Transition to Advanced Encryption Standard (AES)

Cybersecurity and Infrastructure Security Agency (CISA)
Federal Partnership for Interoperable Communications (FPIC)

PURPOSE

Encryption is the primary means for protecting the confidentiality and providing authentication of sensitive land mobile radio (LMR) voice and data communications. In 2001, the National Institute of Standards and Technology (NIST) established the Advanced Encryption Standard (AES) as the new recommendation for encryption for all federal departments and agencies. In 2005, NIST withdrew its approval of the Data Encryption Standard (DES) and incorporated AES as the new encryption algorithm under the Federal Information Processing Standard (FIPS). However, 18 years later, law enforcement and public safety agencies across all levels of government continue to use **DES—a compromised and insecure encryption algorithm.**

BACKGROUND

NIST defines cryptology standards for the federal government that are intended for unclassified uses and is recognized as the nation's leading authority on sensitive but unclassified encryption. In 1977, NIST endorsed DES (56-bit) as the encryption algorithm for securing federal LMR communications. By the late 1990s, the DES algorithm had been compromised multiple times with greater efficiency and in less time. These successful "cracks" of the algorithm were widely reported on a variety of internet media sites and today there are various tools and techniques readily available to compromise the DES algorithm. In 2005, NIST withdrew approvals of DES and published the FIPS 197 establishing AES as the federal standard for the protection of sensitive, unclassified information as compulsory and binding for all federal departments and agencies. DES derivatives, such as Triple DES and Simplified DES, and the various modes of operations, including DES-Cipher Block Chaining (CBC), DES-Cipher Feedback (CFB), DES-Output Feedback (OFB), DES-Electronic Code Book (ECB), and DES-Counter (CTR) are also considered to be easily compromised through similar brute-force attacks.

As computing technology evolves toward Quantum Computing capabilities, which are principles of quantum mechanics that allow quantum computing machines to solve mathematical problems that are challenging or impossible for traditional computers to tackle, NIST continues to assess the current cryptographic protections and implications these next generation computing machines will have when used to mount brute-force attacks against encryption algorithms.[1] NIST's present guidance is that current applications can continue to use AES with key sizes 128, 192, or 256 bits. NIST will issue guidance regarding any transitions of symmetric key algorithms and hash functions to protect against threats from quantum computers when it can foresee a transition need. Until then, users should follow the recommendations and guidelines NIST has already issued.

[1] NIST Post-Quantum Cryptography: csrc.nist.gov/projects/post-quantum-cryptography

In particular, any encryption algorithm that produces encryption keys with less than 112 bits of classical security should not be used[2].

Most federal agencies have implemented, and are actively using AES for all LMR transactions, but budgetary constraints for many non-federal departments and agencies have continually inhibited the timely and necessary transition to AES. This is one of many factors affecting state, local, tribal, and territorial (SLTT) agencies prolonging the continued generation, distribution, and management of DES encryption, despite the inherent vulnerabilities and known inability to adequately protect both wired and wireless voice and data transmissions. The continuing use and reliance upon DES has several detrimental effects:

Agencies using DES encryption risk having sensitive law enforcement, emergency response and planning information, citizen's personal health information (PHI), and personally identifiable information (PII) accessed and exploited by unauthorized and potentially criminal actors.

Agencies continuing to use DES encryption disrupts and diminishes critical interoperability with federal agencies and other mutual aid partners, as their encrypted channels/talkgroups are incompatible with the current federal standard AES algorithm for encrypted public safety channels and increases delays or the inability to achieve and maintain encrypted interoperability. This may increase the risk to mission success, endanger lives and property, and create unsafe conditions for public safety personnel.

Currently, to maintain encrypted interoperability during multijurisdictional incidents, federal agencies using AES encryption, and SLTT agencies using DES encryption must alter their communications protocols to use DES encryption or issue cache/donor radios with proper AES encryption to response partners to achieve secure interoperable communications. **This consumes critical time, effort, and resources, diverting responders from their primary mission of life-safety and security, and introduces increased vulnerabilities of the compromised DES algorithm.**

DES encryption has continued to be used as the lowest common denominator for encrypted interoperable LMR communications between federal agencies and SLTT agencies that do not have AES encryption capabilities, introducing **unnecessary and unanticipated risks.**

SLTT agencies have no federal mandates or requirements to discontinue the use of DES encryption (except for requirements for continued compliant Criminal Justice Information Services [CJIS] access) or other non-standard or manufacturer proprietary encryption or privacy options.

