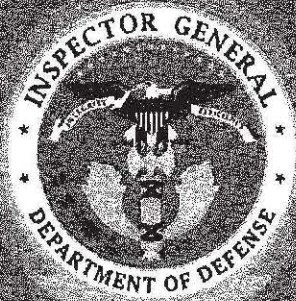


CONFIDENTIAL

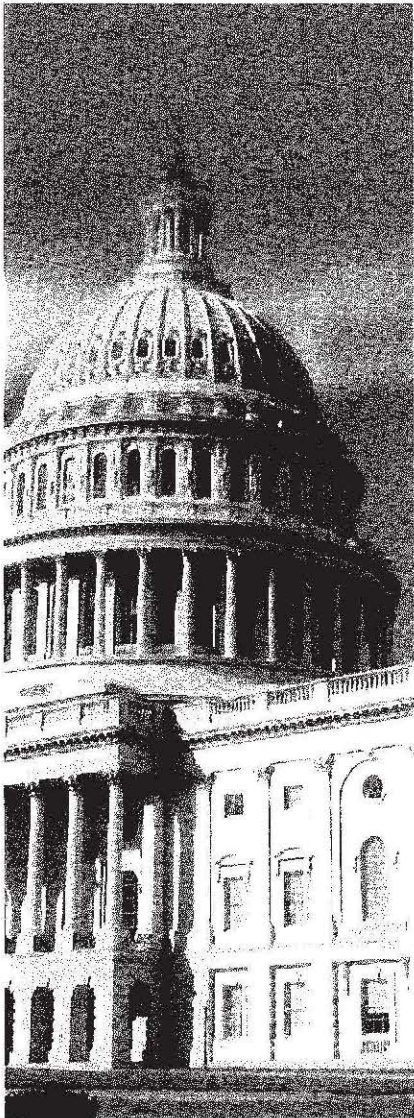
Report No. DDPMG 2015-010



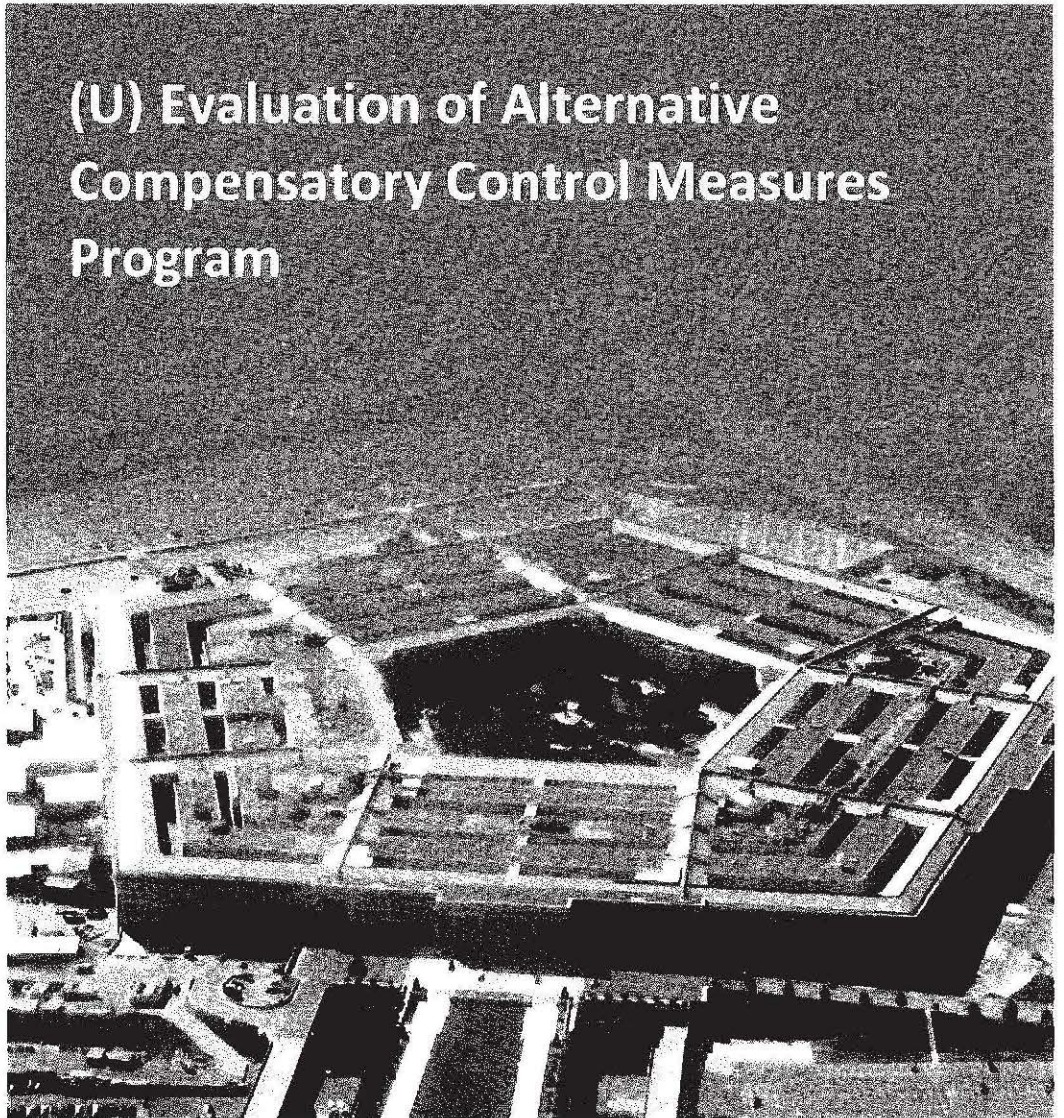
INSPECTOR GENERAL

U.S. Department of Defense

January 27, 2015



(U) Evaluation of Alternative Compensatory Control Measures Program



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Classified by: Anthony C. Thomas, Deputy Inspector General for

Intelligence and Special Program Assessments

Derived from: CIGSM 3213.02A, Joint Staff Focal Point

Communications Procedures Manual (U)

Declassify on: 20400127

CONFIDENTIAL

~~CONFIDENTIAL~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline

For more information about whistleblower protection, please see the inside back cover.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

JAN 27 2015

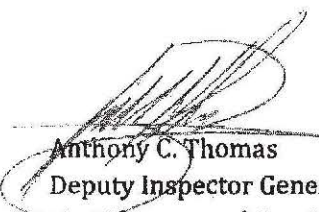
MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY

SUBJECT: (U) Evaluation of Alternative Compensatory Control Measures Program
(Report No. DODIG-2015-070)

(U) We are providing this final report for your information and use. We conducted an evaluation of DoD's Alternative Compensatory Control Measures (ACCM) program. We conducted this evaluation in accordance with the Council of the Inspectors General Quality Standards for Inspection and Evaluation. We found that DoD's ACCM program lacked effective oversight and that the program guidance lacked detail.

