$A650	$A66F
Forsyth	37067	67	0670	0679	0680	0689	$0670	$068F	$A670	$A68F
Franklin	37069	69	0690	0699	0700	0709	$0690	$06AF	$A690	$A6AF
Gaston	37071	71	0710	0719	0720	0729	$0710	$072F	$A710	$A72F
Gates	37073	73	0730	0739	0740	0749	$0730	$074F	$A730	$A74F
Graham	37075	75	0750	0759	0760	0769	$0750	$076F	$A750	$A76F
Granville	37077	77	0770	0779	0780	0789	$0770	$078F	$A770	$A78F
Greene	37079	79	0790	0799	0800	0809	$0790	$07AF	$A790	$A7AF
Guilford	37081	81	0810	0819	0820	0829	$0810	$082F	$A810	$A82F
Halifax	37083	83	0830	0839	0840	0849	$0830	$084F	$A830	$A84F
Harnett	37085	85	0850	0859	0860	0869	$0850	$086F	$A850	$A86F
Haywood	37087	87	0870	0879	0880	0889	$0870	$088F	$A870	$A88F
Henderson	37089	89	0890	0899	0900	0909	$0890	$08AF	$A890	$A8AF
Hertford	37091	91	0910	0919	0920	0929	$0919	$092F	$A919	$A938
Hoke	37093	93	0930	0939	0940	0949	$0930	$094F	$A930	$A94F
Hyde	37095	95	0950	0959	0960	0969	$0950	$096F	$A950	$A96F
Iredell	37097	97	0970	0979	0980	0989	$0970	$098F	$A970	$A98F
Jackson	37099	99	0990	0999	1000	1009	$0990	$09AF	$A990	$A9AF
Johnston	37101	101	1010	1019	1020	1029	$1010	$102F	$B010	$B02F
Jones	37103	103	1030	1039	1040	1049	$1030	$104F	$B030	$B04F
Lee	37105	105	1050	1059	1060	1069	$1050	$106F	$B050	$B06F
Lenoir	37107	107	1070	1079	1080	1089	$1070	$108F	$B070	$B08F
Lincoln	37109	109	1090	1099	1100	1109	$1090	$10AF	$B090	$B0AF
McDowell	37111	111	1110	1119	1120	1129	$1110	$112F	$B110	$B12F
Macon	37113	113	1130	1139	1140	1149	$1130	$114F	$B130	$B14F
Madison	37115	115	1150	1159	1160	1169	$1150	$116F	$B150	$B16F
Martin	37117	117	1170	1179	1180	1189	$1170	$118F	$B170	$B18F
Mecklenburg	37119	119	1190	1199	1200	1209	$1190	$11AF	$B190	$B1AF
Mitchell	37121	121	1210	1219	1220	1229	$1210	$122F	$B210	$B22F
Montgomery	37123	123	1230	1239	1240	1249	$1230	$124F	$B230	$B24F
Moore	37125	125	1250	1259	1260	1269	$1250	$126F	$B250	$B26F

