



# Department of Defense **DIRECTIVE**

NUMBER O-5100.19  
November 12, 2014

---

---

USD(I)

SUBJECT: Critical Information Communications (CRITICOMM) System

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues DoD Directive (DoDD) C-5100.19 (Reference (a)) to establish policy and assign responsibilities for the CRITICOMM System in response to the designation of the Secretary of Defense as the U.S. Government Executive Agent to provide for the establishment of communications means that ensure the timely transmission of critical information to senior U.S. Government officials pursuant to Director of Central Intelligence Directive 7/4 (Reference (b)).

b. Designates the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) as the DoD lead for the handling and reporting of critical information (CRITIC) pursuant to References (b) and United States Signal Intelligence Directive (Reference (c)).

2. APPLICABILITY. This directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), 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 (referred to collectively in this directive as the "DoD Components").

3. POLICY. It is DoD policy that:

a. ~~(FOUO)~~ The CRITICOMM System will connect with communications facilities of U.S. Government departments and agencies that are identified in Section 1.3 of Reference (c).

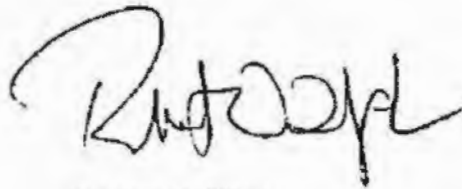
b. CRITIC will be processed and disseminated with a FLASH OVERRIDE priority.

c. The determination as to whether an event must be reported via a CRITIC will be in accordance with the criteria described in Reference (b) and Sections 1.3 and 5.11 of Reference (c).

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Not cleared for public release**. This directive is available to users with Common Access Card authorization on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

6. EFFECTIVE DATE. This directive is effective November 12, 2014.

A handwritten signature in black ink, appearing to read 'R. Work', with a large, stylized initial 'R'.

Robert O. Work  
Deputy Secretary of Defense

Enclosures

1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive C-5100.19, "Critical Information Communications (CRITICOMM) System (U)," June 10, 2008 (hereby cancelled)
- (b) Director of Central Intelligence Directive 7/4, "Critical Information (CRITIC)," January 2, 2001<sup>1</sup>
- (c) United States Signal Intelligence Directive (USSID) CR 1501, Handling of Critical Information, August 13, 2009, as amended<sup>2</sup>
- (d) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)), " November 23, 2005
- (e) DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010
- (f) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," April 22, 2013

---

<sup>1</sup> Available to authorized users at <http://intelshare.intelink.ic.gov/sites/cps/policystrategy/policy/Pages/DCIDs.aspx>

<sup>2</sup> ~~(S)~~ Available to authorized user at <https://www.nsa.ic.gov/producer/ussid/CR1501/ussidCR1501.shtml>

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). In accordance with DoDD 5143.01 (Reference (d)), the USD(I):

a. Oversees management of the CRITICOMM System, including to ensure that communications means are established for the transmission of CRITIC.

b. Consults with the Director of National Intelligence to define Intelligence Community requirements, pursuant to the provisions of Reference (b).

c. Oversees the DIRNSA/CHCSS on CRITICOMM matters, including CRITICOMM operational matters affecting the capability to disseminate CRITIC messages.

2. DIRNSA/CHCSS. In addition to the responsibilities in section 5 of this enclosure, under the authority, direction, and control of the USD(I) and in accordance with DoDD 5100.20 (Reference (e)), the DIRNSA/CHCSS:

(b)(3):P.L. 86-36



3. DoD CHIEF INFORMATION OFFICER (DoD CIO). In accordance with DoDD 5144.02 (Reference (f)), the DoD CIO provides a robust, reliable, and secure communications

infrastructure to support the CRITICOMM System for an uninterrupted level of sustained operations.

4. DIRECTOR, DISA. Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 5 of this enclosure, the Director, DISA:

a. Validates NSA/CSS CRITICOMM circuit requirements in coordination with the DIRNSA/CHCSS and CJCS,.

b. Provides operations and maintenance support for the DoD communications infrastructure.

(b)(3):P.L. 86-36

6. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 5 of this enclosure, the Secretaries of the Military Departments:

a. Provide for the Service-specific manning, training, operating, and equipping of communications facilities that connect with the CRITICOMM System.

b. Include CRITIC message reporting in all appropriate Military Service exercises.

7. CJCS. In addition to the responsibilities in section 5 of this enclosure, the CJCS:

(b)(3):P.L. 86-36

c. Provides for the use of the CRITICOMM Exercise System in CJCS joint training exercises and monitors system performance.

d. Provides guidance to the CCMDs and Military Services to include CRITIC in all joint and Military Service exercises.

8. COMBATANT COMMANDERS (CCDRS). In addition to the responsibilities in section 5 of this enclosure, the CCDRs will include CRITIC in all appropriate CCMD exercises.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CCDR	Combatant Commander
CCMD	Combatant Command
CRITICOMM	Critical Information Communications
DIRNSA/CHCSS	Director National Security Agency/Chief Central Security Service
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
NSA/CSS	National Security Agency/Central Security Service
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this directive.

CRITIC. Defined in Reference (c). CRITIC messages are issued in response to the receipt of intelligence and other information, as described in Annex A of Reference (b).

CRITICOMM. Defined in Reference (c).

FLASH OVERRIDE. In communications, a designation assigned to a message by the originator to indicate to communications personnel the handling and the order in which the message is to be noted. FLASH OVERRIDE cannot be preempted and is considered an “overriding priority” in terms of message traffic precedence. It is a capability available to the President of the United States, the Secretary of Defense, the Joint Chiefs of Staff, the CCDRs when declaring Defense Condition One or Defense Emergency, the United States North American Aerospace Defense Command when declaring either Defense Condition One or Air Defense Emergency, and other national authorities the President may authorize.