(U) We considered management comments on a draft of this report when preparing the final report. Although your office did not comment on the report or findings themselves, nor did it specifically state "concur" or "non-concur," the plan of action or milestones provided in the comments met the intent of each recommendation and we considered them responsive.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 882-DoD OIG (U) (DSN 499-DoD OIG (U)) If you desire, we will provide a formal briefing on the results.


Anthony C. Thomas
Deputy Inspector General for
Intelligence and Special
Program Assessments

~~CONFIDENTIAL~~

(This page is UNCLASSIFIED when separated from the evaluation.)



Results in Brief

Evaluation of Alternative Compensatory Control Measures Program (Report No. DODIG-2015-070)

January 27, 2015

(U) Objective

(U//~~FOUO~~) Our objective was to evaluate Alternative Compensatory Control Measures (ACCM) program establishment and maintenance processes, structure, and use in accordance with DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information"; then-Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, April 18, 2003, "Revised Alternative Compensatory Control Measures (ACCM) Guidance"; and Chairman, Joint Chiefs of Staff Manual 3213.02A, "Joint Staff Focal Point Communications Procedures Manual."

(U//~~FOUO~~) We announced the evaluation on October 15, 2013. During initial field work, we determined that a more in-depth approach was necessary. Therefore, on February 5, 2014, we reissued the announcement letter and data call with expanded distribution to the Service Secretaries; the Chairman, Joint Chiefs of

Staff; the Under Secretary of Defense for Intelligence; the combatant commanders; and the Directors of the Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency.

(U) Findings

(U) We found that:

- (U) DoD ACCM programs lacked effective oversight;
- (U) ACCM guidance lacked detail;
- (U) DoD had no centralized system for ACCM program management or a centralized tracking system for ACCM access;
- (U) DoD did not provide standardized ACCM training; and
- (U) DoD did not provide a yearly ACCM report to Congress.

(U) Recommendations

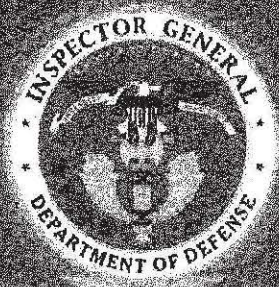
(U) We recommend that the Under Secretary of Defense for Policy, as the staff proponent for ACCM program management, oversight, and reporting:

- (U//~~FOUO~~) Develop a plan of assistance, oversight, and inspections of the components' ACCM programs;
- (U//~~FOUO~~) Revise DoD Manual 5200.01, Volume 3, to include additional definitions, guidance, requirements, formats, and rules for the ACCM program;
- (U//~~FOUO~~) Develop a centralized database of ACCM programs along with users' need-to-know and access status;
- (U//~~FOUO~~) Develop a standard initial ACCM training program; and
- (U//~~FOUO~~) Obtain written legal advice regarding reporting of ACCM program status to Congress.

Visit us at www.dodig.mil

DODIG-2015-07001

CONFIDENTIAL



Results in Brief (cont'd)

*Evaluation of Alternative Compensatory Control Measures
Program (Report No. DODIG-2015-070)*

(U) Management Comments and Our Response

(U) We considered a response from the Office of the Under Secretary of Defense for Policy in preparing the final report. Although OUSD(P) did not comment on the report or findings themselves, nor did they specifically state "concur" or "non-concur," their plan of action or milestones provided in their comments met the intent of each recommendation and we considered them responsive.

DODIG-2015-070

CONFIDENTIAL

~~CONFIDENTIAL~~

Recommendations Table

Management	Recommendations Requiring Comment
Under Secretary of Defense for Policy	A, B, C, D, E

~~CONFIDENTIAL~~

Contents

(U) Introduction	1
(U) Objective.....	1
(U) Background.....	1
(U) Review of Internal Controls	4
(U) Finding A	5
(U) DoD Alternative Compensatory Control Measures Programs Had No Effective Oversight	5
(U) Office of the Under Secretary of Defense for Policy Oversight.....	5
(U) Office of the Under Secretary of Defense for Intelligence Oversight	6
(U) Joint Staff Oversight	7
(U) Internal/Command Oversight.....	8
(U) Services	8
(U) Combat Support Agencies	9
(U) U.S. Central Command.....	9
(U) U.S. Special Operations Command	9
(U) Conclusion	10
(U) Recommendation, Management Comments, and Our Response	11
(U) Finding B.....	12
(U) Alternative Compensatory Control Measures Guidance Lacked Detail.....	12
(U) DoD Manual 5200.01, Volume 3	12
(U) Chairman, Joint Chiefs of Staff Manual 3213.02A.....	13
(U) Guidance Lacking	14
(U) Formats Lacking	15
(U) Conclusion	16
(U) Recommendation, Management Comments, and Our Response	17
(U) Finding C	18
(U) DoD Did Not Have a Centralized Alternative Compensatory Control Measures Access Tracking or Program Management System	18
(U) Centralized Access Tracking.....	18
(U) Centralized Management of Alternative Compensatory Control Measures Programs	20
(U) Conclusion	20

~~CONFIDENTIAL~~

(U) Recommendation, Management Comments, and Our Response	20
(U) Finding D	22
(U) DoD Did Not Have Standardized Alternative Compensatory Control Measures Program Training.....	22
(U) Recommendation, Management Comments, and Our Response	22
(U) Finding E	24
(U) DoD Did Not Provide a Yearly Alternative Compensatory Control Measures Program Report to Congress	24
(U) Conclusion	25
(U) Recommendation, Management Comments, and Our Response	25
(U) Appendix A	27
(U) Scope and Methodology	27
(U) Prior Coverage	27
(U) Appendix B	28
(U) Office of the Under Secretary of Defense for Policy Comments	28
(U) Acronyms and Abbreviations	34

~~CONFIDENTIAL~~

(U) Introduction

(U) Objective

(U//~~FOUO~~) Our objective was to evaluate Alternative Compensatory Control Measures (ACCM) program establishment and maintenance processes, structure, and use in accordance with DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information"; then-Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD(C3I))* Memo, April 18, 2003, "Revised Alternative Compensatory Control Measures (ACCM) Guidance"; and Chairman, Joint Chiefs of Staff Manual (CJCSM) 3213.02A, "Joint Staff Focal Point Communications Procedures Manual." The data, plans, and operations protected by the ACCM programs were beyond this evaluation's scope.

