Federal Partnership for Interoperable Communications

Update of Key FPIC Activities

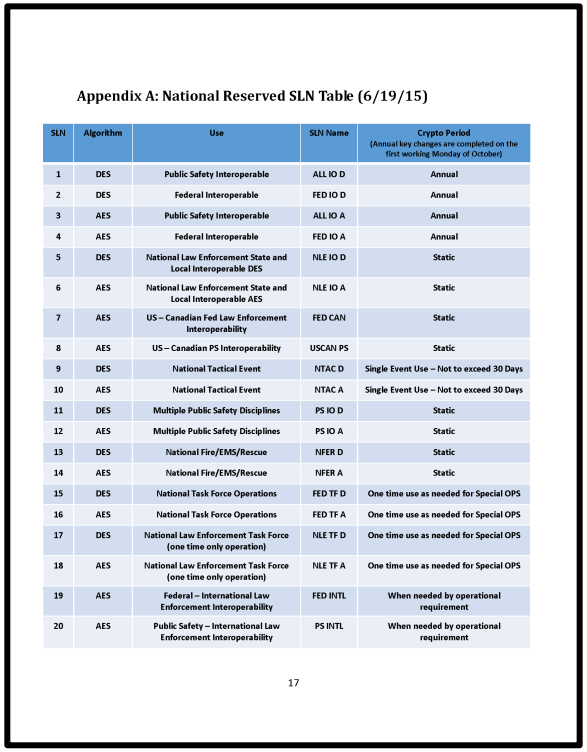
Jim Downes, FPIC Program Manager

Three Key Current Priorities

- Encrypted interoperability and key distribution
- P25 Inter RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) implementation challenges and resolutions and suggested improvements toward interoperability
- Memorandum of understanding for public safety access to NTIA VHF/UHF I/O channels

Encryption Guidance

- The FPIC Security Subcommittee, in coordination with the National Law Enforcement Communications Center (NLECC) and other public safety agencies, developed a standardized SLN assignment list for National Encrypted Interoperability (June 2015)
- OEC and FPIC continues to encourage PS agencies to coordinate SLN and KeyID assignments with the NLECC. An accurate database can minimize conflicts resulting in improved encrypted interoperability
- As a result of challenges identified during recent implementations, the NLECC and FPIC are evaluating key distribution procedures and the SLN Table



Appendix A: National Reserved SLN Table (6/19/15)

SLN	Algorithm	Use	SLN Name	Crypto Period (Annual key changes are completed on the first working Monday of October)
1	DES	Public Safety Interoperable	ALL IO D	Annual
2	DES	Federal Interoperable	FED IO D	Annual
3	AES	Public Safety Interoperable	ALL IO A	Annual
4	AES	Federal Interoperable	FED IO A	Annual
5	DES	National Law Enforcement State and Local Interoperable DES	NLE IO D	Static
6	AES	National Law Enforcement State and Local Interoperable AES	NLE IO A	Static
7	AES	US – Canadian Fed Law Enforcement Interoperability	FED CAN	Static
8	AES	US – Canadian PS Interoperability	USCAN PS	Static
9	DES	National Tactical Event	NTAC D	Single Event Use – Not to exceed 30 Days
10	AES	National Tactical Event	NTAC A	Single Event Use – Not to exceed 30 Days
11	DES	Multiple Public Safety Disciplines	PS IO D	Static
12	AES	Multiple Public Safety Disciplines	PS IO A	Static
13	DES	National Fire/EMS/Rescue	NFER D	Static
14	AES	National Fire/EMS/Rescue	NFER A	Static
15	DES	National Task Force Operations	FED TF D	One time use as needed for Special OPS
16	AES	National Task Force Operations	FED TF A	One time use as needed for Special OPS
17	DES	National Law Enforcement Task Force (one time only operation)	NLE TF D	One time use as needed for Special OPS
18	AES	National Law Enforcement Task Force (one time only operation)	NLE TF A	One time use as needed for Special OPS
19	AES	Federal – International Law Enforcement Interoperability	FED INTL	When needed by operational requirement
20	AES	Public Safety – International Law Enforcement Interoperability	PS INTL	When needed by operational requirement

17

Current FPIC Encryption Activities

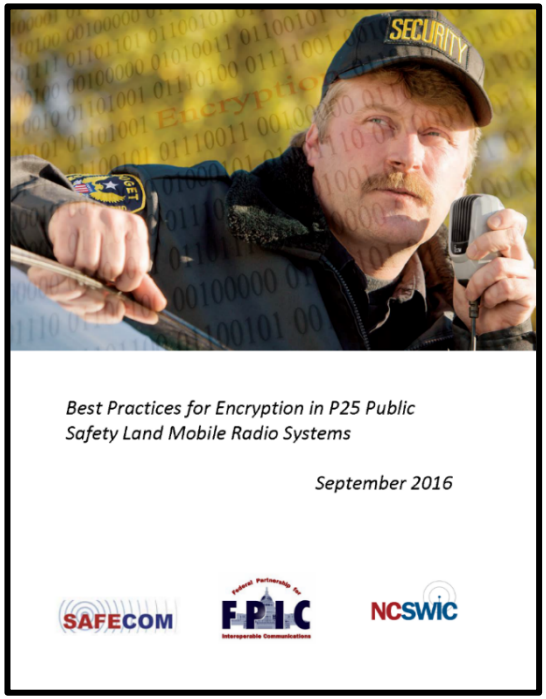
- The FPIC Security Subcommittee is working closely with the NLECC and key PS Agencies to address the challenges recently identified that impact interoperability. Subcommittee efforts include:
  - Addressing specific recommendations to revise the standards relevant to encryption
  - Recommending more stringent requirements for compliant standards (Minimize optional standards)
  - Minimizing the use of non-standard solutions
  - Accelerating the standards development for two key interfaces
  - Reevaluating key distribution procedures and the use of “static keys” for I/O

