



Department of Defense

INSTRUCTION

NUMBER 5240.25
March 30, 2012

USD(I)

SUBJECT: Counterintelligence Badges and Credentials

References: See Enclosure 1

1. **PURPOSE.** This Instruction establishes policy, assigns responsibilities, and provides procedures for issuance of counterintelligence (CI) badges and credentials to civilian and military personnel conducting authorized CI activities pursuant to the authority in DoD Directive (DoDD) 5143.01 (Reference (a)) and DoDD O-5240.02 (Reference (b)).

2. **APPLICABILITY.** This Instruction:

a. Applies to 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 Components”).

b. Does not apply to the Military Department Counterintelligence Organizations (MDCOs), i.e., Army CI, the Naval Criminal Investigative Service, or the Air Force Office of Special Investigations. This Instruction also does not apply to CI personnel under command of the Director of Intelligence, Headquarters Marine Corps.

3. **DEFINITIONS.** See Glossary.

4. **POLICY.** It is DoD policy that:

a. If issued, CI badges and credentials shall be provided only to personnel who are trained to conduct CI activities in accordance with DoD Instruction (DoDI) 3305.11 (Reference (c)).

b. DoD contractor personnel shall not be issued badges. DoD contractor credentials shall identify the bearer as a contractor.

c. CI badges and credentials shall be presented only in the performance of authorized CI activities.

d. Badges and credentials shall be issued by a designated component authority who is a member of the Senior Executive Service or a general or flag officer.

e. CI badges and credentials shall be controlled and accountable in accordance with Enclosure 3.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE

a. This Instruction is effective upon its publication to the DoD Issuances Website.

b. If the Instruction is not otherwise reissued or cancelled in accordance with DoD Instruction 5025.01 (Reference (d)), it will expire effective March 30, 2022 and be removed from the DoD Issuances Website.



Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (b) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007
- (c) DoD Instruction 3305.11, "DoD Counterintelligence (CI) Training," March 19, 2007
- (d) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
- (e) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," February 2, 2009
- (f) DoD Instruction S-5240.09, "Offensive Counterintelligence Operations (OFCO) (U),"
October 29, 2008
- (g) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that
Affect United States Persons," December 1, 1982
- (h) Sections 499, 506, and 701 of title 18, United States Code
- (i) DoD Directive 5210.56, "Carrying of Firearms and the Use of Force by DoD Personnel
Engaged in Security, Law and Order, or Counterintelligence Activities," April 1, 2011
- (j) Directive-Type Memorandum 08-052, "DoD Guidance for Reporting Questionable
Intelligence Activities and Significant or Highly Sensitive Matters," June 17, 2009
- (k) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR),"
May 17, 2011

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall serve as the OSD Principal Staff Assistant and advisor to the Secretary of Defense regarding CI badge and credential policy.

2. DEPUTY UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (DUSD(I&S)). The DUSD(I&S), under the authority, direction, and control of the USD(I), shall:

a. Develop and recommend CI badge and credential policy that is covered by this Instruction.

b. Oversee DoD Component compliance with the CI badge and credential policy.

3. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE CENTER (DCHC). The Director, DCHC, under the authority, direction, and control of the Director, Defense Intelligence Agency, shall in coordination with the DoD Components, develop guidelines and procedures to report lost or stolen CI badges and credentials that are covered by this Instruction.

4. HEADS OF THE DOD COMPONENTS. The Heads of the DoD Components shall develop procedures for the issuance, accountability, and use of CI badges and credentials.

ENCLOSURE 3

PROCEDURES

1. GENERAL

a. Only certain DoD organizations and personnel are authorized to conduct CI investigations and operations, in accordance with DoDI 5240.04 and DoDI S-5240.09 (References (e) and (f)).

b. CI personnel subject to this Instruction may also provide support to DoD organizations authorized to conduct CI investigations and operations in accordance with References (e), (f), and DoD 5240.1-R (Reference (g)).

2. ISSUANCE AND ACCOUNTABILITY OF BADGES AND CREDENTIALS

a. The issuing DoD Component shall maintain a list of personnel issued CI badges and credentials.

b. The issuing DoD Component shall conduct, at a minimum, an annual physical inventory of badges and credentials.

c. The DoD Component office with oversight responsibility for a DoD Component's CI activities shall inspect badges and credentials in accordance with the DoD Component's internal policy and procedures.

d. CI personnel shall sign a receipt for their badge and credentials. At a minimum, the issuing DoD Component shall maintain the receipt for the duration of the recipient's employment.

3. BADGES. Badges shall contain:

a. Embossed sequential serial numbers based on order of issuance.

b. The official seal or emblem of the issuing DoD Component or the DoD official seal.

c. Title of the bearer, ensuring the title or position of the bearer does not imply unauthorized authorities or duties described in paragraph 4.h. of this enclosure.