(U) Background

(U//~~FOUO~~) We announced our evaluation and issued a data call to the Under Secretary of Defense for Policy (USD(P)) on October 15, 2013. We initially planned to focus on Office of the Secretary of Defense elements; however, during initial field work, we determined that a more in-depth approach was necessary. Therefore, on February 5, 2014, we reissued the announcement letter and data call with expanded distribution to the Service Secretaries; the Chairman, Joint Chiefs of Staff (CJCS); the Under Secretary of Defense for Intelligence (USD(I)); the combatant commanders; and the Directors of the Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency.

* (U) Before 2003, overall intelligence management in DoD was the responsibility of the Deputy Secretary of Defense (DEPSECDEF) and the ASD(C3I). On December 2, 2002, Public Law 107-314 authorized creation of the position of Under Secretary of Defense for Intelligence (USD(I)). On May 8, 2003, the USD(I) took over as the principal staff assistant and advisor to the Secretary of Defense and the DEPSECDEF on intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. USD(I) was the top intelligence official in DoD, and managed the Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, and National Reconnaissance Office, as well as the military service intelligence components.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

2000-01-01-0000

(U//~~FOUO~~) The ACCM program was a protection method used to assist in enforcing strict need-to-know when a DoD component head determined that normal security measures were insufficient but Special Access Program (SAP) or Sensitive Compartmented Information (SCI) protections were not warranted. The ACCM program could be characterized as an extra security wrapper around a protected operation, plan, or data. The Office of the Under Secretary of Defense for Policy (OUSD(P)) provided no information as to when DoD's ACCM program was created, but it was in use at least as early as January 1997, when DoDM 5200.1-R, "Information Security Program" was published. That manual contained two pages of general guidance on the requirements and prohibitions of ACCM use. We were told that prior to the late 1990s, DoD ACCMs were not well-regulated, but were handled similar to SAPs. ACCM procedures were reportedly "tightened up" by the then-ASD(C3I) after the contents of a 2002 or 2003 classified briefing on the then-potential invasion of Iraq were revealed in the Washington Post. On April 18, 2003, then-ASD(C3I) issued a memorandum, "Revised Alternative Compensatory Control Measures (ACCM) Guidance." The memo stated that, at the direction of Congress, security policy and procedures pertaining to the ACCM program had been revised to clarify the appropriate use for protecting classified information. The memo also stated that the revised guidance would be issued in a forthcoming revision to the regulation.

(U) DoDM 5200.01-V3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, incorporating Change 1, March 21, 2012, was the governing document for the ACCM program. That document required that the cognizant DoD Component Head approve in writing an ACCM program and include the following information:

- (U) Unclassified nickname;
- (U) Designation of the ACCM sponsor;
- (U) Designation of an ACCM control officer;

2000-01-01-0000

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U//~~FOUO~~) According to DoDM 5200.01-V3, the DoD staff proponent for ACCM management, oversight, and congressional reporting was OUSD(P), and the staff proponent for ACCM security policy was the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). An OUSD(P) official told us that more than 70 ACCMs were in DoD. The official also said that OSD: (b)(5)

[REDACTED]

[REDACTED]

(U) Review of Internal Controls

(U) Other than as explained in the text of this report, evaluation of internal controls was beyond the scope of this project.

~~CONFIDENTIAL~~

(U) Finding A

(U) DoD Alternative Compensatory Control Measures Programs Had No Effective Oversight

(U//~~FOUO~~) OUSD(P) did not maintain an effective oversight program for the DoD ACCM program. In spite of the DoD requirements set out in DoDM 5200.01-V3, OUSD(P) did not fully exercise administrative oversight, perform routine inspections, or assist component users of the DoD ACCM program. Although the ACCM program achieved its primary goal -- putting a security wrapper around planning operations -- the reporting and oversight of the ACCM program was lacking.

(U) Office of the Under Secretary of Defense for Policy Oversight

(U//~~FOUO~~) Data calls produced no records of OUSD(P) inspections, training, or component documentation. A senior OUSD(P) official said that ~~OSD: (b)(5)~~

~~OSD: (b)(5)~~
~~OSD: (b)(5)~~
~~OSD: (b)(5)~~
~~OSD: (b)(5)~~. Another senior OUSD(P) official said that ~~OSD: (b)(5)~~
~~OSD: (b)(5)~~
~~OSD: (b)(5)~~

(U//~~FOUO~~) In our data call to OUSD(P), we asked for program documents from each of DoD's ACCM programs. OUSD(P) provided only 12 documents of ACCM-related

~~CONFIDENTIAL~~

Findings A

information. A senior OUSD(P) official stated that OSD: (b)(5)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. According to another OUSD(P) official, OSD: (b)(5)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. A senior official said that OSD: (b)(5)

[REDACTED]
[REDACTED]. However, OUSD(P) provided none of those documents in response to our data call. A senior OUSD(P) official stated that OSD: (b)(5)

[REDACTED]
[REDACTED]. The official said that OUSD(P) was the designated office for oversight of DoD ACCMs, but OSD: (b)(5)

[REDACTED]
According to the official, OSD: (b)(5)

[REDACTED] As a result, OUSD(P) maintained minimal administrative oversight and no operational oversight of DoD's ACCM programs. ACCM and Focal Point managers at the combatant commands and staff elements said that their ACCM programs had never been inspected by OUSD(P), their office lacked any regular interaction with OUSD(P), and one manager would not even know who to call at OUSD(P) if the office had an ACCM-specific question.

(U) Office of the Under Secretary of Defense for Intelligence Oversight

(U//FOUO) According to an Office of the Under Secretary of Defense for Intelligence (OUSD(I)) representative, oversight of all ACCM programs was provided by OUSD(P),

06-05-2012 10:06

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Findings

which distributed a yearly data call for ACCM information and compiled responses from all of the components. OUSD(I)'s function in the overall ACCM program was involved primarily with security. Beyond DoDM 5200.01-V3, OUSD(I) provided the components with best practices, tools, and recommendations.

(U//~~FOUO~~) According to a senior OUSD(I) official, OSD: (b)(5)

OSD: (b)(5). The senior OUSD(I) official said that OSD: (b)(5)

OSD: (b)(5). The senior OUSD(I) official added that OSD: (b)(5)

OSD: (b)(5). In addition, the official said that ACCMs were being executed, but neither OUSD(P) nor OUSD(I) had performed any oversight.