Entity / County	FED FIPS	Local FIPS	SLN Begin R1[10]	SLN End R1[10]	SLN Begin R2	SLN End R2	KID Begin R1	KID End R1	KID Begin R2	KID End R2
Nash	37127	127	1270	1279	1280	1289	$1270	$128F	$B270	$B28F
New Hanover	37129	129	1290	1299	1300	1309	$1290	$12AF	$B290	$B2AF
Northampton	37131	131	1310	1319	1320	1329	$1310	$132F	$B310	$B32F
Onslow	37133	133	1330	1339	1340	1349	$1330	$134F	$B330	$B34F
Orange	37135	135	1350	1359	1360	1369	$1350	$136F	$B350	$B36F
Pamlico	37137	137	1370	1379	1380	1389	$1370	$138F	$B370	$B38F
Pasquotank	37139	139	1390	1399	1400	1409	$1390	$13AF	$B390	$B3AF
Pender	37141	141	1410	1419	1420	1429	$1410	$142F	$B410	$B42F
Perquimans	37143	143	1430	1439	1440	1449	$1430	$144F	$B430	$B44F
Person	37145	145	1450	1459	1460	1469	$1450	$146F	$B450	$B46F
Pitt	37147	147	1470	1479	1480	1489	$1470	$148F	$B470	$B48F
Polk	37149	149	1490	1499	1500	1509	$1490	$14AF	$B490	$B4AF
Randolph	37151	151	1510	1519	1520	1529	$1510	$152F	$B510	$B52F
Richmond	37153	153	1530	1539	1540	1549	$1530	$154F	$B530	$B54F
Robeson	37155	155	1550	1559	1560	1569	$1550	$156F	$B550	$B56F
Rockingham	37157	157	1570	1579	1580	1589	$1570	$158F	$B570	$B58F
Rowan	37159	159	1590	1599	1600	1609	$1590	$15AF	$B590	$B5AF
Rutherford	37161	161	1610	1619	1620	1629	$1610	$162F	$B610	$B62F
Sampson	37163	163	1630	1639	1640	1649	$1630	$164F	$B630	$B64F
Scotland	37165	165	1650	1659	1660	1669	$1650	$166F	$B650	$B66F
Stanly	37167	167	1670	1679	1680	1689	$1670	$168F	$B670	$B68F
Stokes	37169	169	1690	1699	1700	1709	$1690	$16AF	$B690	$B6AF
Surry	37171	171	1710	1719	1720	1729	$1710	$172F	$B710	$B72F
Swain	37173	173	1730	1739	1740	1749	$1730	$174F	$B730	$B74F
Transylvania	37175	175	1750	1759	1760	1769	$1750	$176F	$B750	$B76F
Tyrrell	37177	177	1770	1779	1780	1789	$1770	$178F	$B770	$B78F
Union	37179	179	1790	1799	1800	1809	$1790	$17AF	$B790	$B7AF
Vance	37181	181	1810	1819	1820	1829	$1810	$182F	$B810	$B82F
Wake	37183	183	1830	1839	1840	1849	$1830	$184F	$B830	$B84F
Warren	37185	185	1850	1859	1860	1869	$1850	$186F	$B850	$B86F
Washington	37187	187	1870	1879	1880	1889	$1870	$188F	$B870	$B88F
Watauga	37189	189	1890	1899	1900	1909	$1890	$18AF	$B890	$B8AF
Wayne	37191	191	1910	1919	1920	1929	$1910	$192F	$B910	$B92F
Wilkes	37193	193	1930	1939	1940	1949	$1930	$194F	$B930	$B94F
Wilson	37195	195	1950	1959	1960	1969	$1950	$196F	$B950	$B96F
Yadkin	37197	197	1970	1979	1980	1989	$1970	$198F	$B970	$B98F
Yancey	37199	199	1990	1999			$1990	$19AF	$B990	$B9AF
State			2000	2999						
Federal			3000	3999						

Table 2 – State of North Carolina Discipline Specific SLN Assignments

SLN/SLN	KID	ALGO	Name	Use	Crypto Period
2990	$2995	AES	NC VIPER PATCH	CONSOLE PATCH KEY	STATIC
2997	$299D	RC4/ADP	NC CSK RC4	PUBLIC SAFETY INTEROPERABLE	STATIC
2998	$299E	AES	NC CSK AES	PUBLIC SAFETY INTEROPERABLE	STATIC
2999	$299F	DES	NC CSK DES	PUBLIC SAFETY INTEROPERABLE	STATIC

***It is recommended that core connected consoles and all subscriber units load the NC patch key in order for patching of two secure talkgroups to occur. This is known as the default SLN. SLN 2997-2999 are the NC Public Safety Interoperability keys in all (3) algorithms. Loading of public safety interoperable keys are strongly suggested for all capable subscriber radios utilized in the State of NC.

