



INTELLIGENCE

UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

April 25, 2013

*Incorporating Change 3, Effective November 20, 2015*

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Directive-type Memorandum (DTM) 13-005, "Deviations from the DoD Physical Security Program"

References: See Attachment 1

Purpose. This DTM, in accordance with DoD Directive (DoDD) 5143.01 (Reference (a)):

- Establishes the responsibilities and procedures for granting deviations to the DoD Physical Security Program as outlined in DoD Instruction (DoDI) 5200.08 (Reference (b)), DoD 5200.08-R (Reference (c)), and DTM 09-012 (Reference (d)).
- This DTM is effective April 25, 2013; it will be incorporated into Reference (c). This DTM will expire effective October 25, ~~2015~~ 2016.

Applicability.

- This DTM 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").

Definitions. See Glossary.

Policy. In accordance with Reference (b), it is DoD policy that:

- Deviations from the standards for physical security of DoD installations, property, and personnel established in Reference (b) will be allowed only in accordance with the guidance in Attachment 2 to this DTM.
- DoD installations, property, and personnel will be protected and applicable laws and regulations will be enforced. Physical security measures required by law, Executive order, or presidential directive are not subject to deviation.

- Appropriate security measures will be implemented to protect DoD property and personnel assigned, attached, or subject to the control of the DoD Components.
- Combatant Commands may not reduce DoD Component or Military Service-specific physical security standards without coordination and approval from the custodial department or agency consistent with Reference (b).

### Responsibilities

- Under Secretary of Defense for Intelligence (USD(I)). The USD(I), in accordance with References (a) and (b), must establish policy, assign responsibilities, and develop procedures for the DoD Physical Security Program.
- Heads of the DoD Components. The Heads of the DoD Components must:
  - Establish and document a deviation program that remediates all deviations as quickly as possible and provides a means to review, monitor, plan, and program for corrections to situations when physical security minimum standards are not met.
  - Specify appropriate levels of review and approval for deviation requests.
  - Review requests for deviations to minimum physical security standards. Deviations from physical security measures that would effectively alter or undermine the standards in the DoD antiterrorism program, in accordance with DoDI 2000.12 and DoDI 2000.16 (References (e) and (f)), must be coordinated and approved by the affected Geographic Combatant Commander.
  - Deviations from minimum physical security standards due to special events or circumstances of limited duration remain the responsibility of the Head of the DoD Component, as identified in Reference (b).

Procedures. See Attachment 2.

Releasability. UNLIMITED. This DTM is approved for public release and is available on the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.



Michael G. Vickers  
Under Secretary of Defense for Intelligence

Attachments:  
As stated

**DISTRIBUTION:**

**SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DEPUTY CHIEF MANAGEMENT OFFICER  
COMMANDERS OF THE COMBATANT COMMANDS  
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
ASSISTANT SECRETARIES OF DEFENSE  
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTOR, NET ASSESSMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DoD FIELD ACTIVITIES**

ATTACHMENT 1

REFERENCES

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),  
November 23, 2005
- (b) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD  
Physical Security Review Board (PSRB)," December 10, 2005, as amended
- (c) DoD 5200.08-R, "Physical Security Program," April 9, 2007
- (d) Directive-type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access  
Control," December 8, 2009
- (e) DoD Instruction 2000.12, "DoD Antiterrorism (AT) Program," March 1, 2012
- (f) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006, as  
amended
- (g) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
- (h) DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of  
Classified Information," February 24, 2012, as amended
- (i) DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1,  
2012, as amended

ATTACHMENT 2

DEVIATION PROGRAM

1. GENERAL. Deviation programs provide a management tool for Heads of DoD Components to review, monitor, plan, and program for corrections to deviations from physical security standards impacting DoD assets or resources over which they have controlling authority and responsibility.

a. Physical security standards that cannot be met must be identified to the Head of the DoD Component, as delegated.

b. For deficiencies that can be corrected within 90 days of finding a problem, a formal request for deviation is not required. Components are required to notify the deviation approving authority and compensate for the vulnerability until corrected.

c. This DTM authorizes deviation from minimum physical security standards applicable to DoD installations and the protection of DoD assets or resources normally found on DoD installations. See Reference (c) for those unique DoD assets or resources having separate guidance.

