07 JAN 2021

State of Idaho

Idaho Public Safety Communications Commission

Land Mobile Radio Encryption Guidance

This page intentionally left blank.

SIGNATURE PAGE

Approved by:

Name/Title/Agency SWIC Date

Name/Title/Agency LMR Chairperson Date

Name/Title/Agency IPSCC Chairperson Date

** This document was formally approved at the 07 JAN 2021 IPSCC meeting with included required changes*

RECORD OF CHANGES

Change No.	Date	Description	Signature

The use of this record of change helps manage modifications throughout the life of this document. All attempts have been made to ensure the accuracy of the information within this overview.

Table of Contents

List of Tables

INTRODUCTION

This document provides guidance for all Idaho public safety / public service entities considering or already utilizing communications encryption. It does NOT require the use of encryption. As the public safety user community continues to implement digital technology to support mission-critical voice communications, there is an increasing need to protect sensitive information transmitted over the air and within the respective networks. Idaho recognizes the need for interoperable, and secure, communications. Agencies considering encryption should carefully weigh the increased security advantages against potential impacts on operability and interoperability.

The Advanced Encryption Standard (AES), at 256 bit encryption, is the nationally recognized cryptographic standard for digital land mobile radio systems. This document strongly recommends compliance with that standard. AES-256 is a standards-based encryption solution using National Institute of Standards (NIST) and Federal Information Processing Standard (FIPS)-197 compliant protocols. Using AES-256 should contribute to the highest level of secure communication in an interoperable environment. It is the strongest and most robust encryption standard that is commercially available today.

This document provides a basic plan that coordinates encryption keys used statewide that may include other keys issued at the local, state, and federal levels. It should be noted that this document does not dictate individual agency generated encryption keys. However, individual agencies need to take steps to avoid Storage Location Numbers (SLN) and Key Identification (KID) conflicts with other agencies. This document is meant to advise and assist agencies that have existing encryption in place as well as agencies considering new encryption implementations.

It should be noted that this guidance only applies to the SLN and KID. Traffic Encryption Keys (TEKs) are left entirely to the agency to create. The only exception to that premise are the National Law Enforcement Communications Center (NLECC) issued keys. NLECC keys are federally managed. 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 choose to share their encryption key(s). This guide does not reveal individual agency keys and or policies.

What are the likely costs incurred by implementing encryption?

Agencies considering the use of encryption should conduct a cost-benefit analysis of their agency’s needs. They should consider what potential side effects or second order affects occur if they choose to encrypt. The following basic questions highlight what an agency may consider. Agencies should consider consulting with other agencies who have successful integrated encryption into their operations. This list is not all inclusive:

1) If my agency chooses to encrypt what will be the resulting follow on effects to other mutual responders?

    a. Will interagency communications still work? For instance, will fire/EMS units still be able to monitor key law enforcement channels?

    b. Will other non-public safety agencies, such as public works, be able to monitor fire department calls and responses?

2) Who will our agency be excluding by encrypting?

    a. Do we have daily operability or interoperability with adjacent jurisdictions that will no longer exist?

    b. Will special arrangements need to be made for media notification?

    c. Will local authorities and the public understand a perceived lack of transparency when they can't scan radio traffic.

3) Who should be included in our decision to encrypt?

    a. Agencies internal to our community?

    b. City, county, state, regional or tribal entities?

    c. Have mutual aid partners been consulted? Existing policy?

4) What are the necessary equipment considerations?

    a. Modifications of feature sets in subscriber devices?

    b. Recording equipment modifications?

    c. Console modifications?

5) What are the actual monetary costs to the agency(s)?

    a. The cost of new feature sets for subscriber devices?

    b. The cost of the time involved in building records for the encryption process? Key management policies, memorandums of agreement or understanding?

    c. Time and manpower costs involved with adoption and operation of encrypted networks?

    d. The cost of encrypting (loading keys) in subscriber devices and/or console systems.

PROJECT 25 (P25) AES-256 ENCRYPTION BASICS

P25 Compliance Assessment Program: In March of 2017, the U.S. Department of Homeland Security announced a change in the Project 25 Compliance Assessment Program (P25 CAP) listing of grant-eligible radio equipment for first responders. In order to be compliant with P25 CAP encryption requirements, radio equipment that utilizes encryption must be capable of AES-256 bit encryption. Equipment that uses proprietary or other non-standard encryption capabilities without also providing AES-256 capability does not meet the requirement specified in the *P25 CAP Encryption Requirements Compliance Assessment Bulletin (CAB).*

Federal and Other Grants: Agencies receiving federal or other source grant funding (state, local, etc.) must ensure compliance with applicable grant requirements. Current SAFECOM guidance specifically states that encryption capable radios purchased with federal funds shall be capable of utilizing the AES-256 algorithm. The 2020 SAFECOM grant guidance specifies AES-256 for P25 radio systems, and the Federal Communications Commission (FCC) specifies the AES-256 encryption algorithm for use on the 700 MHz Interoperability channels. The State Administrative Agency (SAA) and Statewide Interoperability Coordinator (SWIC) are responsible for ensuring communication oriented purchases follow applicable federal and state guidelines.

Coordination: Failure to coordinate encryption technical parameters can hamper operability and interoperability and may even result in loss of communications. Public safety agencies who choose to implement encryption should implement standards-based encryption to ensure multi-vendor compatibility and information security. Deployments of older or proprietary encryption types/algorithms should be avoided. While implementing older or proprietary encryption may appear to cost less upfront, it will certainly cost the agency more in the long run both monetarily and from an interoperability standpoint.

Keys that are developed by The State of Idaho and coordinated interoperable encryption keys will be AES-256 compatible. On a case-by-case basis only, the State of Idaho may opt to temporarily issue a limited number of keys that are not AES 256 during a “transitional period”. This would be for non-standard situational events only. A transitional period would be in place that would allow for agencies that do not have AES 256 to have some level of interoperability on their current encryption platform while migrating to AES 256. National Interoperability keys issued by the NLECC are in both AES-256 and DES algorithms (for transitional purposes) but the preferred algorithm will be AES-256. DES and AES-256 algorithms are not interoperable with each other.