Table 3 – National interoperability Storage Location Numbers (SLN Keys)

SLN	ALGO	NAME	USE	CYPTO PERIOD
1	DES	ALL IO D	PUBLIC SAFETY INTEROPERABLE	ANNUAL
2	DES	FED IO D	FEDERAL INTEROPERABLE	ANNUAL
3	AES	ALL IO A	PUBLIC SAFETY INTEROPERABLE	ANNUAL
4	AES	FED IO A	FEDERAL INTEROPERABLE	ANNUAL
5	DES	NLE IO A	NATIONAL LAW ENFORCEMENT STATE/LOCAL INTEROP DES	STATIC
6	AES	NLE IO D	NATIONAL LAW ENFORCEMENT STATE/LOCAL INTEROP AES	STATIC
7	AES	FED CAN	US-CANADIAN FED LAW ENFORCEMENT INTEROP	STATIC
8	AES	USCAN PS	US-CANADIAN PS INTEROP	STATIC
9	DES	NTAC D	NATIONAL TACTICAL EVENT	SINGLE-USE (NTE 30 DAYS)
10	AES	NTAC A	NATIONAL TACTICAL EVENT	SINGLE-USE (NTE 30 DAYS)
11	DES	PS IO D	MULTIPLE PUBLIC SAFETY DISCIPLINES	STATIC
12(1)	AES	PS IO A	MULTIPLE PUBLIC SAFETY DISCIPLINES	STATIC
13	DES	NFER D	NATIONAL FIRE/EMS/RESCUE	STATIC
14	AES	NFER A	NATIONAL FIRE/EMS/RESCUE	STATIC
15	DES	FED TF D	NATIONAL TASK FORCE OPERATIONS	ONE-TIME USE
16	AES	FED TF A	NATIONAL TASK FORCE OPERATIONS	ONE-TIME USE
17	DES	NLE TF D	NATIONAL LAW ENFORCEMENT TASK FORCE	ONE-TIME USE
18	AES	NLE TF A	NATIONAL LAW ENFORCEMENT TASK FORCE	ONE-TIME USE
19	AES	FED INTL	FEDERAL-INTERNATIONALLAW ENFORCEMENT INTEROP	WHEN NEEDED BY OPS REQUIREMENT
20	AES	PS INTL	PUBLIC SAFETY-INTERNATIONALLAW ENFORCEMENT INTEROP	WHEN NEEDED BY OPS REQUIREMENT

Agencies requesting new talkgroup(s) on VIPER or encryption key access/assignment(s) will be required to fill out associated user agreements: Non-disclosure form, key transfer and talkgroup(s) questionnaire.

[1] Key is user selectable on NPS 700MHz tactical channels

KMF and OTAR (Over-the-Air Rekeying)

Encryption key management through a KMF (Key Management Facility), along with the Over the Air (OTAR) function is a highly efficient way to manage radio encryption. The State of North Carolina is in the process of commissioning a KMF at the time of the creation of this document. Numerous factors must be evaluated such as management of the KMF, associated OTAR feature sets, radio system infrastructure capabilities, key encryption keys (KEK), Radio Set Identifier (RSI) and subscriber device feature sets. Alternative options such as KMF agency partnering may be explored in the future. Utilization of a KMF along with OTAR can greatly decrease the amount of time required for subscriber device key loading. Additionally, radios can be rekeyed immediately upon discovery of compromised key.

Use	SLN Begin	SLN End	KID Begin	KID End
State DES KEKs	61440	61449	F000	F009
State AES KEKs	61450	61459	F00A	F013

If counties require additional KEK assignments, please contact VIPER TSU

Obtaining and Sharing of Key Variable Loader (KVL) keys

National keys will be obtained by VIPER TSU by “dialing-in” with a Key Fill Device (KFD) to the appropriate NLECC modem and receive a key fill consisting of the current National keys. This process may also be utilized by VIPER TSU techs or shared through a manual distribution process using the central KFD. **At no time will any agency transfer keys from one keyloader to another without authorization from VIPER TSU or the SWIC.** All key fill devices will utilize the audit trail function which may be viewed in the keyloader by VIPER TSU upon demand.

Individual agency keys will be created by the agency with a coordinated SLN and KID created in accordance with the County/Agency SLN/SLN plan established in this document. Additional or special circumstanced or needs can be evaluated and coordinated by VIPER TSU and the SWIC.