(U) Joint Staff Oversight

(U//~~FOUO~~) The Joint Staff only provided management or oversight to the Focal Point programs that it owned. However, the Joint Staff also provided staff assistance, when requested by the combatant commands (COCOMs), for both Focal Point and non-Focal Point ACCM programs. The Joint Staff had a rigorous process for managing Focal Point programs; however, in the opinion of some COCOMs, the Joint Staff did not perform oversight.

(U//~~FOUO~~) CJCSM 3213.02A governed the Joint Staff Focal Point program. The manual directed that the COCOMs' Focal Point offices perform internal oversight of ACCM/Focal Point programs. The Joint Staff Management Office performed external oversight. The Joint Staff Special Access Program Central Office (SAPCO) office visited the COCOMs yearly to inspect their SAP programs; at that time, they also reviewed the Focal Point

4-151-40 (1) 07017

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

programs. The Joint Staff SAPCO used its yearly inspections to verify that the components were appropriately handling the Focal Point and SAP programs. If the SAPCO detected misuse, the program was more closely examined. The Joint Staff Focal Point manager said that the Joint Staff collected all ACCM data from the COCOMs and then forwarded it to OUSD(I), with a copy to OUSD(P) for "the yearly reports to Congress." He also said that OUSD(I) was supposed to provide oversight and inspect the ACCM and Focal Point programs, but since 2012, the Joint Staff SAPCO office had not been inspected.

(U//~~FOUO~~) The Joint Staff SAPCO experienced severe personnel constraints. Previously, four contractors worked in the SAPCO -- with one contractor specifically focused on Focal Point program management. A senior Joint Staff official said that contract problems caused the contract to be terminated, leaving only one military officer to work all Joint Staff SAP and Focal Point issues. Possibly as a result, multiple Focal Point managers said that ~~OSD: (b)(5)~~

~~_____~~ The COCOM Focal Point managers reported that their programs had not recently been inspected or been provided training or oversight of any kind from Joint Staff or OUSD(P). One COCOM Focal Point Control Officer said that the Joint Staff inspected that command's programs approximately two years ago [in about 2012] and the COCOM participated in an ACCM and Focal Point conference about four years ago [in about 2010], in addition to adhering to a yearly reporting requirement to the Joint Staff. Another COCOM Focal Point Control Officer said that since 2008, the Joint Staff SAPCO conducted only one inspection of its Focal Point program.

(U) Internal/Command Oversight

(U) Services

(U//~~FOUO~~) Army's ACCM manager said that his office provided a yearly program report to the Army Special Programs Division (ASPD). U.S. Army Special Operations Command

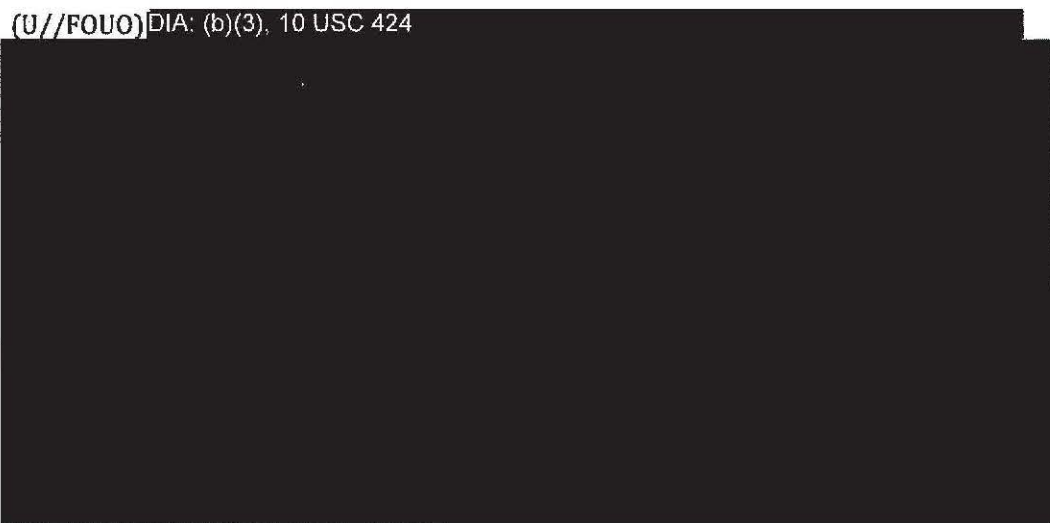
~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(USASOC) conducted a special assistance visit (SAV) for his office every other year and an inspection in the non-SAV years. The HQ staff or OUSD(P) had never inspected Navy's ACCM programs. The Air Force and the Marine Corps did not own or manage any ACCM programs.

(U) Combat Support Agencies

(U//FOUO) DIA: (b)(3), 10 USC 424



(U) U.S. Central Command

(U) The U.S. Central Command (USCENTCOM) Focal Point Program Office maintained internal oversight of its ACCM and Focal Point programs. That office inspected the administrative portion of USCENTCOM's ACCM and Focal Point programs; however, no external agencies had conducted any inspections. USCENTCOM, Joint Staff, and OUSD(P) did not provide any records in response to our data call to document when the USCENTCOM ACCM and Focal Point programs were last inspected.

(U) U.S. Special Operations Command

(U//FOUO) The U.S. Special Operations Command (USSOCOM) Focal Point Control Office (FPCO) and the Office of the Inspector General (OIG) managed the internal

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

oversight of ACCM and Focal Point programs. The USSOCOM FPCO provided oversight to the personnel who were granted ACCM and Focal Point access by USSOCOM, and the OIG conducted security inspections and investigations into violations of USSOCOM's ACCM program. The internal oversight was reportedly accomplished through USSOCOM's training requirement for all those with access to ACCMs to complete a yearly "need-to-know" justification for continued access. The USSOCOM OIG provided oversight of the command's ACCM and Focal Point programs by leading inspections of the Theater Special Operations Commands (TSOCs). USSOCOM headquarters reportedly last inspected the USSOCOM programs in June 2012. The USSOCOM Focal Point manager also said that he could not recall when the Joint Staff last inspected USSOCOM's Focal Point programs, but "it was a while ago."

