~~SECRET~~

(1)

Department of Defense
INSTRUCTION

NUMBER S-4660.04
July 27, 2011

ASD(NII)/DoD CIO

SUBJECT: Encryption of Imagery Transmitted by Airborne Systems and Unmanned Aircraft Control Communications (U)

References: (U) See Enclosure 1

1. (U) PURPOSE. This Instruction:

a. (U) Establishes policy, assigns responsibilities, and prescribes procedures for the encryption of unmanned aircraft control communications and wireless data transmissions of still and motion imagery from manned and unmanned airborne platforms, pods, and air and ground terminals that receive still and motion imagery from airborne systems in accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (a)).

b. (U) Incorporates and cancels Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) Directive-Type Memorandum 09-004 (Reference (b)) and ASD(NII)/DoD CIO Cryptographic Methods Memorandum (Reference (c)).

c. (U) Specifies interoperable encryption implementation standard for Unclassified, Secret, and Top Secret wireless transmission of still and motion imagery and unmanned aircraft control communications.

d. (U) Specifies the key management process to support cross-system interoperability between air and ground terminals and airborne systems that transmit or receive still and motion imagery.

2. (U) APPLICABILITY. This Instruction applies to:

a. (U) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD

~~Classified by: Teresa M. Takai, DoD CIO~~
~~Reason: 1.4(g)~~
~~Declassify on: May 1, 2021~~

~~SECRET~~

Components").

b. (U) Air and ground terminals that receive still and motion imagery wirelessly from manned and unmanned airborne systems and pods.

c. (U) Unmanned aircraft control communications.

d. (U) Air and ground control stations that wirelessly transmit or receive still and motion imagery.

3. (U) DEFINITIONS. See Glossary.

4. (U) POLICY. It is DoD policy that:

a. (U) Air and ground terminals that receive still and motion imagery from airborne systems shall be capable of the interoperable methods of encryption specified in sections 1 through 4 of Enclosure 2.

b. (U) Still and motion imagery transmitted wirelessly by airborne systems shall be encrypted as specified in sections 1 through 4 of Enclosure 2.

c. (U) Unmanned aircraft control communications for unmanned aircraft systems (UASs) shall be encrypted by a National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 level 1 or higher encryption method. The unmanned aircraft control communications may be encrypted by a different mode of encryption than the transmitted still and motion imagery. Aircraft control communications of UASs that carry kinetic weapons shall be encrypted with National Security Agency (NSA)/ Central Security Service (CSS) certified Type 1 encryption.

5. (U) RESPONSIBILITIES. See Enclosure 3.

6. (U) PROCEDURES. See Enclosure 2.

7. (U) RELEASABILITY. RESTRICTED. This Instruction is approved for restricted release. Authorized users may obtain copies on the SECRET Internet Protocol Router Network from the DoD Issuances Website at http://www.dtic.smil.mil/whs/directives.

8. (U) EFFECTIVE DATE. This Instruction is effective immediately.

Teresa M. Takai
DoD Chief Information Officer

Enclosures
1. References
2. Procedures
3. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

The content of this enclosure is UNCLASSIFIED.

(a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(b) Directive-Type Memorandum 09-004, "Encryption of Unmanned Aircraft Systems (UAS) Wireless Communications," April 7, 2009 (hereby cancelled)
(c) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer Memorandum, "Cryptographic Methods for the Protection of Unmanned Aircraft Systems (UAS) Wireless Communications," August 6, 2009 (hereby cancelled)
(d) Information Assurance Advisory (IAA) 001-2007, "Potential Implementations and Use of KGV-135A," January 12, 2007[1]
(e) National Institute of Standards and Technology (NIST) Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation" December 2001
(f) Federal Information Processing Standards (FIPS) Publication 197, "Advanced Encryption Standard (AES)," November 26, 2001
(g) Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules, with changes" December 3, 2002
(h) Performance Specification for the Standard Common Data Link (CDL) Waveform, specification 7681990 Rev. H
(i) National Security Agency/Central Security Service Manual 3-16 "Control of Communications Security (COMSEC) Material" August 5, 2005[2]
(j) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004
(k) Chairman of the Joint Chiefs of Staff Instruction 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," December 15, 2008
(l) Joint Concept of Operations for Unmanned Aircraft Systems Second Edition[3]
(m) Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," April 26, 2010