Approved Key Fill Devices in North Carolina

The following FIPS140-2 compliant devices are approved for use in North Carolina:

Motorola KVL3000+
Motorola KVL4000
Motorola KVL5000

Key sharing is required to be disabled. FIPS140-2 benchmarks must be met before key fills are transferred. *Additional approved key loaders from other vendors will be added as product evaluation occurs.*

Regional ENC POC-Trusted Agents/SMEs

The VIPER TSU in conjunction with the SWIC will maintain a contact list of trusted agents/SMEs across the state to provide additional technical assistance. Please contact the TSU or SWIC for additional information.

General Requirements and Guidance for End Users

- Public safety agencies who choose to implement encryption are encouraged to implement AES256 type encryption to ensure multi-vendor compatibility and information security. Deployments of older or proprietary encryption types/algorithms should be avoided. Agencies receiving grant funds must ensure compliance with relevant grant requirements (i.e. that AES256 is included in the radio if encryption is purchased using federal funds). Agencies need to very carefully consider the specifications / feature sets of subscriber devices, consoles, and other equipment that require keys to be loaded.

- Agencies purchasing radios capable of encryption are strongly encouraged to procure radios with support for multiple encryption keys (sometimes known as "multikey").

- Encryption is not permitted on VHF, UHF, and 800 MHz national interoperability channels. P25 encryption is allowed on 700 MHz channels with the exception of the calling channels. There are some exceptions to this which are highlighted in FCC rules.

- SLN 1 through 20 (decimal) are reserved for nationwide interoperability, as managed by NLECC. No agency in North Carolina shall utilize SLN 1 through 20 for any other purpose unless multikey is unavailable. Existing non-conforming users should migrate from these nationwide reserved SLNs as soon as practical.

- Agencies that choose to utilize encryption are strongly urged to utilize a radio programming mode where the encryption is fixed on or off per channel, commonly known as "strapped encryption". In certain circumstances, allowing a user to select a key on a particular talkgroup or channel may be operationally necessary. Persons using encryption on national interop 700MHz frequencies must be able to readily disable encryption. In some cases, it may be necessary to have the flexibility to utilize multiple keys on selected channels. In this case the channel should be strapped for encryption but set to allow the user to select the appropriate key. If encryption is being utilized on an approved National interoperable frequency then per Federal Communications Commission rule "…encryption must be able to be readily disabled by the user". This could be through the use of a switch or by loading an encrypted zone and an unencrypted zone with the same frequencies.

- Plain text sharing of RC4/ADP keys is not allowed under any circumstances. Single key RC4/ADP equipment will not be able to participate in the North Carolina Interoperable Encryption Plan. Agencies are strongly encouraged to upgrade to AES 256.

- Agencies loading encryption on National 700MHz interoperability tactical channels should use National SLN12 as the default SLN. Agencies are recommended to have selectable keys in the national range based on availability.

- **If an encrypted radio that contains VIPER or NLECC keys is lost or stolen, the SWIC and VIPER TSU shall be notified within 24 hours of the occurrence. A determination will be made at that time to the security risk and next steps. Physical security of equipment is equally important as the encryption itself. Erase Keys on radio inhibit should strongly be considered on subscribers at high risk of compromise.**

GLOSSARY

ADVANCED ENCRYPTION STANDARD (AES) - Generally recognized as the strongest widely available Land Mobile Radio encryption available to State/local public safety. Project 25 (P25) supports the AES-256-bit encryption type. This is the State recommended format for general use, and is the required format for interoperable encryption.

COMMON KEY REFERENCE (SLN) – See "SLN" / Storage Location Number

CRYPTO PERIOD - The period of time that a Traffic Encryption Key is active.

DATA ENCRYPTION STANDARD (DES) - An encryption standard using a 56-bit key that was previously approved by the Federal government. This standard is no longer certified by the Federal government but is still in widespread use.

Key Encryption Key (KEK) - Encryption key that is used for the encryption or decryption of other keys to provide confidentiality protection. Also known as Key-wrapping key.

KEY FILL DEVICE / KEY VARIABLE LOADER – A device that locally contains encryption keys and is utilized to transfer the encryption keys into subscriber or user devices for their use.