[2] Derived from: Post-Quantum Cryptography – FAQ, information to be incorporated into revised SP 800-131A by the end of 2023. Last accessed 9/18/2023.

The transition to AES encryption is the only solution that would provide a lowest common denominator of available interoperable encryption for LMR voice and data communications for all public safety entities at all levels of government.

DES USE CASES

The long-term inadequacy of the DES encryption key size was initially identified in 1975. In the early 1990s, DES keys were demonstrated to be subject to compromise through exhaustive key search (i.e., brute-force attacks) using modern computer systems. This recognition led to the development and adoption of the AES encryption algorithm. AES has been scrutinized by leading cryptographers and security organizations worldwide. Few weaknesses (i.e., mathematical shortcuts that can be used to circumvent an exhaustive key search) have been identified.[3]

> ***Until the computing power of the 1990s was realized, claims that DES encryption keys could be "brute force" guessed were refuted. However, poorly implemented DES encryption solutions were found to be susceptible to these types of attacks. Between 1997 and 1999, RSA, a private-sector identity and access management company, sponsored a series of challenges designed to crack the DES algorithm. Each challenge was increasingly more difficult, requiring the contestants to find the DES encryption key in less time than was done in the previous challenge. All three challenges were met with success.***[4]

Furthermore, the lack of robust and active encryption led to several other compromising situations to public safety:

In 2011, the police department for a county in Virginia dealt with home invasions and robberies targeting one ethnic group. After numerous incidents and calls from eyewitnesses, law enforcement determined the perpetrators were using radio scanners to monitor and avoid responding police units.[5]

[3] Guidelines for Encryption in Land Mobile Radio Systems: cisa.gov/sites/default/files/publications/20160204_Guidelines%20for%20Encryption%20in%20Land%20Mobile%20Radio%20Systems_Final508c_0_0.pdf.

[4] The Day DES Died: sans.org/white-papers/722/.

[5] Considerations for Encryption in Public Safety Radio System: cisa.gov/sites/default/files/publications/20160830%20Considerations%20for%20Encryption_Final%20Draft508_0.pdf.

In January 2013, a major metropolitan police department in the southwest broadcasted the location of a shooting suspect's home, alerting the media and causing the suspect to flee prior to police apprehension. Other incidents in the same city have complicated investigations and allowed public access to criminal information of minors, as well as tactical information regarding stakeouts and criminal investigations including incidents involving juveniles, fugitives from justice, and compromise of tactical positions and response.[6]

In addition to these specific situations, in 2011, the National Information and Communications Technology Australia (NICTA), in partnership with Queensland Research Laboratory and Griffith University conducted a comprehensive investigation into the critical security aspects surrounding Project 25[7] protocols. They found that DES, the mandatory cipher for P25 technical standards compliance at that time, was easily breached through exhaustive key search attacks using specialized hardware, demonstrating minimal effort is needed to recover the encryption key.

CRIMINAL JUSTICE INFORMATION SERVICES POLICY

Public safety agencies who engage in the administration of criminal justice (e.g., law enforcement, corrections, judicial, probation and parole, fire arson) investigation routinely use CJIS data to conduct wanted or missing persons checks, obtain a suspect's criminal history, verify the status of stolen vehicles and property, track criminal activity, and conduct investigations. This relationship is governed by written user access agreements promulgated by the Federal Bureau of Investigation's (FBI) CJIS Division, each State's Criminal Justice Agency or State Identification Bureau and by extension, the respective SLTT criminal justice agency. As part of the agreement, all agencies accessing Criminal Justice Information (CJI) must be compliant with CJIS policy, processes, training, and encryption requirements, for the communications networks used for inquiries and response and the protections of data in transit and data at rest.

[6] Considerations for Encryption in Public Safety Radio System: cisa.gov/sites/default/files/publications/20160830%20Considerations%20for%20Encryption_Final%20Draft508_0.pdf.
[7] Project 25 (P25): cisa.gov/safecom/project-25.