[1] http://www.iad.nsa.smil.mil/resources/library/ia_adv_tech_bulletins_section/index.cfm
[2] http://www.iad.nsa.smil.mil/resources/library/nsa_office_of_policy_section/index.cfm
[3] https://us.jfcom.mil/

ENCLOSURE 2

PROCEDURES (U)

1. (U) SYSTEM INTEROPERABILITY. In order to ensure interoperable encryption of airborne still and motion imagery communications the DoD Components shall only use devices, systems, and technologies in accordance with the following methods:

a. (U) KGV-135A with common data link (CDL) waveforms for Unclassified, Secret, or Top Secret communications implemented in accordance with Information Assurance Advisory 001-2007 (Reference (d)).

(b)(1)

(1) (U) The AES module shall resynchronize automatically if synchronization is lost. For AES implementation in conjunction with CDL equipment use, the AES module shall be self-synchronizing using multiplexer frame synch bits to align the data blocks in accordance with the Performance Specification for the Standard CDL Waveform (Reference (h)).

(2) (U) Figure 2 of Reference (f) defines the bit / byte numbering for the 128-bit block of the AES algorithm. The first bit of serial data shall be stored in the "bit-127" location as shown in Figure 2 of Reference (f).

c. (U) AES for Unclassified non-CDL based systems shall also implement AES as defined in this enclosure.

d. (U) Systems using the KGV-135A or AES shall use NSA/CSS generated keys.

e. (U) As new encryption methods for the transmission and reception of airborne still and motion imagery are approved for implementation by NSA/CSS (commercial or government), they will be considered for inclusion as a standard interoperable encryption method in this Instruction. The DoD will seek to leverage commercial encryption where operationally feasible.

2. (U) UNCLASSIFIED COMMUNICATIONS. DoD Components shall ensure that unclassified airborne still and motion imagery communications and unmanned aircraft control communications products are approved by NSA/CSS, and tested by Joint Interoperability Test Command (JITC) or an approved Service certification process for interoperability. DoD Components shall implement at least one of the following as an interoperable method of encryption for unclassified data:

a. (U) Hardware-Based Encryption. Communications systems may have the KGV-135A encryption module implemented in accordance with subparagraph 1.a. of this enclosure for the encryption of unclassified information. This encryption implementation shall use the NSA/CSS provided KGV-135A encryption module and NSA/CSS provided keys or NSA/CSS approved key sources. The decision to use the KGV-135A encryption module for unclassified communications should be balanced against the need for interoperability, the threat of data interception, and the potential for algorithm compromise.

b. (U) Software-Based Encryption. Communications systems may implement AES in accordance with paragraph 1.b. of this enclosure for the encryption of unclassified information. This encryption implementation shall use NSA/CSS provided AES encryption keys.

3. (U) CLASSIFIED COMMUNICATIONS. DoD Components shall ensure that classified wireless communications implementations are approved by NSA/CSS for secure end-to-end communications. Encryption products, devices, systems, and technologies used to transmit, store, or process classified information shall:

a. (U) Be reviewed and approved by NSA/CSS prior to acquisition and use. In order for a product to be NSA/CSS-approved, the product shall have its implementation, key, key management, concept of operations (CONOPS), and interoperability requirements independently reviewed by NSA/CSS.

b. (U) Use the NSA/CSS Type 1 KGV-135A encryption module with CDL waveforms and keyed for encrypting and decrypting the appropriate level of classified and sensitive national security information.

4. (U) KEY MANAGEMENT. The cryptographic period and supersession rate of each key will be handled on a case-by-case basis by NSA/CSS in coordination with the Combatant Commands, and shall be performed in accordance with NSA/CSS Manual 3-16 (Reference (i)).

5. (U) EXCEPTIONS TO THIS INSTRUCTION

a. (U) Group 1 UAS Exception. Due to size, weight, and power considerations, Group 1 UASs are exempt until the ASD(NII)/DoD CIO and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) determine it is technically and fiscally feasible to implement these encryption requirements.

b. (U) Legacy NSA/CSS Type 1 Encryption Exception. Legacy manned and unmanned systems and pods that implement other NSA/CSS-certified Type 1 products are exempt from using the KGV-135A.

c. (U) Combatant Commanders (CCDRs) Exception. CCDRs may approve exceptions in order to meet operational necessity.

d. (U) Communications Relays Exception. Secondary wireless data links on airborne systems that perform functions other than transmission of still and motion imagery, and UAS control (e.g., data communications relays) may use other means of encryption than those specified in this Instruction.