Purchasing Considerations: Agencies purchasing radios capable of encryption are strongly encouraged to procure radios with support for multiple encryption keys (sometimes known as “multikey”). While other encryption types are sometimes used, it is recommended that all future subscriber device (radio) purchases allow for use of the AES-256 algorithm. Agencies that continue use proprietary or non-AES256, algorithms should consider a plan of transition to AES-256 as soon as practical.

ENCRYPTION KEY ASSIGNMENT AND DISTRIBUTION

SLN and encryption key assignments in this plan are allocated based on de-confliction amongst agencies while also considering the National SLN plan. The SLNs in use by federal agencies are listed to reduce the risk of programming conflicts. Once an agency has decided to implement P25 AES encryption, SLN/KID assignments should be made and reviewed periodically to prevent operational encryption conflicts. Blocks of SLNs, and KIDs have been allocated for each county. If additional SLNs or KIDs are needed they will be issued upon request. Agencies wishing to encrypt are encouraged to contact the PSC License and Frequency Manager listed below for assistance. The guidance flow chart listed in Appendix A will help an agency navigate the process to confirm SLN and Key ID assignments.

Central points of contact for encryption are:

Mr. Brad Maxwell
PSC License and Frequency Manager
Idaho Military Division
Public Safety Communications
bmaxwell@imd.idaho.gov
208-288-4007

Mr. Brian Shields
Statewide Interoperability Coordinator (SWIC)
Idaho Office of Emergency Management
bshields@imd.idaho.gov
208-258-6566

Initial SLN/KID allocations are listed in Appendix G. The PSC License and Frequency Manager will manage the database of assigned CKR/KIDs in an effort to prevent overlap conflicts and record changes. They will also routinely coordinate with the Idaho 700MHz Public Safety Communications Network Administrator to ensure network and/or frequency specific concerns. A yearly report will be provided to the SWIC on the status of known encryption adoption across Idaho.

The table below is an example of SLN and KIDs from the Idaho Encryption SLN and KID plan. It is representative of the interoperability SLN and Key ID assignments available in Idaho. The SLNs and KIDs would be useable by the respective disciplines as noted in the table. The first two listings SLN 1 and SLN 12 are from the National SLN table as issued by the NLECC. They are available through the state for multiple disciplines. KIDs are listed in both decimal and hexadecimal formats. A KID that is entered in a key fill device (key loader) must be entered in a hexadecimal format. The P25 standard utilizes a hexadecimal header in the message string to identify the key being sent from one radio to another. Hexadecimal numbering uses a base numerical notation of 16 versus 10. Decimal numbering uses 10 as a base. SLNs remain in decimal format.

AGENCY / FUNCTION	SLN # (Decimal)	KID (Dec)	KID (Hexadecimal)	ALG
NATIONWIDE INTEROP FED W/ LOCAL DES	00001	TBA		DES
NATIONWIDE INTEROP FED W/ LOCAL AES	00012	TBA		AES
Idaho State Interop Static AES	01000	1000	3E8	AES
Reserved	01001	1001	3E9	
Reserved	01002	1002	3EA	
Reserved	01003	1003	3EB	
Reserved	01004	1004	3EC	
Idaho Interop State & Local Common	01005	1005	3ED	AES
Idaho Interop State & Local Law	01006	1006	3EE	AES
Idaho Interop State & Local Fire	01007	1007	3EF	AES
Idaho Interop State & Local EMS	01008	1008	3F0	AES
Reserved	01009	1009	3F1	

Table 1: State of Idaho basic SLN / CKR Ranges for interoperability

Note: Key IDs must be entered in key fill devices in Hexadecimal format to properly operate within a P25 system.

National Key description and table

NLECC generates and distributes national interoperability keys for SLNs 1-20, as well as unique encryption keys for individual agency use. It can also provide short term special operations voice and data encryption keys in situations where limited use keys are needed. NLECC maintains a database of assigned keys to prevent key overlap and conflicts among agencies. The table below illustrates the National Interoperability Keys in SLNs 1-20 that are available from NLECC through the state. NLECC provides a centralized, secure mechanism for receiving national interoperability keys and unique encryption keys.

Keys are issued from the NLECC Key Management Facility (KMF) to a Key Fill Device (KFD) electronically with Wi-Fi abilities on both ends disabled during key transfer. Disablement of the Wi-Fi is mandatory to secure the transmission of data.   Agencies must develop procedures to notify NLECC of lost/stolen radios loaded with NLECC keys to enable NLECC to take corrective action. Organizations should work with NLECC or other qualified agencies to plan their cryptographic strategies and policies.

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 LE 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-International Law Enforcement Interop	When Needed By Ops Requirement
20	AES	PS INTL	Public Safety-International Law Enforcement Interop	When Needed By Ops Requirement

Key OPERATION must be user selectable on NPS 700MHz tactical channels

Table 2: National Interoperability Storage Location Numbers (SLN Keys)

