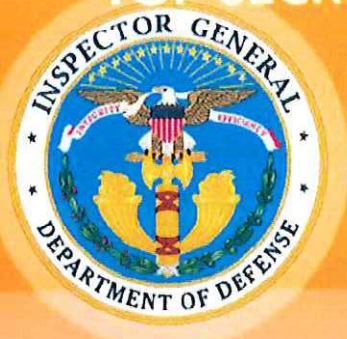


DOWOIG (b)(1) 1.4(a) and (g)

//NOFORN



# INSPECTOR GENERAL

U.S. Department of Defense

May 21, 2024

## (U) Evaluation of Combatant Command Joint Military Deception Planning

~~Classified By: DoD OIG/  
Evaluations  
Derived From Multiple  
Sources Reason: 1.4(a) and (g)  
Declassify On: 20 MAY 2049~~

~~Controlled By: DoD OIG  
Controlled By: Evaluations  
CUI Category: OPSEC  
Distribution/Dissemination Control:  
NOFORN  
POC: DOWOIG (b)(6)~~

Released by the DoW OIG  
FOIA Office under FOIA  
request DODOIG-2024-000660  
on August 14, 2026.

~~This content is classified at the TOP SECRET//ACCM-  
and may contain elements of controlled unclassified information (CUI),  
unclassified, or information classified at a lower level than the overall  
classification displayed. This content shall not be used as a source of  
derivative classification; refer instead to the classified sources appendix or  
the applicable classification guides. It must be reviewed for both Classified  
National Security Information (CNSI) and CUI in accordance with DoDI  
5200.09 prior to public release.~~

DOWOIG (b)(1) 1.4(a) and (g)

level

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

DOWOIG (b)(1) 1.4(a) and (g)

TOP SECRET//ACCM-

//NOFORN





## (U) Results in Brief

### (U) Evaluation of Combatant Command Joint Military Deception Planning

(U) May 21, 2024

#### (U) Objective

(U) The objective of this evaluation was to determine the extent to which the combatant commands have effectively conducted military deception (MILDEC) planning in support of current and future operations.

#### (U) Background

(U) Military deception is the actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions that will contribute to the success of U.S. military operations. MILDEC leverages the visible aspects of friendly operations and combines them with deceptive activities to create plausible alternative facts and conditions in the operational environment. The DoD's MILDEC activities consist of Tactical Deception, Deception in Support of Operations Security, and Joint MILDEC. This evaluation focused specifically on Joint MILDEC.

(S) Joint MILDEC is normally planned prior to, and conducted during, combat operations and is executed by, and in support of, combatant commanders, Joint force commanders, and Joint task force commanders in a theater of operations. Joint MILDEC requires Secretary of Defense approval and operates under the authorities derived from an execute order for the supported operation.

(S) The Under Secretary of Defense for Intelligence and Security serves as the program management lead and advisor to the Secretary of Defense for the DoD MILDEC program and is responsible for developing and overseeing DoD MILDEC policy and integration activities. The Influence and Perception Management Office, under the Office of the Under Secretary of Defense for Intelligence and Security, serves as the office of primary responsibility (OPR) for implementing MILDEC-specific DoD policies

#### (U) Background (cont'd)

(S) and procedures. The Joint Staff (JS) J-3 Deputy Director for Global Operations serves as the Joint MILDEC program director and provides oversight of planned and ongoing MILDEC conducted in support of Joint operations. Within the JS J-3 office, the JS J-39 Special Actions Division serves as the Joint MILDEC program manager and maintains coordinating authority over all Joint MILDEC. The JS J-39 is the single point of contact through which the combatant commands staff their MILDEC concepts, plans, and activities. The JS J-39 is responsible for reviewing, coordinating, deconflicting, and staffing the combatant commands' Joint MILDEC concepts, plans, operations, and executions with appropriate stakeholders, both within and external to the DoD.

#### (U) Finding

(S//NF) CENTCOM (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5), and USEUCOM (b)(1) 1.4a

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S//NF) Additionally, the JS J-39 provided appropriate oversight of the Joint MILDEC program, including review, approval, and deconfliction boards.

(S//NF) However, we determined that the DoD's Joint MILDEC program [REDACTED] CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5), USEUCOM (b)(1) 1.4a and c, and PACOM (b)(1) 1.4a and g

[REDACTED]

[REDACTED]



*(U) Evaluation of Combatant Command Joint Military Deception Planning*



## (U) Results in Brief

### *(U) Evaluation of Combatant Command Joint Military Deception Planning*

## (U) Management Comments and Our Response

(C//U) The ~~CYBERCOM (b)(3) 50 USC 3024(h)~~ agreed to address the recommendation; therefore, we consider the recommendation resolved and open. We will close this recommendation when the ~~CYBERCOM (b)(3) 50 USC 3024(h)~~ provides us documentation supporting the assessment and any identified mitigation strategies that address the recommendation. Therefore, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations.

(C//U) The JS Deputy Director for Global Operations (DDGO), J-39 agreed with the recommendation to develop a plan of action and milestones for any recommendations not addressed by a Deception Capabilities Joint DOTmLPP-P Change Recommendation (DCR). We will close this recommendation once the Influence and Perception Management Office and the JS DDGO J-39 provided a plan of action and milestones to implement recommendations from previous MILDEC studies not addressed by the DCR.

(U) The Under Secretary of Defense for Intelligence and Security, the Director of the Influence and Perception Management Office, and the ~~CYBERCOM (b)(3) 50 USC 3024(h)~~ did not provide responses to the draft report. Therefore, these recommendations are unresolved. We request that the above mentioned organizations provide comments within 30 days in response to the final report to address the recommendation.

(U) Please see the Recommendations Table on the next page for the status of recommendations.

**(U) Recommendations Table**

| (U) Management                                                                   | (U) Recommendations Unresolved | (U) Recommendations Resolved | (U) Recommendations Closed |
|----------------------------------------------------------------------------------|--------------------------------|------------------------------|----------------------------|
| (S//NF) Under Secretary of Defense for Intelligence and Security                 | 1.a, 1.b                       | None                         | None                       |
| (S//NF) Director, Influence and Perception Management Office                     | 2.a, 2.b, 4                    | None                         | None                       |
| (S//NF) Joint Staff J-3 Deputy Director for Global Operations                    | 2.a, 2.b, 4                    | None                         | None                       |
| (S//NF) CYBERCOM (b)(3) 50 USC 3024(b)<br>[REDACTED]<br>[REDACTED]<br>[REDACTED] | [REDACTED]                     | [REDACTED]                   | [REDACTED]                 |
| (S//NF) CYBERCOM (b)(3) 50 USC 3024(b)<br>[REDACTED]<br>[REDACTED]               | [REDACTED]                     | [REDACTED]                   | [REDACTED]                 |

(U) Please provide Management Comments by June 20, 2024.