Specifically, the current FBI CJIS Policy requirements state that any data transmitted, including across LMR systems, is required to be encrypted by a cryptographic module that is FIPS 140-2/3 certified and uses at least an encryption module that supports a key size of a minimum of 128-bits. Additionally, when any CJIS information is stored digitally outside a physically secure location (i.e., cloud networks), CJIS requirements state that a FIPS 197 certified AES cipher with 256-bit strength must be used.[8]

Under these CJIS requirements, any public safety, criminal justice, or law enforcement agencies that uses CJIS information as part of their operations may be considered out of compliance and risk losing access should they rely on any encryption standard other than AES.

In addition to the FBI CJIS Division's policies and procedures for data access, including the National Crime Information Center, many SLTT entities also operate CJIS with similar requirements and regulations for authorized access and protections of their respective systems and information resources. Lastly, the various nationwide, statewide, regional, and local telecommunications networks (e.g., National Law Enforcement Telecommunications System, state-level law enforcement telecommunications systems) facilitating the movement of CJI have robust requirements for access, encryption, and data protections.

PRIVACY AND INFORMATION PROTECTION

The public, for the purpose of transparency and accountability, has historically had access to public safety LMR communications through available scanners, Internet broadcasting sites, and through media sources. Still, some information is purposefully withheld from the public to ensure the integrity of ongoing investigations, protection of public safety personnel, and the safety of citizens and property. However, the transmission of personal identifiable information (PII) and protected health information (PHI) freely over non-encrypted "clear" wireless communications, such as unencrypted LMR channels and talkgroups, remains a significant threat.

As SLTT agencies contemplate the transition to AES equipment and services and begin to plan, procure, and implement this encryption capability, it becomes most important to protect these plans and processes. In 2002, Congress established the Protected Critical Infrastructure Information (PCII) Program through the Critical Infrastructure Information Act of 2002 (CII Act). Its purpose is to safeguard information shared with the Cybersecurity and Infrastructure Security Agency (CISA) regarding public and private sector owner(s) and operator(s) of physical and cyber critical infrastructure and proprietary data. The Title 6 Code of Federal Regulations (CFR) part 29, also known as the "Final Rule for Procedures for Handling Critical Infrastructure Information,"[9] outlines consistent protocols for how critical infrastructure information (CII) that is voluntarily submitted to CISA should be received, validated, handled, stored, marked, and used. The PCII Program provides certain legal protections to private sector and SLTT government agencies that voluntarily share CII, including:

[8] CJIS Security Policy: fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view.
[9] The Final Rule; Procedures for Handling PCII: cisa.gov/resources-tools/resources/final-rule-procedures-handling-pcii.

Protection from Freedom of Information Act (FOIA) request(s)

Permission for use in Regulatory Proceedings

Exemption from SLTT Disclosure Laws Or “Sunshine Laws”

Authorization for use in Civil Actions

The safeguards of the PCII Program enhance the exchange of CII between infrastructure owners/operators and the government, aiding in the identification of:

Security risks and threats from physical and cyber-attacks

Vulnerabilities and mitigation strategies

Critical infrastructure security during planning and emergencies

These safeguards provide partners with confidence that sharing their information with the government will not lead to the exposure of sensitive or proprietary data to the public.[10] Submission of CII through the CISA website[11] is protected immediately, as public safety practitioners leverage this resource when upgrading encrypted operations capabilities and further protecting critical systems, sites, resources, locations, and information used by public safety and criminal justice agencies.

Agencies at all levels of government must also contemplate the implementation of policies with available encryption technologies that enable transparency and accountability for the public, while still ensuring the safety of personnel, protection of CJI, and citizens’ PII/PHI. Failure to do so places public safety personnel and their agencies at risk for civil and criminal liabilities associated with unauthorized access and dissemination of CJI. It further exposes agencies to potential litigation for breaches or unauthorized dissemination of citizens’ PII/PHI, which can be intercepted by criminal actors monitoring unencrypted public safety LMR or broadband voice communications.

[10] PCII Program: cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program.
[11] Submitting Critical Infrastructure Information: cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/submit-critical-infrastructure-information.

ACTIONS AND NEXT STEPS

There have been several federal actions taken thus far to address security concerns with the DES algorithm and encourage transition to the AES algorithm:

✓ The National Law Enforcement Communications Center is **no longer distributing any new DES keys**, as of January 1, 2022, to any federal, state, local, tribal, and territorial public safety agency.