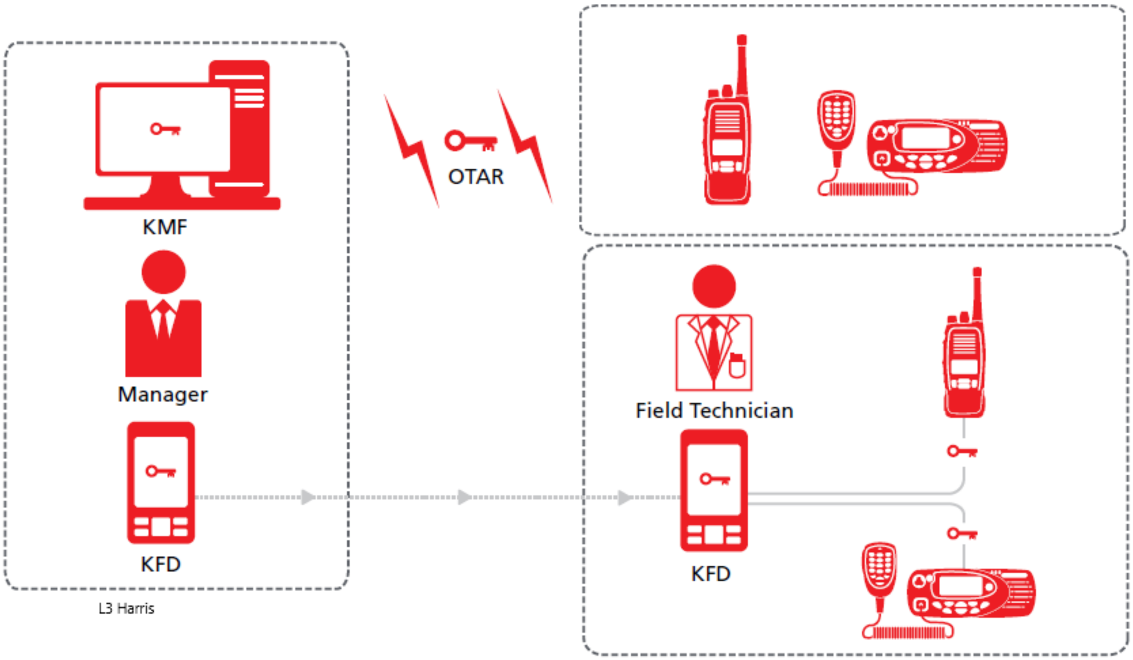
KMF AND OTAR OPERATIONS

A Key Management Facility (KMF) usually consists of a server, client, and an interface to a radio system. Think of the KMF as basically a computer in an office that is normally or habitually connected to a radio system network. The

KMF Server hosts the KMF Server application, handles key management messages (KMMs), manages Over-The-Air-Rekeying (OTAR) operations, and stores all key material and configuration settings. The OTAR function is a highly efficient way to manage radio encryption. Each KMF Client accesses key management information by logging on to the server. From the client, you can configure key management information and load keys on the KMF Server. The KMF Server handles all OTAR operations, including rekey requests, Full and Optimized update, Common (CKR) update, Clear and Encrypted hello, Zeroize, Inhibit, Enable, and Keyset Changeover is highly recommended that Idaho agencies that own and operate KMFs coordinate their efforts with each other. Certain factors need to be identified such as management of the KMFs, associated OTAR feature sets, radio system infrastructure capabilities, key encryption keys (KEK), Radio Set Identifier (RSI) and subscriber device feature sets. Options such as KMF agency partnering should be explored. 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 or lost subscriber device.

Currently, Ada County owns and maintains a KMF. Ada County's KMF does provide for agency partitioning allowing agencies to manage their own encryption operations for radios using the 700 MHz Public Safety Radio Network. Please contact the Public Safety Radio Network Administrator at (208) 577-3618 for more information.

The illustration below is a basic layout of KMF and available methods of key distribution. It depicts both OTAR and KFD encryption key delivery.



OBTAINING AND SHARING OF KEYS

Local Agencies Create Their Own Keys

Individual agency keys are created by the agency with a coordinated SLN and KID issued under the advisement of the PSC License and Frequency Manager. Individual agency keys are then distributed in accordance with the policy of the agency. None of the agency encryption key secret data is seen by any other agency unless deliberately shared. It is possible for an agency to share their key via KFD to KFD. If an agency has a KMF, the agency may also share their keys via OTAR to subscriber devices or to KFDs (through dial-in or manual transfer).

Management of National and / or State of Idaho Interoperability Keys

National keys may be obtained by the State of Idaho designated representative. This would occur by “dialing-in” to a KMF modem with a KFD authorized by NLECC. The KFD will receive a key fill consisting of the current national keys. This process may also be utilized by authorized techs statewide or shared to the techs by Idaho through a manual distribution process using the master KFD. A partnership between a KMF owner agency and the State of Idaho may also be used where the KMF owner receives the keys on behalf of the State, from NLECC and then transfers the keys to a KFD. At no time should any agency transfer State or NLECC keys from one key-loader to another without authorization from the PSC License and Frequency Manager or SWIC. All key fill devices must be password protected and utilize the audit trail function, which may be viewed in the key-loader by the SWIC or their designee upon demand.

Record Keeping Through Memorandums of Understanding / Agreement (MOU/MOA)

A best practice is to keep complete and accurate records of KFDs, subscriber units (SU), and organizations with whom you share keys. For interagency operations requiring encrypted interoperable communications, participating organizations should implement MOU/MOAs when practical to formalize key management and governance processes. Where circumstances do not allow for formal agreements, organizations should agree informally on roles and responsibilities but be certain there is clear understanding among them.