(U) Conclusion

(U//~~FOUO~~) According to DoD 5200.01-V3, authorities that approved using ACCMs were required to establish and maintain a system that provides for recurrent inspection of ACCM use that they had approved, and the inspection program was to be designed to ensure compliance with the regulation's provisions. Using ACCM protections did not mean precluding or impeding congressional, Office of the Secretary of Defense, or other appropriate oversight. Our evaluation determined that the Joint Staff and COCOM ACCM and Focal Point Control Offices maintained a varying degree of administrative oversight of the ACCM program. We could find no indication that the Joint Staff and COCOM ACCM and Focal Point offices conducted routine inspections of their ACCM and Focal Point programs. Both programs lacked standardized DoD guidance on maintaining an ACCM program.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U) Recommendation, Management Comments, and
Our Response

(U) Recommendation A

(U//~~FOUO~~) We recommend that the Office of the Under Secretary of Defense for Policy, as staff proponent for Alternative Compensatory Control Measures program management and oversight, develop a plan of assistance, oversight, and inspections of the components' Alternative Compensatory Control Measures programs. We request that the Office of the Undersecretary of Defense for Policy provide its plan within 90 days from the date of this report.

(U) Office of the Under Secretary of Defense for Policy Response

(U) OSD: (b)(5)

[REDACTED]

(U) Our Response

(U) Although OUSD(P) did not comment on the report or findings themselves, nor did they specifically state "concur" or "non-concur," the plan of action or milestones provided in their comments met the intent of each recommendation, we considered them responsive, and we require no further action.

~~CONFIDENTIAL~~

(U) Finding B

(U) Alternative Compensatory Control Measures Guidance Lacked Detail

(U//~~FOUO~~) DoD Manual 5200.01-V3, which governed DoD's ACCM program, was vague -- DoD's manual contained only six pages covering oversight, creation and use, maintenance, prohibitions, documentation, and reporting requirements for the ACCM program. As a result, program users of the DoD manual were unsure how to format messages, records, and other documents. CJCSM 3213.02A, which covered the Focal Point program, was 48 pages and included numerous formatting examples for associated messages and records. Although the CJCS manual was more specific than the DoD manual, it too lacked specific definitions, guidance, requirements, formats, and rules for the program.

(U) DoD Manual 5200.01, Volume 3

(U) DoD Manual 5200.01-V3 contained six pages of guidance governing the ACCM program. The document stated that an ACCM had three required elements: (1) using an unclassified nickname, obtained in accordance with CJCSM 3150.29C; (2) a list of persons who were authorized access; and (3) a specific description of information subject to the enhanced ACCM controls. Additional requirements included a sponsor and program owner approval, a designated program control officer, a program security classification guide, a program security plan, and a participant introduction briefing.

(U) The manual designated OUSD(P) as the DoD staff proponent for ACCM management, oversight, and congressional reporting. The document also designated the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) as the proponent for ACCM security policy.

~~CONFIDENTIAL~~

Page 5

(U) Chairman, Joint Chiefs of Staff Manual 3213.02A

(U) CJCSM 3213.02A governed a CJCS-directed program established under DoD 5200.1-R, "Information Security Program." The CJCS manual outlined procedures for the Joint Staff Focal Point Communications Systems and implemented additional control measures for protecting operationally-sensitive classified information.

(C) OSD: (b)(1), Sec. 1.4(a)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U//~~FOUO~~) Although DoDM 5200.01-V3, was considered better than its previous version because all of the ACCM-related guidance was in one place, CJCSM 3213.02A was considered superior and "a huge help" by users of both because it included templates and examples of requirements. Although the CJCS manual was more specific than the DoD manual, both lacked specific definitions, guidance, requirements, formats, and rules for the program.

Page 5

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U) Guidance Lacking

(U) DoDM 5200.01-V33, paragraph 18c(7) stated that "Heads of DoD Components must establish and maintain a system that provides for recurrent inspection of the ACCM they approved. This mechanism shall ensure compliance with the provisions of this Manual." The manual did not explain how to create or maintain such a system, nor did it explain how often any "recurrent" inspections should occur. DoDM 5200.01-V3, also stated that "Each ACCM shall be overseen and inspected on a recurrent basis by the ACCM sponsor or OUSD(P)." But by saying either "the sponsor or OUSD(P)", either entity could reasonably expect to be the designated authority, or conversely, expect the other to provide oversight.

(U//~~FOUO~~) DoD guidance did not specify how to track personnel who previously had access to a given program, but no longer had a need to know. In fact, because DoDM 5200.01-V3, paragraph 18d(4) prohibited "Using specialized non-disclosure agreements or any certificates of disclosure or non-disclosure for ACCM access," some personnel believed tracking personnel who had access and no longer had a need to know the program information in question could violate the manual's rules. An Army officer said that ~~OSD: (b)(5)~~

~~_____~~

~~_____~~

~~_____~~

~~_____~~. Further, an

official in OUSD(P) said that ~~OSD: (b)(5)~~

~~_____~~

~~_____~~

~~_____~~

~~_____~~

~~_____~~. For more on tracking of personnel access, see

Finding C, "DoD Did Not Have a Centralized ACCM Access Tracking or Program Management System."

02 JUN 2013 07:00:12

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U//~~FOUO~~) We were told that OUSD(P) had been asked to establish better guidance regarding ACCMs, but that OSD: (b)(5) [REDACTED]

[REDACTED]. We were also told by an OUSD(P) official that OSD: (b)(5) [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

(U) Formats Lacking

(U) DoDM 5200.01-V3 paragraph 18c(1), stated:

The DoD Component Head establishing or terminating any such ACCM [for either DoD intelligence matters or for classified operations, sensitive support, and other non-intelligence activities] shall provide written notification within 30 days to the Director of Security, OUSD(I), and the Director, Special Programs, OUSD(P), who shall maintain this information as long as the ACCM is in use.

Additionally, paragraph 18m stated, "[an] ACCM shall be terminated by the establishing DoD Component when ACCM security measures are no longer required." However, the manual did not provide a format for such establishment or termination notification, and the lack of response to our data call indicated that OUSD(P) either had not received such notifications or did not maintain them.

(U) DoDM 5200.01-V3, paragraph 18c(5), stated, "A roster or listing of all persons accessed to the ACCM shall be maintained by the ACCM control officer." However, the manual did not provide a format for such a roster. One organization tracked only program users' names, the programs the users had access to, and their access status, while other commands held more detailed data, including name, rank, social security number, service association, parent organization, phone and email contact information, date of access, and access status.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U//~~FOUO~~) The DoD manual specified that DoD Component Heads could approve ACCM use for classified information over which they had cognizance, but prior to establishment, they were to do analyses to determine the criticality, sensitivity, and value of the information; threats, both known and anticipated; vulnerability of the data to exploitation; and a countermeasures cost-benefit analysis. Of the program managers and users we interviewed, none had completed these analyses and none claimed to understand, or could explain, what the analyses would include or how they would be done. Further, a review of the documents provided in response to our data calls did not indicate that any analyses were done.