(U) NOTE: The following categories are used to describe agency management's comments to individual recommendations.

- (U) Unresolved – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- (U) Resolved – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- (U) Closed – The DoD OIG verified that the agreed upon corrective actions were implemented.



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

May 21, 2024

**MEMORANDUM FOR UNDERSECRETARY OF DEFENSE FOR INTELLIGENCE  
AND SECURITY**

COMMANDER, UNITED STATES  
COMMANDER, UNITED STATES  
COMMANDER, UNITED STATES  
COMMANDER, UNITED STATES  
DIRECTOR, JOINT STAFF

CYBERCOM (b)(3) 50 USC 3024(h)

**SUBJECT: (U) Evaluation of Combatant Command Joint Military  
Deception Planning (Report No. DODIG-2024-085)**

(U) This final report provides the results of the DoD Office of Inspector General's evaluation. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(~~CU~~) This report contains recommendations that are considered unresolved because the Under Secretary of Defense for Intelligence and Security, the Director of the Influence and Perception Management Office, and the ~~\_\_\_\_\_~~ ~~\_\_\_\_\_~~ did not provide a response to the report. We request that you provide comments within 30 days in response to the final report to address the recommendations.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations.

(~~CU~~) This report also contains recommendations that are considered resolved and open. The Joint Staff and ~~\_\_\_\_\_~~ ~~\_\_\_\_\_~~ agreed to address the recommendations presented in the report; therefore, we consider the recommendations resolved and open. We will close the recommendations when you provide us documentation showing that all agreed upon actions to implement the recommendations are completed. Therefore, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations. Send your response to either [followup@dodig.mil](mailto:followup@dodig.mil) if unclassified or ~~\_\_\_\_\_~~ if classified.

~~(S//)~~ We will track these recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and management officials submit adequate documentation showing that all agreed-upon actions are completed.

(U) Please send responses to [followup@dodig.mil](mailto:followup@dodig.mil) if unclassified or DOWOIG (b)(6) if classified. We appreciate the cooperation and assistance received during the evaluation. If you have any questions, please contact DOWOIG (b)(6)

DOWOIG (b)(6)

FOR THE INSPECTOR GENERAL:



Bryan T. Clark  
Assistant Inspector General for Evaluations  
Programs, Combatant Commands  
and Operations

~~Controlled by: DoD OIG~~

~~Controlled by: Evaluations~~

~~CUI Category: OPSEC~~

~~Distribution/Dissemination Control: NOFORN~~

POC: DOWOIG (b)(6)

## (U) Contents

|                                                                                                                                                         |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| (U) Introduction.....                                                                                                                                   | 1  |
| (U) Objective.....                                                                                                                                      | 1  |
| (U) Background.....                                                                                                                                     | 1  |
| (U) Finding.....                                                                                                                                        | 9  |
| (S//NF) CENTCOM (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [REDACTED]<br>[REDACTED]<br>[REDACTED]<br>[REDACTED] ..... | 9  |
| (U) CYBERCOM (b)(3) 50 USC 3024(h) [REDACTED]<br>[REDACTED] .....                                                                                       | 10 |
| (U) The Joint Staff Provided Appropriate Oversight of the Joint MILDEC Program .....                                                                    | 12 |
| (S//NF) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [REDACTED]<br>[REDACTED] .....                                                     | 13 |
| (S//NF) The DoD CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [REDACTED]<br>[REDACTED]<br>[REDACTED] .....                               | 18 |
| (U) Recommendations, Management Comments, and Our Response .....                                                                                        | 19 |
| (U) Appendix A .....                                                                                                                                    | 23 |
| (U) Scope and Methodology.....                                                                                                                          | 23 |
| (U) Appendix B .....                                                                                                                                    | 25 |
| (S//NF) The DoD's MILDEC Program is CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [REDACTED]<br>[REDACTED] .....                         | 25 |
| (U) Appendix C .....                                                                                                                                    | 27 |
| (U) List of Classified Sources .....                                                                                                                    | 27 |
| (U) Management Comments.....                                                                                                                            | 29 |
| (U) CYBERCOM (b)(3) 50 USC 3024(h) [REDACTED] .....                                                                                                     | 29 |
| (U) CYBERCOM (b)(3) 50 USC 3024(h) [REDACTED] .....                                                                                                     | 31 |
| (U) Joint Staff Deputy Director for Global Operations, J-39 .....                                                                                       | 33 |
| (U) Acronyms and Abbreviations.....                                                                                                                     | 34 |

## (U) Introduction

### (U) Objective

(U) The objective of this evaluation was to determine the extent to which the combatant commands have effectively conducted joint military deception (MILDEC) planning in support of ongoing operations.<sup>1</sup>

### (U) Background

(S//NF) The 2022 National Defense Strategy directs the DoD to focus efforts on U.S. strategic and military pacing challenges, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h)

[REDACTED]. The 2022 National Defense Strategy introduces the concept of integrated deterrence as its core strategy for sustaining and strengthening U.S. interests, directing the DoD to use every tool at its disposal to defend the U.S. homeland, deter strategic attacks against the United States and its allies and partners, deter aggression of our adversaries, and build a resilient Joint force. The 2022 National Military Strategy provides a framework for the integrated deterrence approach, directing the DoD to campaign and build warfighting advantages by synchronizing operations across warfighting domains, theaters, interagency, and allies and partners. Within this framework, the National Military Strategy directs the Joint force to, among other actions, conduct offensive and defensive counterintelligence, cognitive warfare, and military deception.

(U) Joint doctrine defines MILDEC as “the actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.”<sup>2</sup> MILDEC leverages the visible aspects of friendly operations and combines them with deceptive activities to create plausible alternative facts and conditions in the operational environment.

(S) The DoD’s MILDEC activities consist of Tactical Deception (TAC-D), Deception in Support of Operations Security (DISO), and Joint MILDEC. This evaluation focused specifically on Joint MILDEC. Joint MILDEC activities create operational-level effects that support military campaigns and major operations. Joint MILDEC is normally planned prior to, and conducted during, combat operations and is executed by, and in

<sup>1</sup> (U) This report contains information that has been redacted because it was identified by the Department of Defense as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

<sup>2</sup> (U) Joint Publication (JP) 3-13.4, “Military Deception,” February 14, 2017.