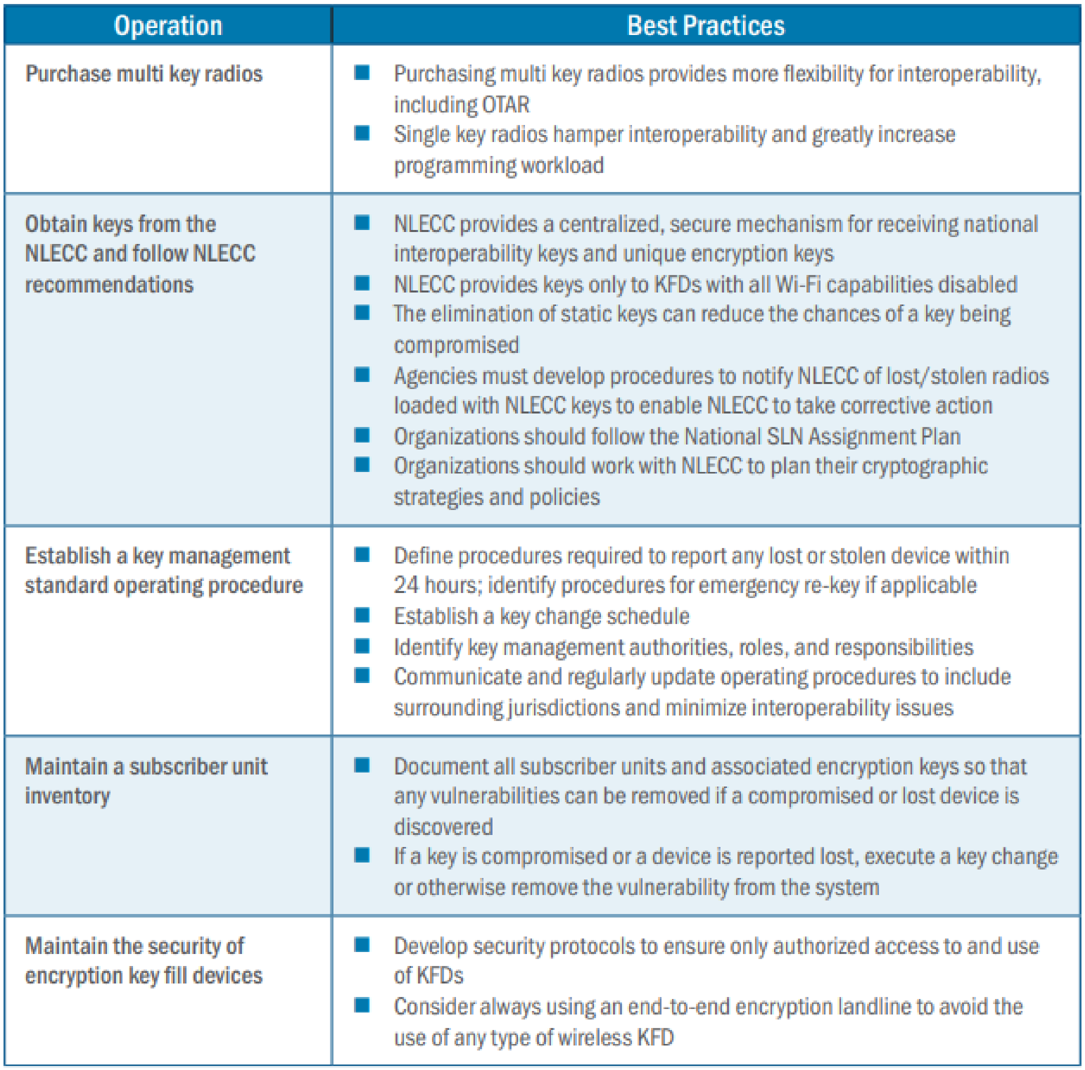
SECURITY CONSIDERATIONS

The core reason for utilizing encryption on a land mobile radio (LMR) system is to maintain information and operational security. With this in mind, it is imperative that security is maintained over the encrypted subscriber units and the key fill devices. Below are a couple of basic security measures that should be considered.

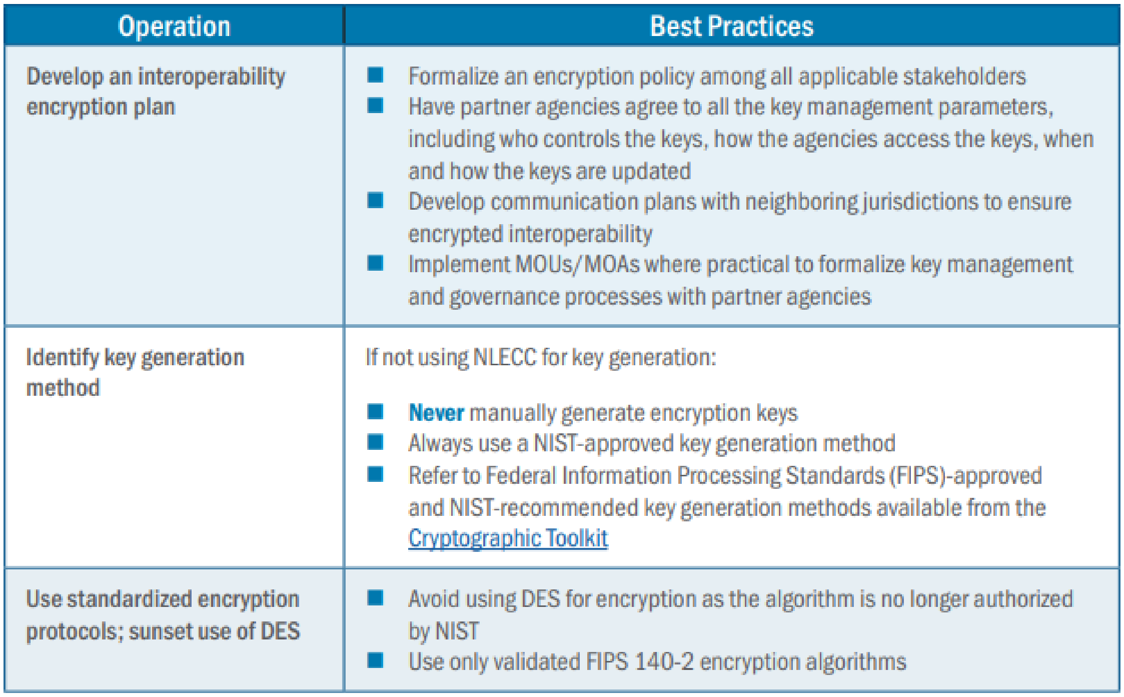
1) Require all personnel to promptly report lost and stolen radios to minimize the risk to the agency's communications. The State will report to NLECC the loss of any radio containing one or more NLECC.

2) Key administrators should maintain accountability and security of all KFDs. If third parties are entrusted with KFDs to load keys into agency radios, those parties should be thoroughly vetted and carefully monitored.

OPERATIONAL BEST PRACTICES CHART



Operation	Best Practices
Purchase multi key radios	■ Purchasing multi key radios provides more flexibility for interoperability, including OTAR ■ Single key radios hamper interoperability and greatly increase programming workload
Obtain keys from the NLECC and follow NLECC recommendations	■ NLECC provides a centralized, secure mechanism for receiving national interoperability keys and unique encryption keys ■ NLECC provides keys only to KFDs with all Wi-Fi capabilities disabled ■ The elimination of static keys can reduce the chances of a key being compromised ■ Agencies must develop procedures to notify NLECC of lost/stolen radios loaded with NLECC keys to enable NLECC to take corrective action ■ Organizations should follow the National SLN Assignment Plan ■ Organizations should work with NLECC to plan their cryptographic strategies and policies
Establish a key management standard operating procedure	■ Define procedures required to report any lost or stolen device within 24 hours; identify procedures for emergency re-key if applicable ■ Establish a key change schedule ■ Identify key management authorities, roles, and responsibilities ■ Communicate and regularly update operating procedures to include surrounding jurisdictions and minimize interoperability issues
Maintain a subscriber unit inventory	■ Document all subscriber units and associated encryption keys so that any vulnerabilities can be removed if a compromised or lost device is discovered ■ If a key is compromised or a device is reported lost, execute a key change or otherwise remove the vulnerability from the system
Maintain the security of encryption key fill devices	■ Develop security protocols to ensure only authorized access to and use of KFDs ■ Consider always using an end-to-end encryption landline to avoid the use of any type of wireless KFD