(U) CJCSM 3213.02A was significantly more detailed than the DoD manual when describing format. This manual included examples and templates of official messages (including headers), written correspondence headers, fax cover headers, program control sheets, and templates for Focal Point program extension to a military unit.

(U//~~FOUO~~) Despite the manual being more detailed, a COCOM Focal Point System Control Officer (FPSCO) told us that ~~OSD: (b)(5)~~

~~_____~~
~~_____~~
~~_____~~
~~_____~~

(U) Conclusion

(U//~~FOUO~~) Although CJCSM 3213.02A was more specific than DoD Manual 5200.01-V3 and provided format requirements and examples for communication of protected data, both manuals lacked specific definitions, guidance, requirements, formats, and rules for the program.

~~CONFIDENTIAL~~

CONFIDENTIAL

(U) Recommendation, Management Comments, and
Our Response

(U) Recommendation B

(U//~~FOUO~~) We recommend that the Office of the Under Secretary of Defense for Policy, as staff proponent for Alternative Compensatory Control Measures program management and oversight, revise DoD Manual 5200.01, Volume, 3 to include additional definitions, guidance, requirements, formats, and rules for the Alternative Compensatory Control Measures program.

(U) Office of the Under Secretary of Defense for Policy Response

(U) OSD: (b)(5)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Our Response

(U) Although OUSD(P) did not comment on the report or findings themselves, nor did they specifically state "concur" or "non-concur," the plan of action or milestones provided in their comments met the intent of each recommendation, we considered them responsive, and we require no further action.

CONFIDENTIAL

(U) Finding C

(U) DoD Did Not Have a Centralized Alternative Compensatory Control Measures Access Tracking or Program Management System

(U//~~FOUO~~) DoD lacked a centralized ACCM program access tracking system. Some ACCM program users interpreted the DoDM 5200.01-V3 rules against using increased security standards, certificates of disclosure or non-disclosure, and billet structure to mean that a central registry of ACCM programs, and personnel who had been granted access to the ACCM programs, would be prohibited. As a result, components had created command-specific access rosters and relied on email and telephone contact between control officers to communicate a given user's access status.

(U) Centralized Access Tracking

(U//~~FOUO~~) DoD Manual 5200.01-V3, paragraph 18d, prohibited the use of personnel security investigative or adjudicative standards that were more stringent than those normally required for a comparable level of classified information to establish access eligibility to ACCM-protected information. The manual also prohibited the use of specialized non-disclosure agreements or any certificates of disclosure or non-disclosure for ACCM access and using a billet structure or system to control the position or numbers of persons afforded ACCM access.

(U//~~FOUO~~) Although the DoD SAP community used the Distributed Common Access Database System (DCADS) to track individuals' SAP access, using DCADS or a DCADS-like system for tracking ACCM access was not the standard. An OUSD(P) official said that using DCADS or a DCADS-like system to track ACCM access would be beneficial, but
OSD: (b)(5)

CONFIDENTIAL

Page 10

OSD: (b)(5)

. We could find no prohibition or reason for avoiding the use of a common access tracking system, and the OUSD(I) SAPCO said that OSD: (b)(5)

. Because no central access-tracking capability existed for ACCMs, ACCM and Focal Point Control Officers relied on spreadsheets and email correspondence between commands to ensure users' need-to-know and access.

(U//FOUO) A variety of alternate methods were being developed and used by Joint Staff, USCENTCOM, USSOCOM, and possibly others to track ACCM access status. Based on our interviews with personnel in a variety of commands and responses to our data calls, we determined that most commands and components tracked who had a need-to-know and had been granted access to a given ACCM program using a Microsoft Excel (or similar) spreadsheet. A Joint Staff official said that using a spreadsheet was easier for access control lists because the lists could be "locked down"; however, in that official's opinion, OSD: (b)(5)

. Ultimately, no enterprise solution existed that could bring the users to the database instead of pushing the database (individual access lists) to the users.

(U//FOUO) OUSD(I) and some of the COCOMs had attempted to use DCADS to track select ACCM accesses, and DCADS was updated to support tracking of individuals' ACCM status. However, DCADS was not a universally-available system, and requiring its use could be impractical for some users, particularly those who were deployed. A Joint Staff official said that OSD: (b)(5)

. A USCENTCOM official informed us that USCENTCOM maintained a database on the internal SIPRNET portal for tracking which USCENTCOM personnel had access to which programs, but user data had to be

10/10/10 10:10:10

CONFIDENTIAL

~~CONFIDENTIAL~~

entered manually. A USSOCOM official said that the command also used a (separate) web-based portal to track access to its ACCM and Focal Point programs.

(U//~~FOUO~~) Regardless of what system would ultimately be used, we found wide agreement that the greater ACCM program would benefit from a centralized database capable of tracking program accesses or, at a minimum, show who owned and managed each of the ACCMs so a centralized POC could be found.

(U) Centralized Management of Alternative Compensatory Control Measures Programs

(U//~~FOUO~~) In addition to the need to track personnel accesses, an OUSD(I) official pointed out that DoD needed a central location for managing ACCMs for deconfliction. No centralized governance process existed to deconflict resources with other ACCMs or SAPs, and the users in the components who create ACCMs are not required to deconflict their programs with other SAP or ACCM programs.

(U) Conclusion

(U//~~FOUO~~) No centralized ACCM program management system existed; nor was a centralized database established for tracking an ACCM program user's need-to-know or program access status. As a result, each component used a separate tracking method and database, and relied on email and telephone communication to relay a user's status.

(U) Recommendation, Management Comments, and Our Response

Recommendation C

(U//~~FOUO~~) We recommend that the Office of the Under Secretary of Defense for Policy, as staff proponent for Alternative Compensatory Control Measures program management and oversight, develop a centralized database of Alternative

DDI-2015-011 20

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Compensatory Control Measures programs, along with users' need-to-know and access status.

(U) Office of the Under Secretary of Defense for Policy Response

(U) OSD: (b)(5)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Our Response

(U) Although OUSD(P) did not comment on the report or findings themselves, nor did they specifically state "concur" or "non-concur," the plan of action or milestones provided in their comments met the intent of each recommendation, we considered them responsive, and we require no further action.