2. CATEGORIES OF DEVIATIONS. Approving authorities will categorize deviations from Office of the USD(I) and DoD Component physical security policy as waivers, limited exceptions, or permanent exceptions, or other terms that have the same definitions as these terms.

a. Waivers

(1) Installation commanders or facility directors must request a waiver when compliance with a prescribed minimum standard is not currently achievable, and the deficiency is not correctable within 90 days, but can be corrected within 1-year.

(2) The approving authority must formally review waivers every 9 months and document progress made to correct the waived deficiency.

(3) If security standards or the situation affecting the security of the DoD assets or resources changes, another deviation request must be submitted.

(4) Submitted and approved waiver requests must be retained on file, to include periodic reviews of waivers, in accordance with DoDD 5015.2 (Reference (g)).

b. Limited Exceptions

(1) Installation commanders or facility directors must request a limited exception when compliance with a prescribed minimum standard is not currently achievable, and the deficiency is correctable within 3 years.

(2) Limited exceptions are granted when:

(a) Corrective action of a security deficiency is beyond the capability of the organization; or

(b) The deficiency can be corrected within 3 years.

(3) The approving authority will formally review limited exceptions every 12 months and document progress made to correct the deviation.

(4) If security standards or the situation affecting the security of the DoD assets or resources changes, another deviation request must be submitted.

(5) Submitted and approved limited exceptions requests must be retained on file, to include annual reviews of limited exceptions, in accordance with Reference (g).

c. Permanent Exceptions

(1) Installation commanders or facility directors must request a permanent exception when conditions are such that compliance with a prescribed minimum standard is not currently achievable, and is not correctable in 3 or more years. Justification must clearly explain why the standard cannot be met and why correcting the deviation is adjudged not to be feasible or cost-effective after a most careful and critical evaluation of the facts.

(2) Deviations approved as permanent exceptions require compensatory measures.

(3) Permanent exceptions, once formally approved, will be incorporated into security plans. If a security standard or situation affecting the security of the DoD assets or resources changes, another deviation request must be submitted.

(4) Submitted and approved permanent exceptions requests must be retained on file, to include annual reviews of permanent exceptions, in accordance with Reference (g).

3. COMPENSATORY MEASURES

a. Compensatory measures are required for each deviation in effect. A single compensatory measure may be applied for more than one deviation.

b. Acceptable compensatory measures must mitigate or compensate for vulnerabilities created by the inability to achieve a minimum physical security standard.

c. Compensatory measures must be designed to compensate for the specific vulnerability created by the deficiency, and must provide an equivalent or greater level of protection as the standard for which the deviation was granted.

d. Compensatory measures must go above and beyond routine security measures already required or in place at the site. Security forces, facilities, equipment, and procedures that are already required and in place to meet minimum standards are not normally adequate as compensatory measures. However, use of existing DoD assets or resources in a new way to provide protection for a deviation may constitute compensatory measures as long as their use does not create vulnerabilities in other areas.

e. Instructions consisting of non-specific orders such as “increase vigilance” are inadequate as compensatory measures.

f. Compensatory measures must be implemented immediately upon detection of vulnerability and shall not be delayed pending consideration of a deviation request.

#### 4. REVIEW AND APPROVAL OF DEVIATION REQUESTS

a. Requests for deviations from specific requirements will be submitted as directed by the Head of the DoD Component.

b. Different levels of deviation request approvals may be delegated according to levels of protection required to meet physical security standards, except for permanent exceptions.

c. The approving authority must carefully weigh all factors, to include potential value of physical security measures during wartime or contingency operations.

d. The approving authority must review each deviation to ensure adequate compensatory measures have been identified and can be implemented, and will determine the appropriate document handling, marking or classification designation consistent with applicable security classification guides. All deviation requests containing classified information must contain the required security classification markings in accordance with DoD Manual 5200.01, Volume 2 (Reference (h)).

e. When considering a deviation request for a particular installation or facility, the approving authority must review all other approved deviations currently in effect for that installation or facility. This review is to ensure that, collectively, the deviations do not establish an overall site vulnerability greater than the designated compensatory measures.

f. Each deviation must be evaluated and approved on a case-by-case basis. Blanket approvals for deviations are not allowed.

g. Any forms or memoranda used to approve deviations must be signed by the approving authority.