KEY ID (KID) - The unique identifier for the actual over the air encryption key. This is a hex value between 0000 and ffff and is transmitted in the P25 data stream. This is the identifier that the radio utilizes to locate the proper internal key for the transmission.

KEY MANAGEMENT FACILITY (KMF) - A powerful secure computer that serves as an application server and key material storage facility. The KMF can create, store, and manage keys.

NATIONAL LAW ENFORCEMENT COMMUNICATIONS CENTER (NLECC) - US Customs and Border Patrol KMF facility

OVER THE AIR REKEYING (OTAR) - Message either to or from the KMF to provide encryption information to a radio, such as a request for an encryption key, keyset changeover, etc.

PROPRIETARY ENCRYPTION - An encryption algorithm that is not adopted as a standard.

RADIO SET ID (RSI) - A unique identifier for each unit in an OTAR system.

STORAGE LOCATION NUMBER (SLN) - A common method to refer to an encryption key. In an OTAR system, each SLN contains two TEK's (one active/one inactive). This is decimal value between 1 and 4095. The value is used by the subscriber unit to locate the encryption key with memory This is also known as a "SLN." Or Common Key Reference.

STATE LEVEL INTEROPERABILITY KEY - An encryption key provided by North Carolina for the purposes of interoperability.

TRAFFIC ENCRYPTION KEY (TEK) - The unique hexadecimal key used to encrypt and decrypt voice and data traffic. The length and composition of the TEK depends on the algorithm used.

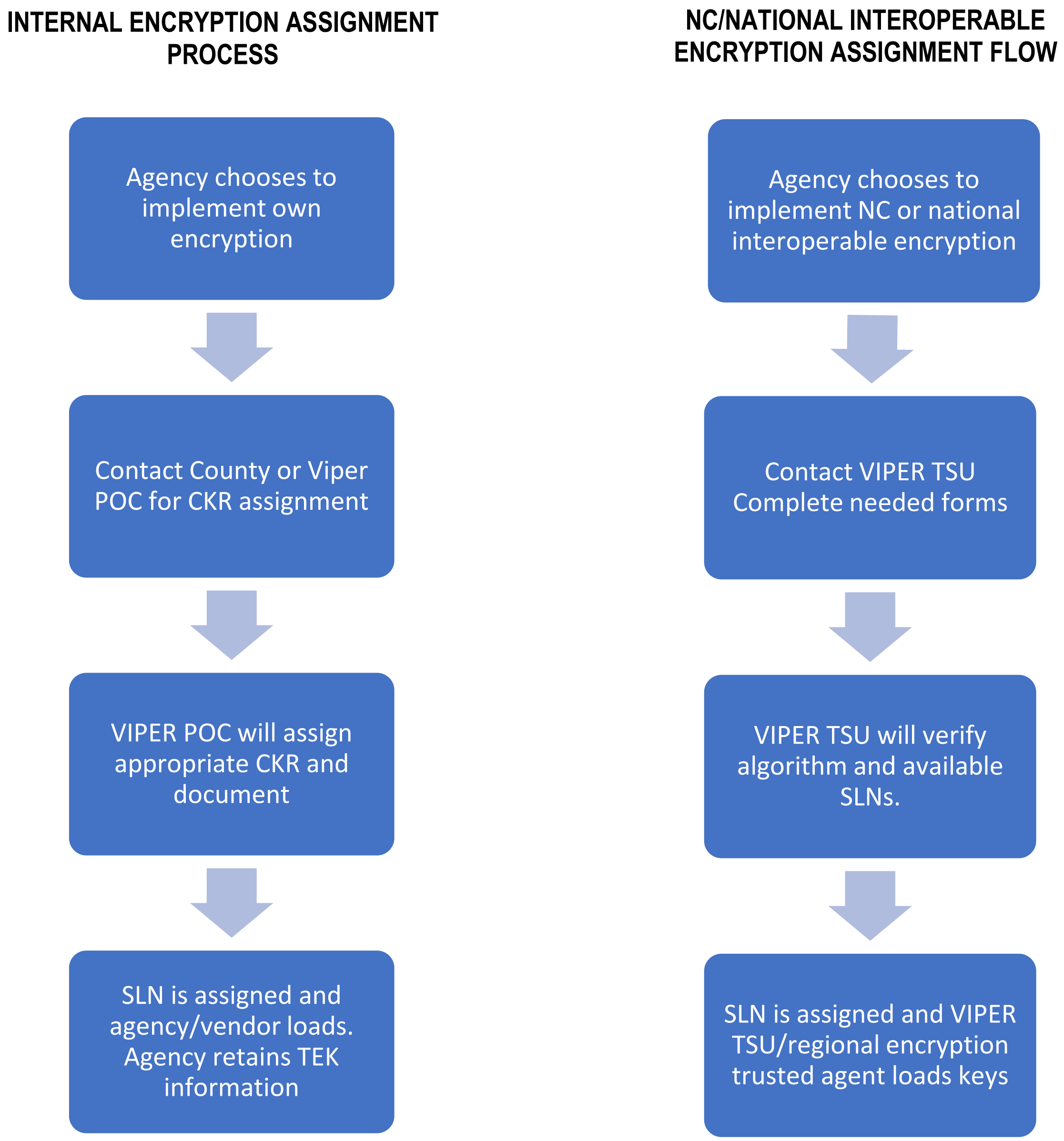
INTERNAL ENCRYPTION ASSIGNMENT PROCESS
Agency chooses to implement own encryption
Contact County or Viper POC for CKR assignment
VIPER POC will assign appropriate CKR and document
SLN is assigned and agency/vendor loads. Agency retains TEK information
NC/NATIONAL INTEROPERABLE ENCRYPTION ASSIGNMENT FLOW
Agency chooses to implement NC or national interoperable encryption
Contact VIPER TSU Complete needed forms
VIPER TSU will verify algorithm and available SLNs.
SLN is assigned and VIPER TSU/regional encryption trusted agent loads keys