Operation	Best Practices
Develop an interoperability encryption plan	■ Formalize an encryption policy among all applicable stakeholders ■ Have partner agencies agree to all the key management parameters, including who controls the keys, how the agencies access the keys, when and how the keys are updated ■ Develop communication plans with neighboring jurisdictions to ensure encrypted interoperability ■ Implement MOUs/MOAs where practical to formalize key management and governance processes with partner agencies
Identify key generation method	If not using NLECC for key generation: ■ **Never** manually generate encryption keys ■ Always use a NIST-approved key generation method ■ Refer to Federal Information Processing Standards (FIPS)-approved and NIST-recommended key generation methods available from the Cryptographic Toolkit
Use standardized encryption protocols; sunset use of DES	■ Avoid using DES for encryption as the algorithm is no longer authorized by NIST ■ Use only validated FIPS 140-2 encryption algorithms

SUMMARY OF RECOMMENDATIONS

- Agencies need to very carefully consider the feature sets of subscriber devices, consoles, and other equipment that require keys to be loaded in order to maintain functionality and interoperability.
- Agencies planning to use federal grant funding for P25-compliant equipment with encryption should ensure that they are ordered with the AES-256 encryption algorithm. Agencies that are planning to utilize federal or state grants should consult with the SWIC for SAFECOM and DHS guidance prior to making a purchase.
- National standards designate AES as the primary encryption algorithm.
- Agencies purchasing radios capable of encryption are strongly encouraged to procure radios with support for multiple encryption keys (sometimes known as “multikey”).
- By FCC rule, 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. (See Appendix G)
- CKR 1 through 20 (decimal) are reserved for nationwide interoperability, as managed by NLECC. Agencies should avoid using CKR 1 through 20. Existing 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 method where the encryption is active and fixed on a per channel basis, which is commonly known as “strapped encryption”, so that the user can’t accidently disable encryption.

- Agencies shall avoid patching encrypted channels to un-encrypted channels either within system or across disparate systems using an LMR gateway device as this results in the entire communication being compromised. This, in turn, could result in jeopardizing the security and/or safety of responders.
- Per Federal Communications Commission rules users utilizing encryption on national interop 700 MHz frequencies must be able to "readily disable encryption". This can be done on a per channel basis with a switch or simply with the channels programmed as unencrypted in an adjacent zone.

  In other cases, it may be necessary to have the flexibility to utilize multiple keys on selected talk-groups or channels, such as with the National keys. In this case the talk-group or channel should be strapped for encryption but still allow the user to select the appropriate key.
- Any radio that is lost or stolen that contains state or NLECC keys should be handled in accordance with the user's agency policy. The SWIC and PSC License and Frequency Manager should receive notification. In radios having NLECC keys, the loss must be reported immediately to NLECC through the SWIC.

GLOSSARY OF TERMS

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 (CKR): A decimal value between 1 and 4095 that is utilized by the radio and programming software to locate the encryption key within memory. Also known as the Storage Location Number (SLN).

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.

DECIMAL: Relating to or denoting a system of numbers and arithmetic based on the number ten, tenth parts, and powers of ten.

HEXADECIMAL: The hexadecimal number system, also called *base-16* or sometimes just *hex*, is a number system that uses 16 unique symbols to represent a particular value. Those symbols are 0-9 and A-F. P25 radio systems use both decimal and hexadecimal.

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 (KFD): A module used to load cryptographic keys into electronic encryption machines.

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 secure computer that serves as an application server and key material storage facility. The KMF can create, store, and manage keys.

KEY VARIABLE LOADER (KVL): A KVL is also known as a Key Fill device and generally uses a data protocol for transferring cryptographic keys to a radio or other devices.

MEGAHERTZ (MHz): A unit of electromagnetic (EM) wave frequency equal to one million hertz (1,000,000 Hz).

NATIONAL LAW ENFORCEMENT COMMUNICATIONS CENTER (NLECC): US Customs and Border Patrol key management operation in Orlando Florida.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST): NIST standards are based on best practices from several security documents, organizations, and publications, and are designed as a framework for federal agencies and programs requiring stringent security measures.

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.

PROJECT 25 (P25): Project 25 defines system interfaces that are utilized to build P25 communications networks. TIA-102 Standards documents define the messages and procedures required for P25 features to operate across the P25 system interfaces.

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

RADIO SET IDENTIFIER (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. This is also known as a "CKR."

STATEWIDE INTEROPERABILITY COORDINATOR (SWIC): As the central coordination point for their state or territory, the SWIC plays a critical role in a state’s interoperability effort. The SWIC works with emergency response leaders across all levels of government to implement a statewide strategic vision for interoperability.

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

ULTRA-HIGH FREQUENCY (UHF): Radio frequencies in the range between 300 megahertz (MHz) and 3 gigahertz (GHz).

VERY HIGH FREQUENCY (VHF): Radio frequencies in the range between 30 and 300 MHz.