Current FPIC Encryption Activities

- The FPIC Security Subcommittee formed a small focus group comprised of knowledgeable SMEs to address the following topics:
  - Major areas relevant to standards, including, P25 standard adoption by manufacturers and minimize optional standards that impact interoperability
  - The Subcommittee is also considering more effective methods to educate the user before implementing encryption
  - There is a Focus Group meeting scheduled on September 14-15, at the NLECC in Orlando to develop recommendations and draft a position paper to be presented to TIA TR8 in October

Identify & Adopt Best Practices for Encryption

- SAFECOM, FPIC, and NCSWIC partnered to develop the following three documents, with accompanying facts sheets, to provide guidance to public safety agencies who are considering implementing encryption
  - *Guidelines for Encryption in Land Mobile Radio Systems*
  - *Considerations for Encryption in Public Safety Radio Systems*
  - *Best Practices for Encryption in P25 Public Safety Land Mobile Systems*
- http://www.dhs.gov/technology



ISSI Overview

- The Inter RF Subsystem Interface (ISSI), a P25 Phase 2 technology, enhances public safety's ability to interconnect multiple P25 systems

- Many users have successfully implemented ISSIs, and to a lesser extent the console subsystem interface (CSSI), to expand coverage and provide enhanced interoperability between P25 systems regardless of vendor

- Because ISSI is a relatively new technology, there is a learning curve for users and manufacturers alike to understand ISSI expectations and standards

Developing Solutions Through User Engagement

- The standards supporting the P25 ISSI and CSSI are still in progress and both user and manufacturer involvement is critical
- The FPIC is leading an effort to address misunderstandings and miscommunications concerning the ISSI/CSSI
- In May 2016, the FPIC sponsored a working session to share ISSI/CSSI implementation successes, challenges, and experiences between users and manufacturers

FPIC Sponsored ISSI/CSSI User Focus Group

- The ISSI/CSSI User Focus Group was established to consolidate/ consider information from users and identify successes, challenges, and mitigation experienced during implementations (the good, the bad, and the ugly)
- Participants identified several action items for consideration by the group. Two of the more immediate actions are to:
  - Develop an action plan and baseline interoperability requirements
  - Develop discussion topics and hold follow-up working sessions between users and manufactures
- Initial discussions revealed challenges were both technical and governance/funding related

Preliminary Findings

- Preliminary findings revealed a wide range of misunderstandings, including:
  - Users may not understand the functionality covered by the standard
  - Some manufacturers may not have implemented standard functionality desired by the user
  - Manufacturers and users may have different interpretations of the standard definitions of functionality desired by the user;
  - Manufacturers may have different interpretations of the users' desired standard functionality
  - Manufacturers may have implemented the functionality requested by the user, but not covered the by standard

- Some challenges are not technical, but deal with governance and funding

- The best time to identify these misunderstandings is during the planning or testing process.

Upcoming In-Person Working Session

- The upcoming FPIC ISSI/CSSI User Working Session is scheduled for September 19-20, in Arlington, TX
- This meeting is open to any user employed by a government user agency (both days) and any manufacturer (second day) that provides or supports ISSI/CSSI
- This meeting will focus on suggestions and recommendations developed by the Focus Group in a collaborative environment with both users and manufacturers
- If you are interested in attending the upcoming working session, please email FPIC@hq.dhs.gov

Memorandum of Understanding (MOU) for Interoperability Channels

- FPIC is working with state, local, and Federal users to enhance interoperability across the nation
- The NTIA revised procedures within the NTIA Manual to allow the PS Agencies easier access to the NTIA I/O Channels
- DOI led an effort in coordination with the DOJ, DHS Spectrum Management Offices, and FPIC Spectrum Subcommittee to develop an MOU. The MOU was accepted by FCC, NTIA and the SWICs to share interoperability channels in each state
- Chris Lewis, DOI, is the federal signatory and the SWIC (or designated representative) will sign on behalf of the state
- To date, five states have executed the MOU and several others are coordinating efforts with DOI

QUESTIONS ????

For additional information about the FPIC and their initiatives please send an email or visit the FPIC website

FPIC Email: FPIC@HQ.DHS.GOV

FPIC Website: WWW.DHS.GOV/SAFECOM/FPIC