4. CREDENTIALS. Credentials shall contain:

a. The official seal or emblem of the issuing DoD Component.

b. Security features to prevent unlawful and or malicious duplication.

- c. Embossed sequential serial numbers based on order of issuance.
- d. The name and title of the bearer, CI element of the component, a passport-size photograph of the bearer, signature of the bearer, and signature of the issuing authority.
- e. Instructions on the back of the credential as to where and how to return if found.
- f. A statement on the back of the credential that unauthorized use or possession by any individual is subject to penalties according to sections 499, 506, and 701 of title 18, United States Code (Reference (h)).
- g. Language to describe the bearer's authorized CI activities. Figures 1 and 2 provide examples of the appropriate credential language.

Figure 1. Example 1 of Credential Language

NAME OF BEARER
CI Representative, Agent, Officer, Professional, or Contractor (title as applicable)

Is authorized to conduct official business in furtherance of the counterintelligence responsibilities and mission of the (insert agency name) and is authorized in accordance with DoD Directive 5240.02 to gather information on behalf of the aforementioned agency.

Figure 2. Example 2 of Credential Language

NAME OF BEARER
CI Representative, Agent, Officer, Professional, or Contractor (title as applicable)

This credential certifies that the bearer is a counterintelligence representative with the (insert agency name), and is conducting official business in accordance with DoD Directive 5240.02.

- h. No language implying or inferring that the bearer has the authority to investigate criminal violations of law, conduct CI investigations, conduct CI operations, or carry weapons, in accordance with authorities in References (b), (e), (f), and DoDD 5210.56 (Reference (i)).

5. LOSS, DAMAGE, COMPROMISE, MISUSE, OR THEFT

a. DoD Components shall conduct an administrative-type inquiry to determine the facts surrounding the loss, damage, compromise, misuse, or theft of CI badges and credentials. Information that indicates the loss was caused by a criminal act shall be referred to the appropriate law enforcement (LE) authority.

b. If the loss, compromise, misuse, or theft of CI badges or credentials was caused by employee misconduct as described in Procedure 14 of Reference (g), DoD Components shall report the incident to the Assistant to the Secretary of Defense For Intelligence Oversight (ATSD(IO)) through established procedures and appropriate intelligence component General Counsel or IG under Procedure 15 of Reference (g). If information indicates that loss, damage, compromise, misuse, or theft of CI badges or credentials meets the criteria established in DTM 08-052 (Reference (j)) for the identification, investigation, and reporting of significant or highly sensitive matters, report the incident to the ATSD(IO) immediately.

c. Personnel who lose their CI badges or credentials shall notify their chain-of-command or supervisory channels within 24 hours. Supervisors shall notify DCHC and the appropriate U.S. LE authority of the loss. This notification affords the loss to be entered into the National Crime Information Center database as stolen or missing Government property.

d. Any misuse of badges and credentials may be a violation of law, policy, or component guidance. Misuse of CI badges and credentials includes, but is not limited to:

- (1) Misrepresenting the bearer as an LE officer.
- (2) Misrepresenting that the bearer has the authority to investigate criminal violations of law, conduct CI investigations, or conduct CI offensive operations.
- (3) Falsifying, forging, changing, photographing or copying, or tampering with CI badges and credentials.
- (4) Using CI badges and credentials to represent oneself beyond the issuing organization's authorized CI activities.
- (5) Using CI badges and credentials to gain unnecessary or unauthorized access to information, facilities, or persons, even when done in the performance of authorized activities and duties.
- (6) Using CI badges and credentials as identification when not performing official duties related to authorized CI activities; for example, in place of appropriate personal identification or in place of other Government identification.
- (7) Using CI badges and credentials in an attempt to avoid personal liability or civil citations, such as traffic or parking violations.
- (8) Using CI badges and credentials to obtain discounted or free products or services.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ATSD(IO)	Assistant to the Secretary of Defense for Intelligence Oversight
CI	counterintelligence
DCHC	Defense Counterintelligence and Human Intelligence Center
DoDD	DoD Directive
DoDI	DoD Instruction
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
LE	law enforcement
MDCO	Military Department Counterintelligence Organization
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

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

badge. A distinctive official device usually made of cast metal, which is provided by the DoD Component and worn or carried by the bearer as a sign of authority.

CI activities. Defined in Reference (b).

CI investigation. Defined in Reference (e).

CI operation. Defined in Reference (f).

credentials. An official document or set of documents presenting evidence of the identity, authority, and status of the bearer and for use in conducting authorized CI activities.

MDCOs. Defined in DoDD 5240.06 (Reference (k)).