Figure 1: Encryption process flow for local and State of North Carolina/National keys

PROGRAMMERS CHECKLIST	PROCESS
Load county specific SLN(s) (Obtain SLN assignment from VIPER POC)	INTERNAL
Load SLNs 1-20 (Discipline specific) if desired? NAT keys 3, (5/6), 11, 12, 13, 14 (LE only)	NC/NAT
Load default SLN 2990 (NC Patch Key)	NC/NAT
Load SLN 2997-2999 NC Interoperability keys (ALGO dependent)?	NC/NAT
Any State Entity SLN(s) need to be loaded? (Contact entity POC initially)	NC/NAT
Functionality test	LOADER

APPENDIX A STATE CHECKLIST FOR SUCCESSFUL ENCRYPTION

STATE CHECKLIST FOR SUCCESSFUL INTEROPERABLE ENCRYPTION	CHECK
Identify key management authorities, roles, and responsibilities	Complete
Utilize Project 25 standards-based encryption to maximize communications interoperability	Complete
Develop an encryption key management plan to protect against compromise and reduce operational uncertainty	Complete
Coordinate key management plan with partner agencies	All
Maintain accountability of all key management devices	All
Limit key distribution only to authorized entities	All
Determine number of encryption keys needed from NLECC	Complete
Obtain interoperability encryption keys from NLECC	In Progress
Coordinate with NLECC for agency specific operational keys	Complete
Follow key management practices recommended by NLECC	Complete
Maintain a record of all devices that receive encryption keys	VIPER POC and TSU
Purchase multikey radios to provide flexibility for interoperability, including OTAR	All
NLECC provides a centralized, secure mechanism for receiving national interoperability keys and unique encryption keys	Complete
NLECC provides keys only to KFDs with all Wi-Fi capabilities disabled	Complete
Agencies must develop procedures to notify NLECC of lost/stolen radios loaded with NLECC provided keys to enable NLECC to take corrective action	Complete
Organizations should follow the National SLN Assignment Plan	Complete
Establish a key management SOG. Define guidelines required to report any lost or stolen device with 24 hours; identify guidelines for emergency re-key if applicable	Complete
Maintain a subscriber unit inventory. Document all subscriber units and associated encryption keys so if a subscriber device is compromised or lost, the vulnerability can be eliminated	VIPER POC and TSU
Agencies using DES should create plans to migrate toward AES 256	All
Use only validated FIPS 140-2 encryption algorithms	All