(U) Introduction

(S) support of, combatant commanders, joint force commanders (JFCs), and joint task force (JTF) commanders in a theater of operations. Joint MILDEC requires Secretary of Defense (SecDef) approval and operates under the authorities derived from an execute order (EXORD) for the supported operation.

### ***(U) Joint MILDEC Policy, Guidance, and Authorities***

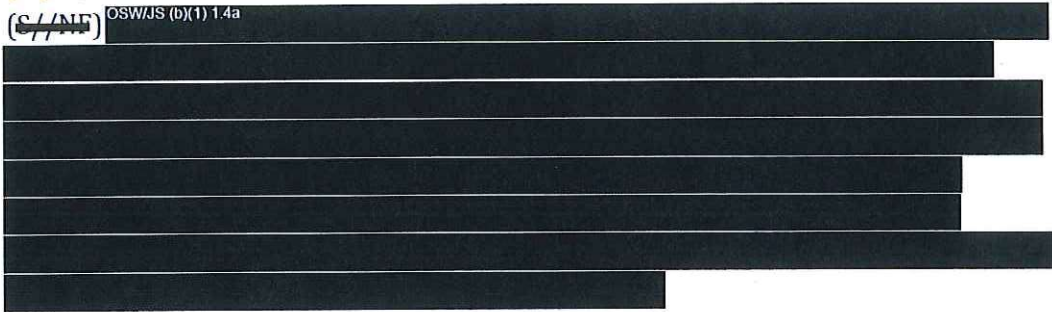
(U) Three DoD issuances specify Joint MILDEC policy, establish roles and responsibilities, and define policy and guidance for planning, approval, execution, and assessment of Joint MILDEC.

#### ***(U) DoD Instruction S-3604.01***

(S) DoD Instruction (DoDI) S-3604.01 establishes policy, assigns responsibilities, and provides direction for DoD deception activities.<sup>3</sup> The Instruction states that DoD Components may, but are not required to, conduct military deception. Combatant commanders who choose to conduct Joint MILDEC are required to assign responsibilities and establish policy and procedures for planning, integration, review, execution, and oversight of Joint MILDEC. The Instruction further directs that deception activities comply with U.S. law, the law of armed conflict, treaties and agreements, Presidential and DoD Component policy and regulations, and rules of engagement, and expressly prohibits the use of deception activities to support non-DoD Federal Department or Agency (NDFDA) activities unless approved.<sup>4</sup>

#### ***(U) CJCSI 3211.01F***

(S//NF) OSWJS (b)(1) 1.4a



<sup>3</sup> (U) DoDI S-3604.01, "DoD Deception Activities," September 18, 2019, and the "DoD Law of War Manual," Sections 5.21 through 5.25, June 2015, provide policies and guidance regarding unlawful deception activities.

<sup>4</sup> (S) NDFDA activities must be approved in accordance with DoDD S-5205.61, "DoD Cover and Cover Support Activities," July 15, 2014; and DoDI S-5105.63, "Implementation of DoD Cover and Cover Support Activities," June 20, 2013.

<sup>5</sup> (U) CJCSI 3211.01F, "Joint Policy for Military Deception," May 14, 2015.

<sup>6</sup> (U) CJCSI 3211.01F.

### ***(U) Joint Publication 3-13.4***

(U) Joint Publication (JP) 3-13.4 provides Joint doctrine for planning, executing, and assessing military deception in support of Joint operations.<sup>7</sup> JP 3-13.4 defines the roles, functions, and tenets of MILDEC and establishes a framework for MILDEC planning in conjunction with information operations, operations security, and intelligence support. The Joint publication also defines the steps and sequence of the MILDEC planning process and states that MILDEC should be planned and executed as part of the commander's concept of the operation.

### ***(U) Roles and Responsibilities***

(U) The planning, reviewing, approving, and implementation of military deception activities occurs at multiple levels within the DoD. DoDI S-3604.01 defines the basic roles and responsibilities for MILDEC, and CJCSI 3211.01F and JP 3-13.4 provide additional implementing guidance for DoD component MILDEC planners, reviewers, and approval authorities.

### ***(U) Office of the Secretary of Defense***

~~(S//NF)~~ According to CJCSI 3211.01F, the SecDef is responsible for approving or disapproving the execution, modification, and termination of all MILDEC plans and approving or disapproving Joint MILDEC executions.

~~(CUI)~~ The Under Secretary of Defense for Intelligence and Security (USD[I&S]) serves as the program management lead and advisor to the SecDef and DepSecDef for the DoD MILDEC program.<sup>8</sup> As the program lead, the USD(I&S) develops and oversees DoD MILDEC policy and integration activities. The Influence and Perception Management Office, under OUSD(I&S), serves as the office of primary responsibility (OPR) for implementation of MILDEC-specific DoD policies and procedures.<sup>9</sup>

~~(S//NF)~~ The USD(I&S), Under Secretary of Defense for Policy (USD[P]), and the DoD General Counsel coordinate to ensure that all joint MILDEC plans, operations, and executions are reviewed for legal sufficiency and relevancy; are consistent with current

---

<sup>7</sup> (U) JP 3-13.4.

<sup>8</sup> (U) DoDI S-3604.01 and CJCSI 3211.01F reflect the title of this office as the Office of the Under Secretary of Defense for Intelligence (OUSD[I]). In 2019, Congress renamed OUSD(I) as the Office of the Under Secretary of Defense for Intelligence and Security (OUSD[I&S]).

<sup>9</sup> ~~(CUI)~~ DoDI S-3604.01 disestablished the Defense Military Deception Program Office and re-assigned MILDEC responsibilities to the Director for Defense Intelligence (Collection and Special Programs) (DDI[C&SP]). In the summer of 2023, the office of primary responsibility was transitioned to the Influence and Perception Management Office.

(U) Introduction

(~~S//NF~~) DoD and national policy objectives and guidance; and are deconflicted with NDFDAs prior to SecDef approval.

**(U) Joint Staff**

(~~S~~) The Chairman of the Joint Chiefs of Staff serves as the proponent for Joint MILDEC and is the principal military advisor to the SecDef on all Joint MILDEC matters. The CJCS is responsible for maintaining oversight of MILDEC support to Joint operations, which includes an annual review of the overall status of Joint MILDEC activities that affect Joint plans, operations, or commands.