APPENDIX A: ENCRYPTION SLN / KID PROCESS FLOW

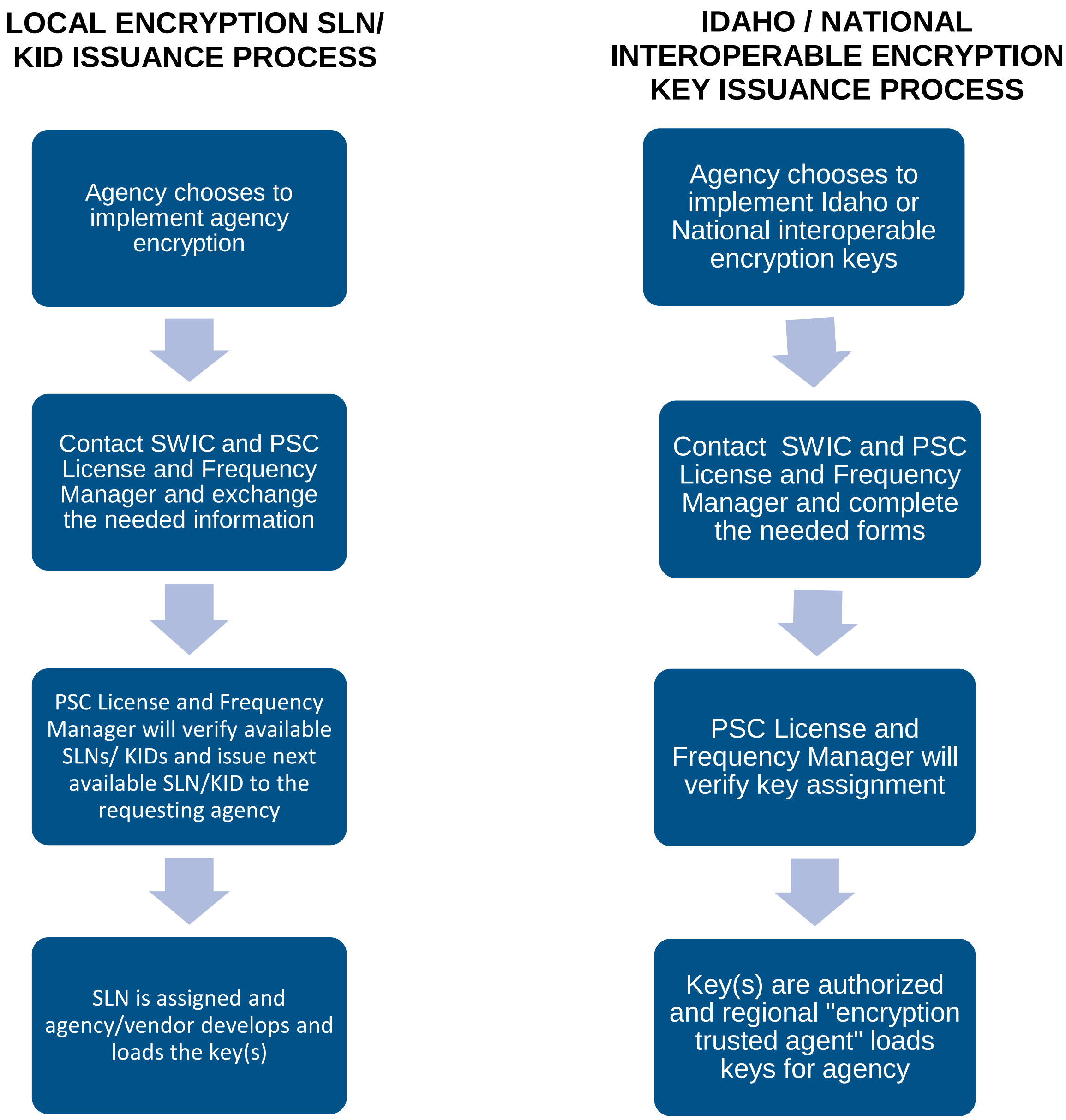

LOCAL ENCRYPTION SLN/ KID ISSUANCE PROCESS
Agency chooses to implement agency encryption
Contact SWIC and PSC License and Frequency Manager and exchange the needed information
PSC License and Frequency Manager will verify available SLNs/ KIDs and issue next available SLN/KID to the requesting agency
SLN is assigned and agency/vendor develops and loads the key(s)
IDAHO / NATIONAL INTEROPERABLE ENCRYPTION KEY ISSUANCE PROCESS
Agency chooses to implement Idaho or National interoperable encryption keys
Contact SWIC and PSC License and Frequency Manager and complete the needed forms
PSC License and Frequency Manager will verify key assignment
Key(s) are authorized and regional "encryption trusted agent" loads keys for agency

Figure 1: Encryption Process Flow for Local and State of Idaho / National Keys

APPENDIX B: CHECKLIST FOR SUCCESSFUL ENCRYPTION

STATE CHECKLIST FOR SUCCESSFUL INTEROPERABLE ENCRYPTION	CHECK
Identify key management authorities, roles, and responsibilities	
Utilize Project 25 standards-based encryption to maximize communications interoperability	
Develop an encryption key plan to protect against operational compromise and reduce uncertainty of having successful missions	
Coordinate key plan with partner agencies to maintain operability and interoperability	
Maintain accountability of all key management devices	
Limit key distribution only to authorized agencies	
Determine number of encryption keys needed for secure operations	
State coordination / distribution of national interoperability encryption keys from NLECC	
Agencies coordinate with the PSC License and Frequency Manager and or SWIC for discipline specific state and National keys	
Follow good key management practices recommended by groups such as FPIC and NCSWIC	
Maintain a record of all KFDs that receive encryption keys	
Utilize multi-key radios to provide flexibility for interoperability, including OTAR if applicable	
NLECC provides keys only to KFDs with all Wi-Fi capabilities disabled	
SWIC utilizes procedures to notify NLECC of lost/stolen radios loaded with NLECC provided keys to enable NLECC to take corrective action	
Organizations should follow the National SLN Assignment Plan	
Define procedures required to report any lost or stolen device with 24 hours; identify procedures for emergency re-key if applicable	
Maintain a subscriber unit inventory. Document all subscriber units and associated encryption keys so, the vulnerability can be removed if a subscriber device is lost or stolen	
Agencies utilizing non-standard encryption should create a plan to migrate to AES-256	

APPENDIX C: EXAMPLE ENCRYPTION END USER AGREEMENT AND NON-DISCLOSURE FORM FOR *NLECC NATIONAL KEYS AND STATE DEVELOPED INTEROPERABILITY KEYS*

Form Description

This form is an example that can be tailored as needed. It was developed in response to several security breaches that have occurred with encryption keys in the past. Maintaining security over encryption keys is of utmost importance. Nationally, there have been incidents where persons entrusted with encryption keys in key fill devices working with public and private agencies have improperly or illegally shared encryption keys with persons who were not authorized to receive the keys. In addition, certain persons from public safety agencies have falsely represented their authority on behalf of an agency to receive keys for that agency. It is important for administrators to know who is holding keys. The primary reason for using a form such as this is to formalize and emphasize to the key holder that they understand the responsibility they are accepting.