✓ Existing DES keys may be retained by SLTT agencies with the understanding that they should be **considered compromised** based on the practicality of brute-force attacks of DES keys and the deprecation of the algorithm. This process will delay requirements to significantly change LMR programming code plugs until AES keys are comprehensively supported for interoperability.

✓ The Federal Partnership for Interoperable Communications (FPIC) Security Subcommittee has developed various **informational documents** to illustrate the continuing threat to secure encrypted communications that the use of DES, other non-standardized encryption algorithms, and LMR manufacturer's proprietary "privacy offerings" pose to the public safety community.

As part of the ongoing transition to AES, the following next steps are underway:

- **Develop an AES transition stakeholder engagement strategy** to increase stakeholders' awareness about the necessary transition to AES. This includes introducing the topic with various stakeholder groups and engagements, developing additional educational materials, repetitive and periodic social media/email awareness campaigns, alerts, and notifications (e.g., CISA cyber-risk notifications), and collaborating with the federal interagency community to address concerns and identifying needs surrounding AES transition and implementations.
- **Encourage SLTT entities to optimize** the use of existing federal grant funding to plan, procure, and implement new or expanded AES services and equipment.[12]
- **Advise states and territories through their Statewide Interoperability Coordinators (SWICs)** and/or State Administrative Agencies to include emergency communications equipment and the AES transition activities of planning, procurements, and implementation into their state/territory cybersecurity grant plans.
- **Coordinate with federal agencies with grant authorities** to establish a multiyear grant program for SLTT entities' AES transitions and the implementation of Link Layer Authentication (for trunked LMR systems) and Link Layer Encryption (when available) services.
- **Ascertain if the recently provided and future cybersecurity grant funding** may be used to support specific SLTT AES transitions.
- **Develop a CISA campaign webpage** and supporting information that public safety stakeholders can access for the latest encryption information, AES transition activities, and LMR cybersecurity alerts.

[12] Any SLTT entity seeking to add an emission designator to or modify an existing emission designator on its license must first obtain a recommendation from an approved frequency coordinator before submitting its application for license to the Federal Communications Commission (FCC).

ANTICIPATED IMPACTS

The following impacts to the public safety community are anticipated to result from an immediate, coordinated, and joint transition to AES.

Enhances critical communications security by improving the secure exchange of critical information and protecting it from criminal groups, non-state actors, foreign adversaries, and other unauthorized persons.

Reduces the monetary and personal cost of mitigation and recovery efforts of information security breaches.

Increases the provision of secure LMR operability and interoperability across all levels of government.

Enables public safety responders and law enforcement personnel at all levels of government the ability to **focus efforts on their primary mission of life safety and security for the nation.**

Improves the support of end-to-end encryption (without transcoding) for wirelessly transmitted information.

Permits the establishment of comprehensive key management cryptoperiods while ceasing the use of static encryption keys that are more easily susceptible to compromise.

Provides encryption longevity. As NIST notes, "even with the impact of quantum computers, AES-128, AES-192, and AES-256 will remain secure for decades to come." [13] Thus, once AES transitions are completed, it is unlikely that public safety agencies will need to move to another encryption algorithm as both AES 192 and AES 256 will still be safe for decades, making the transition cost effective.

[13] Derived from https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs, information to be incorporated into revised SP 800-131A by the end of 2023. Last accessed 9/15/2023.

Immediate, coordinated, and joint transition to AES is essential to ensuring the nation's emergency LMR systems and interoperable communications are secure. Collaboration and coordination across the federal interagency with SLTT agencies are the key to accomplishing this transition in the immediate future and for ensuring that the nation's public safety LMR communications systems are interoperable and protected with robust FIPS 140 2/3 NIST validated AES 256-bit encryption.

ACKNOWLEDGEMENTS

We would like to thank the FPIC Security Subcommittee for their contributions to this document. The FPIC Security Subcommittee includes representatives from federal, state, local, tribal, and territorial government agencies. Special thanks to subject matter experts from the following entities:

- NIST Computer Security Division
- CISA Protective Critical Infrastructure Information Program
- CISA Office of Privacy
- FBI Criminal Justice Information Services Policy Division
- National Council of Statewide Interoperability Coordinators (NCSWIC) Executive Committee
- Emergency Communications Preparedness Center (ECPC) Interoperability Working Group