(~~CONF~~) The Joint Staff (JS) J-3 Deputy Director for Global Operations (DDGO) serves as the Joint MILDEC program director. The DDGO, acting for the CJCS, manages JS MILDEC personnel and resources to ensure that oversight and assessment requirements are met. The DDGO also provides oversight of planned and ongoing MILDEC conducted in support of Joint operations. This includes ensuring that MILDEC operations that overlap functional combatant command (FCC) or geographic combatant command (GCC) responsibilities are coordinated and integrated with all applicable DoD components.

(~~S//NF~~) OSW/JS (b)(1) 1.4a  
[REDACTED]

**(U) Combatant Commands**

(~~S//NF~~) CYBERCOM (b)(1) 1.4a, c, g; (b)(3) 50 USC 3024(h)  
[REDACTED]

(U) Introduction

(S//NF) CYBERCOM (b)(1) 1.4a, c, g; (b)(3) 50 USC 3024(h) and OSW/JS (b)(1) 1.4a

(U) Within the CCMD, personnel in the Directorate of Operations (J-3) recommend the deception objective, plans the deception effort; coordinates the deception plan with the information operations cell and the staff judge advocate; supervises the MILDEC executions; and controls the termination of the deception plan. In conjunction with the MILDEC planner, the J-3 also develops the measures of effectiveness (MOEs) to assess the deception operation.

(S//NF) CYBERCOM (b)(1) 1.4a, c, g; (b)(3) 50 USC 3024(h) and OSW/JS (b)(1) 1.4a

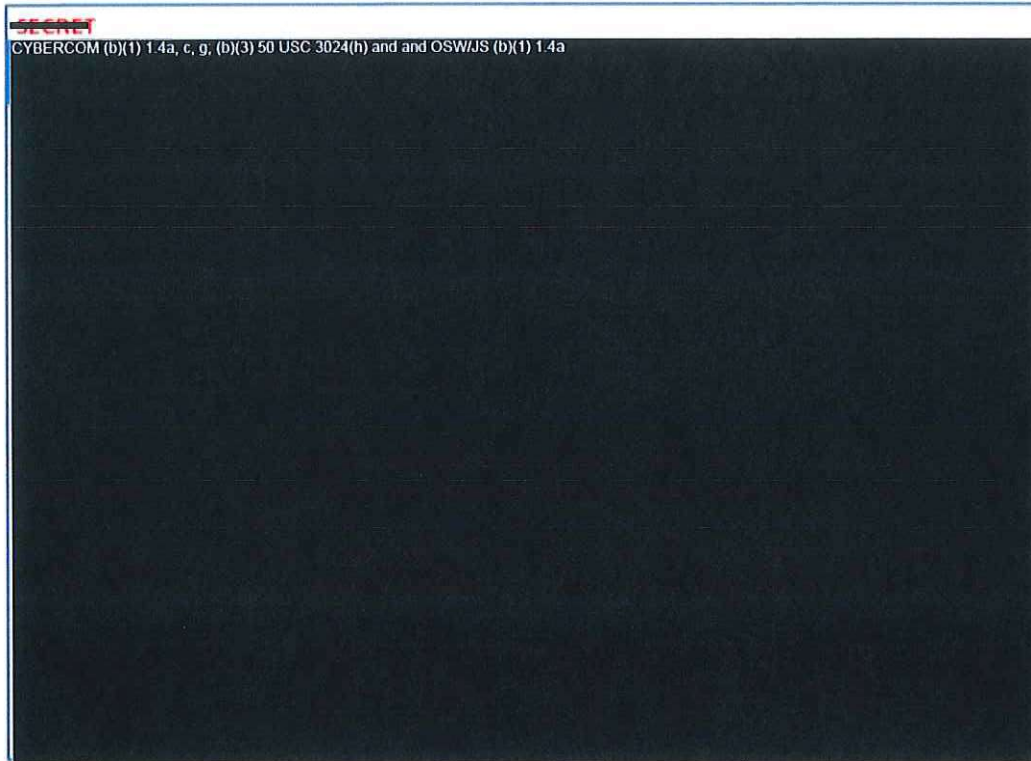
### ***(U) Joint MILDEC Review, Approval, Deconfliction, and Assessment and Reporting Process***

(U) Joint MILDEC executions are reviewed, deconflicted, synchronized, and coordinated at multiple levels prior to approval or execution to assess their potential impact on other plans, operations, and national policies. See Figure 1 for a graphic depiction of the Joint MILDEC review and approval process, to the point of execution.

10 (S//NF) OSW/JS (b)(1) 1.4a

(U) Introduction

*(U) Figure 1. Joint MILDEC Review and Approval Process*



(U) Source: CJCSI 3211.01F.

***(U) Joint MILDEC Review and Approval Process***

(S) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h)  
[Redacted text block containing approximately 10 lines of blacked-out content]

(S) OSW/JS (b)(1) 1.4a  
[Redacted text block containing approximately 4 lines of blacked-out content]

***(U) Joint MILDEC Deconfliction Process***

### ***(U) Joint MILDEC Assessment and Reporting Process***

(U) CJCSI 3211.01F instructs deception planners to consider assessment ways, means, and measures during the initial deception planning and preparation and subsequent execution to focus assessment and collection at each level, reduce redundancy, and enhance the efficiency of the overall assessment process. MILDEC is assessed using measures of performance (MOPs) to determine if a MILDEC event was executed

(U) Introduction

(U) according to plan and MOEs to determine if the event created the desired impact or effect.

(S//NF) OSW/JS (b)(1) 1.4a CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and OSW/JS (b)(1) 1.4a  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

(U) Finding

## (U) Finding

(S//NF)

CENTCOM (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a

[REDACTED]

(S//NF)

CENTCOM (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a

[REDACTED]

(S//NF)

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

CENTCOM (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(S//NF)

CENTCOM (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(U) Finding

(U) CYBERCOM (b)(3) 50 USC 3024(h) [Redacted]

(S//NF) CYBERCOM (b)(1) 1.4a, c, g; (b)(3) 50 USC 3024(h) and (b)(5) [Redacted]

### (U) Combatant Command Joint MILDEC Activities

(TS//ACCM) DOWOIG (b)(1) 1.4(a) and (g) (S//NF) DOWOIG (b)(1) 1.4(a) and (g) [Redacted]

(TS//ACCM) DOWOIG (b)(1) 1.4(a) and (g) (S//NF) DOWOIG (b)(1) 1.4(a) and (g) [Redacted]

(S//ACCM) DOWOIG (b)(1) 1.4(a) and (g) (S//NF) DOWOIG (b)(1) 1.4(a) and (g) [Redacted]

(TS//ACCM) DOWOIG (b)(1) 1.4(a) and (g) (S//NF) DOWOIG (b)(1) 1.4(a) and (g) [Redacted]