Example Idaho Encryption End User Agreement and Non-Disclosure Form

I,___________________________________, an individual, official, employee, consultant, or contractor of or to ____ (the authorized entity), as defined by existing encryption keyloading and programming guidance, intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the issuing agency.

Idaho Land Mobile Radio Encryption Guidance

I attest that I am familiar with, and I will comply with all requirements of the Idaho Land Mobile Radio Encryption Guidance, as amended from time to time, and with any such additional requirements that may be officially communicated to me by the PSC Frequency Coordinator or SWIC.

Sensitive Security Information

I attest that I am familiar with the encryption process and associated operational security principles. I understand that the programming of secure talk-groups and encryption keys into unauthorized radios may adversely affect the integrity and safety of highly sensitive operations, protection of public infrastructure, movement of mass care medications, command and control of terrorism related and other significant events that may place the safety of first responders, support personnel and the general public at risk, and may lead to serious INJURY and even DEATH of the aforementioned parties. I agree that only authorized radios, as defined by the authorized entity or current Idaho encryption guidelines will receive secure key programming.

Secure Key & Key Fill Device (KFD) Protection

I agree that by receiving the **Idaho statewide or NLECC National encryption keys** and/or Key Fill Device (KFD) that I will protect said keys and devices and, if applicable, the written key code(s), from unauthorized access, use or distribution. I further agree that I will not transfer any interoperability related keys to an unauthorized KFD or to any party that is not signatory to a fully executed non- disclosure agreement that includes Secure Key & Key Fill Device (KFD) protection.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. By being granted conditional access to the information indicated above, IPSCC and the __________(authorized entity) has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.

2. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access.

3. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization from the (authorized entity). Should situations arise that warrant the disclosure or release of such information I will do so only under circumstances

approved by the authorized entity and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

4. The encryption related information which I have or will have in my possession is covered by this Agreement, and I will handle and safeguard this information in a manner that affords sufficient protection so as to prevent the unauthorized disclosure of or inadvertent access to such information. Such protective measures shall be taken consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return to the authorized entity all information to which I have had access or which is in my possession upon the occurrence of any of the following circumstances: 1) upon demand by an authorized individual; 2) the conclusion of my duties, association, or support to the Authorized Entity; 3) upon the determination by the authorized entity that my official duties do not require further access to such information.

5. I shall report any loss, theft, misuse, misplacement, unauthorized disclosure, or other security breach, I have knowledge of and whether or not I am personally involved to the designated representative within 48 hours. My identity will be kept private to the extent possible when reporting security violations.

6. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement.

7. This Agreement is made and intended for the benefit of encryption partners. By granting me conditional access to information in this context, encryption partners may seek any remedy available to them to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

8. Unless and until I am released in writing, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

10. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the State of Idaho or any of its departments or agencies.

11. I represent and warrant that I have the authority from the (authorized entity) to enter into this Agreement.

12. I have read and understand the terms of this Agreement.

NON-DISCLOSURE AGREEMENT ACKNOWLEDGMENT

Type/Print Name:	Authorized entity:	Telephone Number:
Signature:		

Witness: (optional at the discretion of using entity policy)

Typed/Printed Name:	Agency:	Telephone Number:
Signature:		

APPENDIX D: SPECIFIC KFD TRANSFER ACKNOWLEDGMENT

ACKNOWLEDGEMENT

I ___________________________________, acknowledge receipt of the following Idaho and or National encryption keys:

____

They have been transferred into Keyloader:

Manufacturer ____________________

Model____________________________ Serial # ________________________

________________________________ ________________________________

Printed Name Agency Name

________________________________ ______________________

Signature Date

________________________________ ________________________

Issuer Printed Name Issuing Agency

________________________________ ________________________

Issuer Signature Date

The information is completed at time of KFD / KMF to KFD key transfer and is used to provide a method of tracking which KFDs State and / or NLECC Keys are transferred to. The “audit trail’ feature must be activated on the KFDs so when necessary a determination can be made about what keys have been loaded or transferred to subscriber devices or other key fill devices from the KFD that may be under review. This process is necessary to maintain program security.

APPENDIX E: ENCRYPTION REFERENCE DOCUMENTS

FPIC Encryption documents: https://www.cisa.gov/safecom/blog/2016/10/12/fpic-releases-encryption-documents

Fiscal Year 2020 SAFECOM Guidance on Emergency Communications Grants: https://www.cisa.gov/blog/2020/02/14/release-fiscal-year-2020-safecom-guidance-emergency-communications-grants

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

Cybersecurity & Infrastructure Security Agency (CISA) documents on encryption:

https://www.cisa.gov/publication/encryption

- Guidelines for Encryption in Land Mobile Radio Systems
- Best Practices for Encryption in P25 Public Safety LMR Systems
- Developing Methods to Improve Encrypted Interoperability in Public Safety Communications
- Considerations for Encryption in Public Safety Radio Systems
- Determining the Need for Encryption in Public Safety Radios Fact Sheet
- Encryption Key Management Fact Sheet
- Operational Best Practices for Encryption Key Management

APPENDIX F: NATIONAL PUBLIC SAFETY (NPS) CHANNELS - QUICK REFERENCE

Band	Encryption use
National Interoperability 800 MHz	Not permitted
National Interoperability VHF	Not permitted
National Interoperability UHF	Not permitted
National Interoperability 700 MHz	Allowed EXCEPT on calling channels
Mutual Aid Channels	Depends upon state rules or practices (see information below)
	** 700 MHz NPS Channels are the only channels allowed to have encryption. The user needs to be familiar with how to enable/disable the encryption

The FCC has prohibited the use of encryption on national interoperability channels as noted above. Current rules dictate encryption is effectively prohibited on both the calling and tactical nationwide interoperability channels in the VHF, UHF, and 800 MHz bands and on the calling nationwide interoperability channels in the 700 MHz band.

Any information that must be encrypted can be transmitted over operational channels outside those specifically designated by the FCC for nationwide interoperability. For example, local, regional, and statewide interoperability channels that are distinct from these nationwide interoperability channels are not affected by the FCC order and have the option to be used with encryption. There are also a number of public safety mutual aid channels in use across the U.S. which are not affected by this order. This includes the VFIRE, VMED, VLAW, UHF MED frequencies, and all 700 MHz Air to Ground channels, on which encryption can occur Finally, the NTIA designated interoperability channels (e.g., IR and LE) channels are not impacted by the FCC order. See also the National Interoperability Field Operations Guide (NIFOG).