~~CONFIDENTIAL~~

(U) Finding D

(U) DoD Did Not Have Standardized Alternative Compensatory Control Measures Program Training

(U//~~FOUO~~) DoD lacked a formal ACCM-specific training program. Some control officers and users equated the program access briefings to be the same as training. Others said they had not received any initial ACCM training.

(U) DoDM 5200.01-V3, paragraph 18j(4) stated that "Personnel requiring access to ACCM-protected information shall receive specialized training upon initial access to the program and annually thereafter." Although the manual did specify the minimum topics to be covered, neither the manual nor OUSD(P) specified a format for the specialized training. We were told by personnel at the OUSD(I) level, the Joint Staff level, the COCOM level, and at the combat support agency level that they had not received any formal ACCM training. Some personnel in the same organizations said that the units relied on individual program briefs and on-the-job training, and in some cases, the users were expected to read the manuals and interpret the contents for themselves.

(U) Recommendation, Management Comments, and Our Response

(U) Recommendation D

(U//~~FOUO~~) We recommend that the Office of the Under Secretary of Defense for Policy, as staff proponent for Alternative Compensatory Control Measures program management and oversight, develop a standard initial Alternative Compensatory Control Measures training program.

~~CONFIDENTIAL~~

(U) Office of the Under Secretary of Defense for Policy Response

(U) The Office of the Under Secretary of Defense for Policy provided a response that USD(P) SAPCO had developed a standardized ACCM implementation plan for the initiation of ACCMs. This implementation plan provided broad customizable guidance for the management of an ACCM within a component. OSD: (b)(5)

[REDACTED]

[REDACTED]

[REDACTED]

(U) Our Response

(U) Although OUSD(P) did not comment on the report or findings themselves, nor did they specifically state "concur" or "non-concur," the plan of action or milestones provided in their comments met the intent of each recommendation, we considered them responsive, and we require no further action.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U) Finding E

(U) DoD Did Not Provide a Yearly Alternative Compensatory Control Measures Program Report to Congress

(U//~~FOUO~~) DoD did not provide a regular report of ACCM programs to Congress. Although DoD 5200.01-V3 specifically designated OUSD(P) as the DoD staff proponent for congressional reporting, we were told by OUSD(P) officials that no legal requirement existed to provide a yearly report and, as a result, OUSD(P) had not reported DoD's ACCM program status to Congress since 2009.

(U//~~FOUO~~) We were told by an OSD official that in the early 2000s, Congress directed DoD to provide yearly reports on its ACCM programs. OSD: (b)(5)

[REDACTED]

[REDACTED]

[REDACTED]. The OSD official said that soon after the meeting, a directive type memo was issued, in conjunction with a SAP requirement, to provide a yearly report to Congress on the DoD's ACCM programs. We were unable to locate any such directive type memo through data calls or interviews.

(U//~~FOUO~~) Although DoDM 5200.01-V3, stated, "The DoD staff proponent for ACCM management, oversight and Congressional reporting is the OUSD(P)," and a component control officer told us he provided OUSD(P) a yearly update on the programs for "the report to Congress," OUSD(P) had not made an ACCM-specific report to Congress since 2009. An OUSD(P) official said that the DoD Office of General Counsel (OGC) gave OUSD(P) advice or guidance that DoD OIG: (b)(5)

[REDACTED]

[REDACTED]. The OUSD(P) official said that OSD: (b)(5)

[REDACTED]

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

OSD: (b)(5)

[REDACTED]. A data call to DoD OGC did not reveal any written guidance or advice regarding congressional reporting. Further, when asked specifically about the legal advice, the Associate Deputy General Counsel for Intelligence, who compiled the data call response, responded that she had specifically looked for that item and had asked about it in her office, but could find nothing in writing and no one with whom she worked recalled giving that advice.

(U) Conclusion

(U//~~FOUO~~) DoD did not provide Congress with a yearly status report of the department's ACCM programs. OUSD(P) officials said that they had received legal advice from DoD OGC to DoD OIG: (b)(5), but we were unable to verify that guidance.

(U) Recommendation, Management Comments, and Our Response

(U) Recommendation E

(U//~~FOUO~~) We recommend that the Office of the Under Secretary of Defense for Policy, as staff proponent for Alternative Compensatory Control Measures program congressional reporting, either obtain written legal advice against reporting Alternative Compensatory Control Measures program status to Congress, or resume regular yearly reports.

(U) Office of the Under Secretary of Defense for Policy Response

(U) The Office of the Under Secretary of Defense for Policy provided a response that USD(P) SAPCO had engaged the OSD/GC staff on definitive guidance on the reporting of ACCM program status to Congress. OSD/GC staff had advised that DoD OIG: (b)(5)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Page 6

OSD: (b)(5)

[REDACTED]

(U) Our Response

(U) Although OUSD(P) did not comment on the report or findings themselves, nor did they specifically state "concur" or "non-concur," the plan of action or milestones provided in their comments met the intent of each recommendation, we considered them responsive, and we require no further action.

OSD: (b)(5) - 23

~~CONFIDENTIAL~~

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this evaluation from October 2013 through June 2014 in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation. We focused on DoD units' processes and documentation of ACCM program creation, use, and maintenance. We evaluated the larger DoD ACCM program and its protection of the DoD components' sensitive plans, operations, support, and intelligence data. Our evaluation encompassed two data calls and 28 interviews of subject-matter experts in OUSD(P) and OUSD(I); the Office of the Joint Staff; the DoD OGC; the DoD SAPCO; the U.S. Army and U.S. Navy; DIA; and USCENTCOM and USSOCOM. The U.S. Air Force, U.S. Marine Corps, National Reconnaissance Office, and the National Security Agency did not own any ACCM programs. The data, planning, and operations that the ACCM programs protect were beyond the scope of this evaluation. We did not evaluate the legality, legitimacy, feasibility, differentiation, acceptability, or sensitivity of the protected data, and we did not interview the end users of the data to determine whether the actual data being protected was as described in the program briefings, security plans, and security classification guides.

(U) Prior Coverage



(U) No prior coverage of the DoD ACCM program has been conducted during the last 5 years.