<sup>11</sup> (S//ACCM) DOWOIG (b)(1) 1.4(a) and (g) [Redacted]

(U) Finding

*(U) CCMDS are Appropriately Implementing the Joint MILDEC Planning Process*

(S//NF) CENTCOM (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

[REDACTED]

(TS//ACCM) DOWOIG (b)(1) 1.4(a) and (g) // (NF) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

DOWOIG (b)(1) 1.4(a) and (g) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h)

(U) CYBERCOM (b)(3) 50 USC 3024(h)

(S//NF) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and OSW/JS (b)(1) 1.4a

[REDACTED]

(S//NF) CENTCOM (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and OSW/JS (b)(1) 1.4a

[REDACTED]

(TS//ACCM) DOWOIG (b)(1) 1.4(a) and (g) // (NF) DOWOIG (b)(1) 1.4(a) and (g)

DOWOIG (b)(1) 1.4(a) and (g)

(U) Finding

(TS//ACCOM) DOWOIG (b)(1) 1.4(a) and (g) // (NF) DOWOIG (b)(1) 1.4(a) and (g)  
DOWOIG (b)(1) 1.4(a) and (g)  
DOWOIG (b)(1) 1.4(a)

### ***(U) CCMDs are Conducting Joint MILDEC Assessments in Accordance With Policy***

(S//NF) OSW/JS (b)(1) 1.4a  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

(TS//ACCOM) DOWOIG (b)(1) 1.4(a) and (g) // (NF) We reviewed DOWOIG (b)(1) 1.4(a) and (g)  
DOWOIG (b)(1) 1.4(a) and (g)  
DOWOIG (b)(1) 1.4(a) and (g) to determine whether the required assessment factors were included in the plan. The plan included template tables for reporting good, moderate, or no collection of assessment data for each execution, with the corresponding information requirements DOWOIG (b)(1) 1.4(a) and (g)  
DOWOIG (b)(1) 1.4(a) and (g)  
DOWOIG (b)(1) 1.4(a) and (g)

### ***(U) The Joint Staff Provided Appropriate Oversight of the Joint MILDEC Program***

(S//NF) OSW/JS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g; (b)(3) 50 USC 3024(h)  
[Redacted]  
[Redacted]  
[Redacted]

### ***(U) The Joint Staff Effectively Coordinated, Managed, and Provided Oversight of Joint MILDEC Review and Deconfliction Boards***

(S//NF) OSW/JS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g; (b)(3) 50 USC 3024(h) and (b)(5)  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

(U) Finding

(S//NF)

OSW/JS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(TS//ACCOM)

DOWOIG (b)(1) 1.4(a) and (g)

(S//NF)

OSW/JS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(TS//ACCOM)

DOWOIG (b)(1) 1.4(a) and (g)

(S//NF)

DOWOIG (b)(1) 1.4(a) and (g)

[REDACTED]

(S//NF)

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(S//NF)

OSW/JS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(U) Finding

(S//NF) OSW/JS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

(S//NF) OSW/JS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

***(U) The Roles and Responsibilities of the Office of Primary Responsibility for Military Deception Are Not Clearly Defined***

(S//NF) The DoDI S-3604.01 issued in 2019 does not define the roles and responsibilities of the OPR for military deception.

CENTCOM (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

to the  
Director for Defense Intelligence (Collection and Special Programs) (DDI[C&SP]). We were told by the DDI(C&SP) that the OPR responsibility for deception activities was transferred from the DDI(C&SP) to the Influence and Perception Management Office in 2023. As of the date of this report, Influence and Perception Management Office did not have a formal charter for deception; however, it was developing a deception management program.

(S//NF) OSW/JS (b)(1) 1.4a

(U) Finding

(S//NF) OSW/JIS (b)(1) 1.4a

[REDACTED]

(S//NF) OSW/JIS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(S//NF) OSW/JIS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

OSW/JIS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(S//NF) OSW/JIS (b)(1) 1.4a, CENTCOM (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

OSW/JIS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

(S//NF) OSW/JIS (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

OSW/JIS (b)(1) 1.4a, CENTCOM (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

[REDACTED]

OSW/JIS (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

(U) Finding

**(U) CCMDs Generally Have Little Joint MILDEC Capacity Within Their Staffs**

(S//NF) OSW/JS (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5), USEUCOM (b)(1) 1.4a and and PACOM (b)(1) 1.4a and g

[REDACTED]

(S//NF) OSW/JS (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

[REDACTED]

(S//NF) OSW/JS (b)(1) 1.4a, CENTCOM (b)(1) 1.4a and CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

OSW/JS (b)(1) 1.4a; CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

[REDACTED]

(U) Finding

(C//NF) To address these personnel related challenges the Influence and Perception Management Office in coordination with the Joint Staff J-39 should

CYBERCOM (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(C//NF) OSW/JS (b)(1) 1.4a

[REDACTED] OSW/JS (b)(1) 1.4a and USEUCOM (b)(1) 1.4a and g OSW/JS (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g,

(S)

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(S//NF)

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and PACOM (b)(1) 1.4a and g

[REDACTED]

(C//NF)

OSW/JS (b)(1) 1.4a, CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(TS//ACCM)

DOWOIG (b)(1) 1.4(a) and (g)

(//NF)

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

DOWOIG (b)(1) 1.4(a) and (g)

DOWOIG (b)(1)

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

DOWOIG (b)(1) 1.4(a) and (g)

CYBERCOM (b)(1) 1.4a, c, g,

[REDACTED]

DOWOIG (b)(1) 1.4(a) and (g)

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

(U) Finding

(S//NF) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [Redacted]

(S//NF) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [Redacted]

[Redacted]

(S//NF) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [Redacted]

[Redacted]

(S//NF) CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) [Redacted]

[Redacted]

(U) Finding

## (U) Recommendations, Management Comments, and Our Response

### (U) Recommendation 1

(U) We recommend that the Under Secretary of Defense for Intelligence and Security:

- a. ~~(S//NF)~~ Update the DoDI S-3604.1 to clarify the roles and responsibilities of the military deception office of primary responsibility.
- b. ~~(S//NF)~~ Issue a memorandum formally to formally document the designation of the Influence and Perception Management Office as the office of primary responsibility for military deception.

(U) CYBERCOM (b)(3) 50 USC 3024(h)

~~(S//NF)~~ Though not required to comment, the CYBERCOM (b)(3) 50 USC 3024(h) agreed with the recommendation to update the DoDI-S 3604.1 and underscored the need for the instruction to clarify roles and responsibilities to build a deception program that includes the capability to advocate for and address DOTmLPF-P and acquisition requirements.