## 5. DEVIATION DOCUMENTATION

a. DoD Components will make available approved waivers, permanent exceptions or exceptions during periodic Defense Security Enterprise (DSE) Executive Committee (ExCom) and DSE ExCom-related meetings consistent with DoDD 5200.43 (Reference (i)).

b. All installation commander and facility director requests, extensions, and approvals of deviations from physical security requirements must:

(1) Be prepared in writing and forwarded through the DoD Component for review and approval, if appropriate.

(2) Have a unique alphanumeric code for tracking its status.

(a) The code must indicate:

1. The requesting DoD Component.

2. Initial year of the deviation.

3. Whether the deviation is a waiver or permanent exception.

4. Additional code to distinguish it from all other waivers or exceptions, as appropriate, issued in the same year.

(b) Requests for deviation extensions must use the same code.

(3) Be submitted and documented at a classification level appropriate to its associated vulnerability.

c. Documentation for each deviation must reflect:

(1) The specific name and address of the installation, facility, or site involved to include facility or building number.

(2) Month and year of issue of the initial deviation.

(3) Month and year of issue of each deviation extension.

(4) Name and contact information for the approving official.



- (5) Current status (e.g., under review, approved through a specified date, denied).
- (6) Specific description of condition(s) that cause the need for the deviation and reason(s) why applicable standards cannot be met.
- (7) Detailed description of the impact on mission and any problems that will interfere with safety or operating requirements if the deviation request is not approved.
- (8) Detailed results of risk assessments based on evaluations of threat, vulnerability, and consequence associated with being granted a deviation from a minimum physical security standard.
- (9) Complete description of the compensatory measures applied, and detailed explanations of how the compensatory measures mitigate risk.
- (10) Actions initiated or planned to eliminate the need for the deviation and the estimated time to complete, to include the organization's plan of action and milestones.
- (11) Assets or resources, including estimated cost, as defined by the DoD Component, to eliminate the need for the deviation.
- (12) Deviation expiration date in the absence of an official extension.

## GLOSSARY

### PART I. ABBREVIATIONS AND ACRONYMS

DoDD	DoD Directive
DoDI	DoD Instruction
DSE	Defense Security Enterprise
DTM	Directive-type Memorandum
ExCom	Executive Committee
USD(I)	Under Secretary of Defense for Intelligence

### PART II. DEFINITIONS

These terms and their definitions are for the purposes of this DTM.

compensatory measure. An action or condition that mitigates or compensates for vulnerabilities created by the inability to achieve a minimum physical security standard. Examples of compensatory measures include, but are not limited to, such physical security measures as additional security forces, security procedures, and physical security equipment or devices such as locks, intrusion detection systems, lighting, barricades, alarms, and anti-intrusion devices.

concern. An existing condition that is exploitable and can directly or indirectly lead to the injury or death of DoD personnel or damage or compromise of DoD assets or resources.

deviation. Inability to achieve compliance with a minimum physical security standard for facilities, equipment, and procedures either combined or individually.

limited exception. Approval of a long term deviation from minimum physical security standards due to a security condition that can be corrected within 3 years.

permanent exception. Approval of a permanent deviation from minimum physical security standards that cannot be corrected in 3 years or more.

vulnerability. A situation or circumstance, which left unchanged, may result in the degradation of physical security, injury or death of DoD personnel, or damage or compromise of DoD assets or resources.

waiver. Approval of a short term deviation from minimum physical security standards due to a security condition that cannot be corrected within 90 days, but can be corrected within 1 year.