ENCLOSURE 3

RESPONSIBILITIES (U)

1. (U) ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO shall monitor and provide oversight and policy development for the encryption of wireless airborne still and motion imagery transmitted between air and ground terminals and the encryption of unmanned aircraft control communication.

2. (U) DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO and in addition to the responsibilities in section 5 of this enclosure, shall ensure that the Joint Interoperability Test Command (JITC) performs interoperability testing and provides interoperability certification of devices deployed within the DoD, in accordance with DoDD 4630.05 (Reference (j)) and Chairman of the Joint Chiefs of Staff Instruction 6212.01E (Reference (k)).

3. (U) DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA). The DIRNSA, under the authority, direction, and control of the Under Secretary of Defense for Intelligence and in addition to the responsibilities in section 5 of this enclosure, shall:

a. (U) Provide management and oversight for cryptographic key management to include establishing policy, standards, and approving or providing key management products and services.

b. (U) Determine the cryptographic period and the supersession rate for AES keys and NSA/CSS Type 1 keys in coordination with the CCDRs.

c. (U) Review and approve encryption products, devices, systems, and technologies prior to their acquisition and use.

4. (U) USD(AT&L). The USD(AT&L), in coordination with the ASD(NII)/DoD CIO, shall ensure acquisition compliance with encryption methods and develop a roadmap and implementation timeline for Group 1 UASs, manned Intelligence, Surveillance, and Reconnaissance (ISR) airborne systems, and pods.

5. (U) HEADS OF THE DoD COMPONENTS. The Heads of DoD Components shall:

a. (U) Ensure that all DoD Component airborne systems that transmit still and motion imagery and unmanned aircraft control communications systems comply with this Instruction.

b. (U) Deliver DoD Component joint airborne systems that transmit still and motion imagery and implement interoperable encryption methods in accordance with the requirements of this Instruction.

c. (U) Ensure all products used for the wireless transmission of unclassified still and motion imagery are approved by NSA/CSS, and tested by JITC or an approved Service certification process for interoperability.

d. (U) Ensure all products used for the wireless transmission of classified still and motion imagery are approved by NSA/CSS for secure end-to-end communications.

6. (U) CCDRs. CCDRs shall in addition to the responsibilities in section 5 of this enclosure:

a. (U) Determine their command's cryptographic period and the supersession rate for AES keys and NSA/CSS Type 1 keys, in coordination with the NSA/CSS.

b. (U) Approve exceptions to this Instruction in order to meet operational necessity.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

The entire contents of this Glossary are UNCLASSIFIED

AES	Advanced Encryption Standard
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer
CCDR	Combatant Commander
CDL	common data link
CFB	Cipher Feedback Mode
CONOPS	concept of operations
CSS	Central Security Service
DIRNSA	Director, National Security Agency/Chief Central Security Service
DISA	Defense Information Systems Agency
DoDD	DoD Directive
FIPS	Federal Information Processing Standard
ISR	Intelligence, Surveillance, and Reconnaissance
JITC	Joint Interoperability Test Command
NIST	National Institute of Standards and Technology
NSA	National Security Agency
UAS	unmanned aircraft system
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology & Logistics

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

air and ground terminals. Any devices capable of receiving still and motion imagery wirelessly from an airborne platform.

Group 1 UAS. Classification system for current UASs based primarily on three enduring attributes: unmanned aircraft weight, normal operating altitude, and speed per the Joint Concept of Operations for Unmanned Aircraft Systems (Reference (l)). Group 1 UASs weigh less than 20 pounds and normally operate below 1,200 feet above ground level at speeds less than 250 knots.

NSA/CSS Type 1 Encryption. Defined in Committee on National Security Systems Instruction

No. 4009 (Reference (m)).

pods. Target designating, listening, or watching tools used by aircraft, for identifying targets, guiding precision guided munitions such as laser-guided bombs to their targets, and capturing still and motion imagery.

unmanned aircraft control communications. The communications between an operator and UAS that are used to control the aircraft and payload.