### (U) Management Comments Required

(U) The Under Secretary of Defense for Intelligence and Security, did not respond to the recommendation in the report. Therefore, the recommendation is unresolved. We request that the Under Secretary of Defense for Intelligence and Security provide comments within 30 days in response to the final report to address the recommendation.

### (U) Recommendation 2

~~(S//NF)~~ We recommend that the Influence and Perception Management Office Director, in coordination with the Joint Staff J-39 Deputy Director for Global Operations:

- a. ~~(S//NF)~~ CYBERCOM (b)(3) 50 USC 3024(h) and (b)(5)

1. ~~(S//NF)~~ CYBERCOM (b)(3) 50 USC 3024(h) and (b)(5)

2. ~~(S//NF)~~ CYBERCOM (b)(3) 50 USC 3024(h) and (b)(5)

(U) Finding

3. (CUI) ~~(S//NF)~~ CYBERCOM (b)(3) 50 USC 3024(h) and (b)(5)

- b. (S//NF) Gather Joint MILDEC staffing requirements and practices from the CCMDs and assess methods to surge MILDEC planners to CCMDs facing facility limitations.

*(U) Joint Staff Deputy Director for Global Operations,  
J-39 Comments*

(CUI) The JS DDGO, J-39 neither agreed nor disagreed with the recommendation, but stated that there is a Deception Capabilities Joint DOTmLPF-P Change Recommendation (DCR) that is currently in the staffing process that makes a similar recommendation. The Joint DCR is sponsored by the JS Directorate for Force Structure, Resources, and Assessments, Deputy Directorate for Force Protection, J-8.

*(U) Our Response*

(CUI) We reviewed the comments from the JS DDGO, J-39 and obtained the referenced DCR, which was approved by the Vice Chairman of the Joint Chiefs of Staff on August 18, 2023. The DCR included a detailed implementation plan with phased execution steps.

CYBERCOM (b)(3) 50 USC 3024(h) and (b)(5)

We also reviewed a related working group update from January 2024 as well as the update brief provided to the April 2024 session of the

CYBERCOM (b)(3) 50 USC

(CUI) The JS DDGO, J-39 response addressed the intent of the recommendation; however the Influence and Perception Management Office did not provide comments to the recommendation. Therefore, the recommendation is unresolved. We will close the recommendation 2.a when the JS provides us the related documentation and outcome of the implementation plan. We will close recommendation when IPMO and the JS provides us the results of the review of the CCMD's deception staffing requirements and practices and potential surge staffing strategies.

*(U) Management Comments Required*

(U) The Influence and Perception Management Office Director, did not respond to the recommendation in the report. We request that the Influence and Perception Management Office Director provide comments within 30 days in response to the final report to address the recommendation.

*(U) Recommendation 3*

(S//NF) We recommend that the following officials conduct an assessment of ways to

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

(U) Finding

a. (CUI) CYBERCOM (b)(3) 50 USC 3024(h)

(U) CYBERCOM (b)(3) 50 USC 3024(h)

### Comments

(CUI) The CYBERCOM (b)(3) 50 USC 3024(h) agreed with the recommendation to conduct an assessment as presented in the report.

### (U) Our Response

(CUI) The CYBERCOM (b)(3) 50 USC 3024(h) agreed to address the recommendation presented in the report; therefore, we consider the recommendation resolved but it will remain open. We will close this recommendation when the CYBERCOM (b)(3) 50 USC 3024(h) provides us documentation showing the results of the assessment and any associated mitigation strategies.

b. (CUI) CYBERCOM (b)(3) 50 USC 3024(h)

### Management Comments Required

(U) The CYBERCOM (b)(3) 50 USC 3024(h) did not respond to the recommendation in the report. Therefore, the recommendation is unresolved. We request that the CYBERCOM (b)(3) 50 USC 3024(h) provide comments within 30 days in response to the final report to address the recommendation.

### (U) Recommendation 4

(S//NF) We recommend that the Influence and Perception Management Office Director, in coordination with the Joint Staff J-3 Deputy Director for Global Operations develop a plan of actions and milestones to implement the findings of the studies on the military deception program previously commissioned by the Office of the Secretary of Defense and the Joint Staff.

### (U) Joint Staff Deputy Director for Global Operations,

#### J-39 Comments

(CUI) The JS DDGO J-39 agreed with the recommendation to develop a plan of action and milestones for any recommendations not addressed by the DCR. The JS DDGO J-39 Chief stated they will work with the IMPO to identify recommendations not addressed by the DCR, assess the feasibility of the remaining recommendations, and develop a plan of action and milestones.

### (U) Our Response

(CUI) The response from the JS DDGO J-39 met the intent of the recommendation, however the Influence and Perception Management Office Director did not respond; therefore the recommendation is unresolved. We will close this recommendation once

(U) Finding

~~(S//)~~ IPMO and the JS DDGO J-39 provided a plan of action and milestones to implement recommendations from previous MILDEC studies not addressed by the DCR and provide documentation describing why any remaining recommendations were not selected for implementation.

***(U) Management Comments Required***

(U) The Influence and Perception Management Office Director, did not respond to the recommendation in the report; therefore, the recommendation is unresolved. We request that the Influence and Perception Management Office Director provide comments within 30 days in response to the final report to address the recommendation.

## (U) Appendix A

### (U) Scope and Methodology

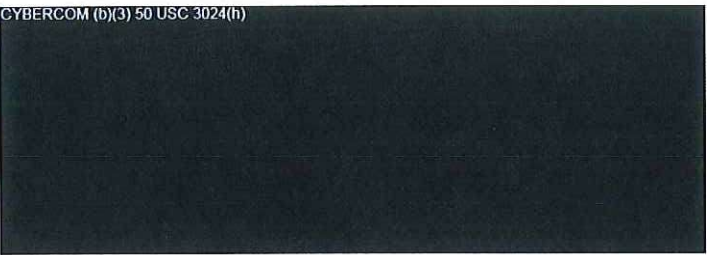
(U) We conducted this evaluation from October 2022 through March 2024 in accordance with the “Quality Standards for Inspection and Evaluation,” published in December 2020 by the Council of Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

(U) We identified and reviewed the following policies, directives, and DoD guidance.