APPENDIX B NLECC PROCESSES AND PROCEDURES

NLECC generates and distributes national interoperability keys for SLNs 1-20, as well as unique encryption keys for individual agencies' use. They can also provide short-term special operations encryption keys (both voice and data) in situations where limited use keys are needed. NLECC maintains a database of assigned keys to prevent key overlap and conflicts among agencies.

NLECC has established the following voice privacy security settings:

- **Level 1:** Clear voice. No security. Assumes all communications and data transmissions are being monitored.
- **Security Level 2**: Non-changing (static) secure voice encryption using DES-Output Feedback (OFB) or AES 256 keys. Initially provides a high level of security, but over time the likelihood of compromise increases significantly as radios are lost, stolen or misplaced.
- **Security Level 3**: Monthly changing of secure voice and data encryption DES-OFB keys. Provides a high level of voice and data communications security; however, DESOFB encryption has been compromised and is vulnerable to attack.
- **Security Level 4**: Monthly changing of AES 256 key secure voice and data encryption keys. Provides a very high level of voice and data communications security.
- **Security Level 5**: One-time, highly restricted and limited-use tactical operations AES 256 secure voice and data encryption keys. Provides the maximum level of voice and data communications security because the user groups are small, and the crypto period is short.

APPENDIX C REFERENCE DOCUMENTS ON ENCRYPTION

Security Requirements for Cryptographic Modules (FIPS PUB 140-2)
https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

NIST Withdraws Outdated Data Encryption Standard
www.nist.gov/news-events/news/2005/06/nist-withdraws-outdated-data-encryption-standard

NIST Key Management Guidelines
https://csrc.nist.gov/Projects/Key-Management/Key-Management-Guidelines

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

NIST Special Publication SP 800-57 Part 2 Rev. 1: Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations
https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final

NIST Special Publication SP 800-57 Part 3 Rev. 1: Recommendation for Key Management, Part 3: Application-Specific Key Management guidance
https://csrc.nist.gov/publications/detail/sp/800-57-part-3/rev-1/final

NIST Special Publication 800-130: A Framework for Designing Cryptographic Key Management Systems
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf

NIST Special Publication 800-131A Revision 2: Transitioning the Use of Cryptographic Algorithms and Key Lengths
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

NIST Special Publication 800-175A: Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf

NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Federal Information Security Modernization Act of 2014
https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

The E-Government Act of 2002 (FISMA public law 107-347)
https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Fiscal Year 2019 SAFECOM Guidance on Emergency Communications Grants
https://www.dhs.gov/sites/default/files/publications/safecom_guidance_fact_sheet_april_2019_final_508c_v2.pdf

APPENDIX D NPS CHANNELS - QUICK REFERENCE

Band	Encryption use
National Interoperability 800MHz	Not permitted
National Interoperability VHF	Not permitted
National Interoperability UHF	Not permitted
National Interoperability 700MHz	Allowed EXCEPT on calling channels - National SLN 12**
	It is highly recommended to load 700MHz encryption
	** 700MHz NPS Channels are the only channels allowed to have user selectable encryption. The user needs to be familiar with how to enable/disable the encryption

Any mention of vendor/radio in this document is for information or illustration purposes only and does not indicate an endorsement of a particular vendor or product

Persons looking for further information about encryption in the State of North Carolina should contact:

Greg Hauser
Statewide Interoperability Coordination
North Carolina Emergency Management
1636 Gold Star Dr.
Raleigh, NC 27607
(919)825-2262
Greg.hauser@ncdps.gov

Michael Hodgson
VIPER System Administrator
North Carolina State Highway Patrol
Technical Services Unit
3318 Garner Rd.
Raleigh, NC 27610
Michael.hodgson@ncshp.org