~~CONFIDENTIAL~~

Appendix B

(U) Appendix B

(U) Office of the Under Secretary of Defense for Policy Comments

	SECRET//NOFORN
	PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE 2100 DEFENSE PENTAGON WASHINGTON, DC 20301-2100
POLICY	JAN 09 2015
MEMORANDUM FOR OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF DEFENSE (ATTN: ANTHONY C. THOMAS)	
SUBJECT: (U) Evaluation of the Alternative Compensatory Control Measures (ACCM) Program (Project No. D2014-DINT01-0007.000)	
(U) Thank you for completing this review and providing the report. My Special Access Program Central Office has reviewed the report and provides the attached responses to the recommendations outlined in the draft report.	
(U) The OUSD(P) SAPCO, OSD: (b)(6) , is my point of contact for this matter.	
 Brian P. McKeon	
1 Attachment: Response Tables for Recommendations	
SECRET//NOFORN (COVER MEMO IS UNCLASSIFIED WHEN ATTACHMENT IS REMOVED)	

This Page is unclassified

DODIG-2015-070828

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Appendix B

(U) Office of the Under Secretary of Defense for Policy
Comments (cont'd)

REFERENCE	COMPONENT	ACTION/COMMENT
A.1 (U) OUSD(P), as staff, proponent for ACCM program management and oversight, develop a plan of assistance, oversight and inspections of the components' ACCM programs. We request OUSD(P) provide its plan within 90 days from the date of this report.	USD(P) SAPCO	(u) OSD (b)(5) OSD (b)(5) (u) OSD: (b)(5) OSD: (b)(5) (u) OSD: (b)(5) OSD: (b)(5)

Derived from: ~~OSD: (b)(6)~~ OUSD(P) SAPCO, 703-49-~~OSD (b)(6)~~
Derived from: Multiple sources
Reason: E.O. 12958, Sec 1.5(a)(1)(i)(A)
Declassify on:
Review: 28 Mar 2047
Authority FSI 20 Mar 2005

~~SECRET NOFORN~~

This page is unclassified.

DODIG-2015-070029

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Appendix B

(U) Office of the Under Secretary of Defense for Policy
Comments (cont'd)

SECRET//NOFORN		
REFERENCE	COMPONENT	ACTION/COMMENT
B.1 OUSD(P), as staff proponent for ACCM program management and oversight, revise DoDM 5200.01, Volume 3, to include additional definitions, guidance, requirements, formats, and rules for the ACCM program.	USD(P) SAPCO	(U) OSD (b)(5) OSD (b)(5)

Derived from: OSD (b)(6) USD(P) SAPCO, 703-697-
Derived from: Multiple Sources
Reason: E.O. 12958, Sec. 1.5(a)(1)(ii)(d)
Declassify on:
Review: 25 Mar 2047
Authority: FSI 30 Mar 2005

~~SECRET//NOFORN-2~~

This page is unclassified.

DODIG-2015-070030

~~CONFIDENTIAL~~

CONFIDENTIAL

Appendix B

(U) Office of the Under Secretary of Defense for Policy
Comments (cont'd)

REFERENCE	COMPONENT	ACTION/COMMENT
C.1 OUSD(P), as staff proponent for ACCM program management and oversight, develop a centralized database of ACCM programs, along with users' need-to-know and access status.	USD(P) SAPCO	(U) OSD (b)(5) OSD (b)(5) (U) OSD: (b)(5) OSD: (b)(5)

Derived from: OSD: (b)(6) USD(P) SAPCO, 703-697-
Derived from: 703-697-
Reason: E.O. 11652, Sec 1.4(c)(1)(ii)(A)
Declassify: N/A
Review: 25 Mar 2017
Authority FSE 20 Mar 2005

This page is unclassified.

DDIG-2015-070031

CONFIDENTIAL

~~CONFIDENTIAL~~

Appendix B

(U) Office of the Under Secretary of Defense for Policy
Comments (cont'd)

REFERENCE	COMPONENT	ACTION/COMMENT
D.1 OUSD(P), as staff proponent for ACCM program management and oversight, develop a standard initial ACCM training program.	USD(P) SAPCO	(U) OSD (b)(5) OSD (b)(5)

Derived from: ~~OSD (b)(6)~~ OUSD(P) SAPCO, 703-097 ~~OSD (b)(6)~~
Derived from: Multiple Sources
Reasons: E.O. 12958, Sec. 1.5(a)(1)-(4)(g)
Declassify: 44-
Review: 25 Mar 2047
Authority: FIE 20 Mar 2005

~~SECRET NOFORN 4~~

This page is unclassified.

DODIG-2015-070032

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Appendix B

(U) Office of the Under Secretary of Defense for Policy
Comments (cont'd)

REFERENCE	COMPONENT	ACTION/COMMENT
E.1 OUSD(P), as staff proponent for ACCM program congressional reporting, either obtain legal advice against reporting ACCM program status to Congress, or resume regular yearly reports.	USD(P) SAPCO	(U) OSD (b)(5) OSD (b)(5) (U) OSD (b)(5) DoD OIG: (b)(5) DoD OIG: (b)(5) OSD: (b)(5) [USD: (b)(5)]

Derived from: OSD: (b)(6) OUSD(P) SAPCO, 709-487 [REDACTED]
Derived from: Multiple Sources
Reason: E.O. 13526, Sec 3.5(a)(1)(i)(A)
Declassify: N/A
Revised: 25 Mar 2017
Authority: PLE 20 Mar 2005

~~SECRET//NOFORN~~

This page is unclassified.

DODIG-2015-070#33

~~CONFIDENTIAL~~

(U) Acronyms and Abbreviations

ACCM	Alternative Compensatory Control Measures
COCOM	Combatant Command
CJCS	Chairman, Joint Chiefs of Staff
CJCSM	Chairman, Joint Chiefs of Staff Manual
COI	Community of Interest
DCADS	Distributed Common Access Database System
DIA	Defense Intelligence Agency
DSSCS	Defense Special Security Communications System
FPCO	Focal Point Control Officer
FPSCO	Focal Point System Control Officer
GENSER	General Service (message traffic)
OIG	Office of Inspector General
OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OUSD(P)	Office of the Under Secretary of Defense for Policy
SAP	Special Access Program
SAPCO	Special Access Program Central Office
SCI	Sensitive Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
SPECAT	Special Category (message traffic)
SSO	Special Security Office
USCENTCOM	U.S. Central Command
USSOCOM	U.S. Special Operations Command

~~CONFIDENTIAL~~

Whistleblower Protection U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison

congressional@dodig.mil; 703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

Monthly Update

dodigconnect-request@listserve.com

Reports Mailing List

dodig_report@listserve.com

Twitter

twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline

~~CONFIDENTIAL~~

CONFIDENTIAL



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

1800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

CONFIDENTIAL