- (U) DoD Instruction S-3604.01, “DoD Deception Activities,” September 18, 2019
- (U) CJCSI 3211.01F, “Joint Policy for Military Deception,” May 14, 2015
- (U) Joint Publication 3-13.4, “Military Deception,” February 14, 2017
- (U) Joint Publication 3-13.4, Appendix C, “Supplemental Guidance,” February 14, 2017
- (S) Joint Staff Memorandum, Deputy Director for Global Operations, J-39, “Interim Implementation Guidance for Joint MILDEC Authorities,” June 2021
- (U) Execute Orders

(U) We obtained, reviewed, and analyzed documentation from MILDEC program stakeholders and organizations, including commander’s guidance, organization charts, briefing slides, concept plans, and operations plans and orders, to determine if officials conducted joint MILDEC operations in accordance with the CCMD commanders’ guidance and objectives. We reviewed current CCMD operations plans; a sample of CCMD EXORDs and joint MILDEC CONOPs and activities for the past 3 years; and current CCMD EXORDs and joint MILDEC CONOPs and activities to determine whether they were planned and conducted in accordance with DoD guidance. A complete list of the classified documents and sources is listed at Appendix C.

(U) We conducted site visits to and interviewed personnel at the following organizations and CONUS and OCONUS locations to gain information about military deception guidance, policies and procedures, best practices, and challenges:

- (U) Office of Under Secretary of Defense (Intelligence & Security), Washington D.C.
  - (U) OUSD(I&S) Collection & Special Programs
  - (U) Influence and Perception Management Office
- (U) Office of the Under Secretary of Defense, Office of General Counsel, Washington D.C.
- (U) Joint Staff Deputy Director for Global Operations, J-39, Washington D.C.
- (U) HQ U.S. CYBERCOM (b)(3) 50 USC 3024(h) 
- (U) HQ U.S.
- (U) HQ U.S.
- (U) HQ U.S.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

## (U) Use of Computer-Processed Data

We did not use computer-processed data to perform this evaluation.

## (U) Prior Coverage

(U) During the last 5 years, the DoD Office of Inspector General (DoD OIG) issued one report discussing military deception planning.

## (U) DoD OIG

(U) Report No. DODIG-2020-039, "Audit of Combatant Commands Integration of Space Operations Into Military Deception Plans," December 13, 2019

(U) This report is classified. To file a Freedom of Information Act request, please submit a request to FOIA.gov.

## (U) Appendix B

### (S//NF) The DoD's MILDEC Program

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

(U) The Joint Requirements Oversight Council (JROC) and Joint Capabilities Integration and Development System (JCIDS) directly support the Chairman of the Joint Chiefs of Staff's effort to identify, assess, and prioritize joint military capability requirements. Validated JCIDS requirements guide acquisition, programming, budgeting, and resourcing efforts to fund, develop, field, and sustain capability solutions for the Warfighter. JCIDS leverages the joint concepts of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTmLPF-P) to focus capability development recommendations.

(S//NF) In the past 15 years, the DoD has commissioned three studies to review the Department's MILDEC program, two capability needs assessments and a training needs assessment. These studies developed findings and recommendations, couched in the DOTmLPF-P framework, with input from the MILDEC community, to improve strategic program development, management, and oversight of the DoD's MILDEC program.

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

### (S//NF) A 2010 Office of the Under Secretary of Defense for Intelligence, Capability Based Assessment Found that the DoD MILDEC Program

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

(S//NF) In 2010, the Office of the Under Secretary of Defense for Intelligence (OUSD[I]), Joint Military Deception Program Office sponsored a capability based assessment. The report published by the RAND National Security Research Institute reviewed the DoD's MILDEC capabilities and developed a draft Capabilities-Based Assessment CBA for submission to JCIDS. The study revealed four key themes and couched them in the JCIDS aligned DOTmLPF-P framework. A major finding from the study identified that

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

(S) The 2010 study also found that doctrine

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

***(U) A 2013 Military Deception and Operations Security Education and Training Needs Assessment Found the Same Broad Issues and Trends for the DoD MILDEC Program***

~~(S)~~ In 2013, OUSD(I) commissioned a Military Deception and Operations Security Education and Training Needs Assessment that was conducted by Booz-Allen-Hamilton. Though the assessment focused on MILDEC education and training, it also identified broader issues and trends that impacted the successful conduct of MILDEC. The study resulted in several findings aligned to DOTmLPF-P recommendations, and included a draft outline of requisite knowledge, skills, and abilities associated with competent MILDEC planning. In addition, the assessment found that

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

***~~(S//NF)~~ A 2024 Joint Staff J-8 Sponsored Review of MILDEC Echoed Findings from the 2010 Study, the DoD MILDEC Program***

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

~~(S//NF)~~ A 2024 Rand study, commissioned by the JS J-8, echoed the key themes made in the previous two studies, again highlighting

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED] The latest report contains many of the same findings as the previous two reports and relates them to the DOTmLPF-P structure, including

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5)

[REDACTED]

## (U) Appendix C

### (U) List of Classified Sources

|                |                                                                                                                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (U) Source 1:  | (U) 2022 National Defense Strategy of the United States of America (March 28, 2022) ( <del>SECRET//NOFORN</del> )<br>Declassification Date: March 28, 2047<br>Date of Source: March 28, 2022            |
| (U) Source 2:  | (U) DOD Instruction S-3604.01 "DOD Deception Activities" (September 18, 2019) ( <del>SECRET</del> )<br>Declassification Date: September 18, 2044<br>Date of Source: September 18, 2019                  |
| (U) Source 3:  | (U) CJCSI 3211.01F Joint Policy For Military Deception (May 14, 2015) ( <del>SECRET//NOFORN</del> )<br>Declassification Date: May 31, 2040<br>Date of Source: May 15, 2015                              |
| (U) Source 4:  | (S) Operation <del>TOP SECRET//NOFORN//ACGM</del> EXORD MOD 1 (December 1, 2021)<br>Declassification Date: January 1, 2072<br>Date of Source: December 1, 2021                                          |
| (U) Source 5:  | (S) Operation <del>TOP SECRET//MCS P/SL C//ORCON//NOFORN//FISA//ACGM</del> EXORD (March 2021)<br>Declassification Date: December 31, 2046<br>Date of Source: March 2021                                 |
| (U) Source 6:  | (S) Operation <del>TOP SECRET//ACGM</del> EXORD (March 4, 2021)<br>Declassification Date: March 5, 2071<br>Date of Source: March 4, 2021                                                                |
| (U) Source 7:  | (S) Operation <del>TOP SECRET//SI//CYBERCOM (b)(3) 50 USC 3024(h) //NOFORN//FISA//ACGM</del> EXORD (December 17, 2021)<br>Declassification Date: January 6, 2072<br>Date of Source: December 17, 2021   |
| (U) Source 8:  | (S//ACGM) Joint MILDEC Plan <del>TOP SECRET//MCS P/SL C//CC//NOFORN//FISA//ACGM</del> (December 29, 2021)<br>Declassification Date: October 28, 2046<br>Date of Source: December 29, 2021               |
| (U) Source 9:  | (U) CT EXORD (September 6, 2012) ( <del>TOP SECRET//SPECAT//MR</del> )<br>Declassification Date: September 6, 2037<br>Date of Source: September 6, 2012                                                 |
| (U) Source 10: | (C//U) Military Deception (MILDEC) Capabilities-Based Assessment Report (January 10, 2010) ( <del>SECRET//NOFORN</del> )<br>Declassification Date: Source marked 1X<br>Date of Source: January 10, 2010 |