APPENDIX G: IDAHO AND FEDERAL SLN/KID ALLOCATION CHART

Idaho Static Interoperability Keys

STATE	BLK	SLN #	KID		STATE	BLK	SLN #	KID
	0	**01000 - 01009**	**1000 - 1009**		Lemhi Co(2L)	30	01300 - 01309	1300 - 1309
Ada Co(1A)	1	01010 - 01019	1010 - 1019		Lewis Co(3L)	31	01310 - 01319	1310 - 1319
Adams Co(2A)	2	01020 - 01020	1020 - 1029		Lincoln Co(4L)	32	01320 - 01329	1320 - 1329
Bannock Co(1B)	3	01030 - 01039	1030 - 1039		Madison Co(1M)	33	01330 - 01339	1330 - 1339
Bear Lake Co(2B)	4	01040 - 01049	1040 - 1049		Minidoka Co(2M)	34	01340 - 01349	1340 - 1349
Benewah Co(3B)	5	01050 - 01059	1050 - 1059		Nez Perce Co(1N)	35	01350 - 01359	1350 - 1359
Bingham Co(4B)	6	01060 - 01069	1060 - 1069		Oneida Co(1O)	36	01360 - 01369	1360 - 1369
Blaine Co(5B)	7	01070 - 01079	1070 - 1079		Owyhee Co(2O)	37	01370 - 01379	1370 - 1379
Boise Co (6B)	8	01080 - 01089	1080 - 1089		Payette Co(1P)	38	01380 - 01389	1380 - 1389
Bonner Co(7B)	9	01090 - 01099	1090 - 1099		Power Co(2P)	39	01390 - 01399	1390 - 1399
Bonneville Co(8B)	10	01100 - 01109	1100 - 1109		Shoshone Co(1S)	40	01400 - 01409	1400 - 1409
Boundary Co(9B)	11	01110 - 01119	1110 - 1119		Teton Co(1T)	41	01410 - 01419	1410 - 1419
Butte Co(10B)	12	01120 - 01129	1120 - 1129		Twin Falls Co(2T)	42	01420 - 01429	1420 - 1429
Camas Co(1C)	13	01130 - 01139	1130 - 1139		Valley Co(1V)	43	01430 - 01439	1430 - 1439
Canyon Co(2C)	14	01140 - 01149	1140 - 1149		Washington Co(1W)	44	01440 - 01449	1440 - 1449
Caribou Co(3C)	15	01150 - 01159	1150 - 1159		**RESERVED**	**45**	**01450 - 01459**	**1450 - 1459**
Cassia Co(4C)	16	01160 - 01169	1160 - 1169		ID-ISP	46	01460 - 01469	1460 - 1469
Clark Co(5C)	17	01170 - 01179	1170 - 1179		ID-ITD	47	01470 - 01479	1470 - 1479
Clearwater Co(6C)	18	01180 - 01189	1180 - 1189		ID-EMS & HW	48	01480 - 01489	1480 - 1489
Custer Co(7C)	19	01190 - 01199	1190 - 1199		ID-F&G	49	01490 - 01499	1490 - 1499
Elmore Co(1E)	20	01200 - 01209	1200 - 1209		ID-IDL	50	01500 - 01509	1500 - 1509
Franklin Co(1F)	21	01210 - 01219	1210 - 1219		ID-CORRECTIONS	51	01510 - 01519	1510 - 1519

Fremont Co(2F)	22	01220 - 01229	1220 - 1229		ID-EDUCATION	52	01520 - 01529	1520 - 1529
Gem Co(1G)	23	01230 - 01239	1230 - 1239		IMD & ALL ST GOVT.	53	01530 - 01539	1530 - 1539
Gooding Co(2G)	24	01240 - 01249	1240 - 1249		**RESERVED**	**54**	**01540 - 01549**	**1540 - 1549**
Idaho Co(1I)	25	01250 - 01259	1250 - 1259		Shoshone-Bannock	55	01550 - 01559	1550 - 1559
Jefferson Co(1J)	26	01260 - 01269	1260 - 1269		Kootenai	56	01560 - 01569	1560 - 1569
Jerome Co(2J)	27	01270 - 01279	1270 - 1279		Coeur D'Alene	57	01570 - 01579	1570 - 1579
Kootenai Co(1K)	28	01280 - 01289	1280 - 1289		Nez Perce	58	01580 - 01589	1580 - 1589
Latah Co(1L)	29	01290 - 01299	1290 - 1299		Shoshone-Paiute	59	01590 - 01599	1590 - 1599

FED Agency	SLN #				
Interoperable SLN's	001 - 020	CBP/ICE	101 - 110	US Postal	205 - 209
Secret Service SLN's	021 - 025	ATF	111 - 115	NOAA	210 - 214
FEMA	026 - 030	Treasury OIG	116 - 120	DCIS	215 -219
TSA	031 - 035	Justice OIG	121 - 125	Reserved	220 - 224
Coast Guard	036 - 040	USMS	126 - 129	HUD	225 - 229
IRS	041 - 045	DOE	130 - 134	HHS	230 -234
BEP	046 - 050	Local PD's	135 - 140	FDIC	235 - 239
FBI	051 - 060	DHS-OIG	141 - 145	CIS	240
TIGTA	061 - 065	Reserved	146 - 150	Reserved	241 -299
DEA	066 - 070	SSA	151 - 155	Capital PD	300 -304
Reserved I	071 - 080	Reserved	156 - 179	FDA	305 - 309
ICE/CBP	081 - 090	VA OIG	180 - 184	DOL	310 - 314
BOP	091 - 095	Reserved	185 - 200	USDA	315 - 320
USMS	096 - 100	DHS OEM	200 - 204	Reserved	320 - 4095

For further information about Encryption in the State of Idaho, contact:

Idaho Statewide Interoperability Coordinator (SWIC)

Brian Shields
Idaho Office of Emergency Management
bshields@imd.idaho.gov
208-258-6566