(U) Appendixes

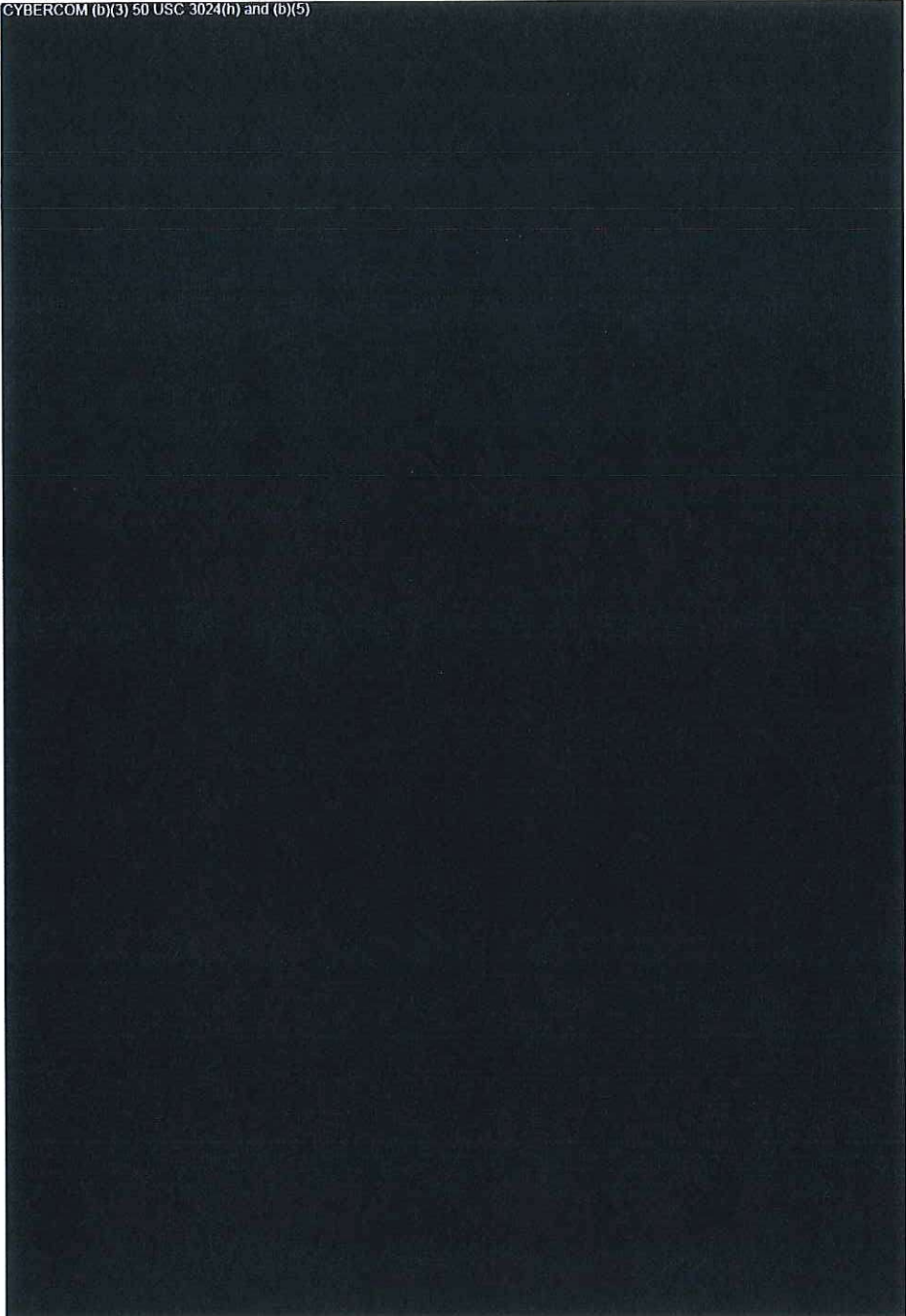
|                |                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (U) Source 11: | (U) Military Deception and Operations Security Education and Training Needs Assessment (ETNA) Final Report (January 3, 2013) ( <del>SECRET</del> )<br>Declassification Date: January 3, 2038<br>Date of Source: January 3, 2013                                                                                                          |
| (U) Source 12: | (U) Chairman of The Joint Chiefs of Staff National Military Strategy (2022) ( <del>SECRET//NOFORN</del> )<br>Declassification Date: August 15, 2047<br>Date of Source: 2022                                                                                                                                                              |
| (U) Source 13: | (U) By Way of Deception (March 2024) ( <del>SECRET//NOFORN</del> )<br>Declassification Date: 50X1HUM<br>Date of Source: March 2024                                                                                                                                                                                                       |
| (U) Source 14: | ( <del>SECRET//ACCM</del> DOWOIG (b)(1) 1.4(a) and (g) ) Military Deception Plan Supporting<br>CYBERCOM (b)(3) 50 USC 3024(h)<br>DOWOIG (b)(1) 1.4(a) and (g) CYBERCOM (b)(3) 50 USC 3024(h)<br>( <del>SECRET//ACCM</del> DOWOIG (b)(1) 1.4(a) and (g) )<br>Declassification Date: January 22, 2031<br>Date of Source: December 16, 2015 |
| (U) Source 15: | ( <del>SECRET//ACCM</del> DOWOIG (b)(1) 1.4(a) and (g) ) TAB B to Appendix 2 to ANNEX C<br>(MILDEC Plan DOWOIG (b)(1) 1.4(a) and (g) ) CYBERCOM (b)(3) 50 USC 3024(h)<br>( <del>SECRET//ACCM</del> DOWOIG (b)(1) 1.4(a) and (g) )<br>Declassification Date: January 22, 2031<br>Date of Source: March 7, 2016                            |

(U) Management Comments

## (U) Management Comments

(U)

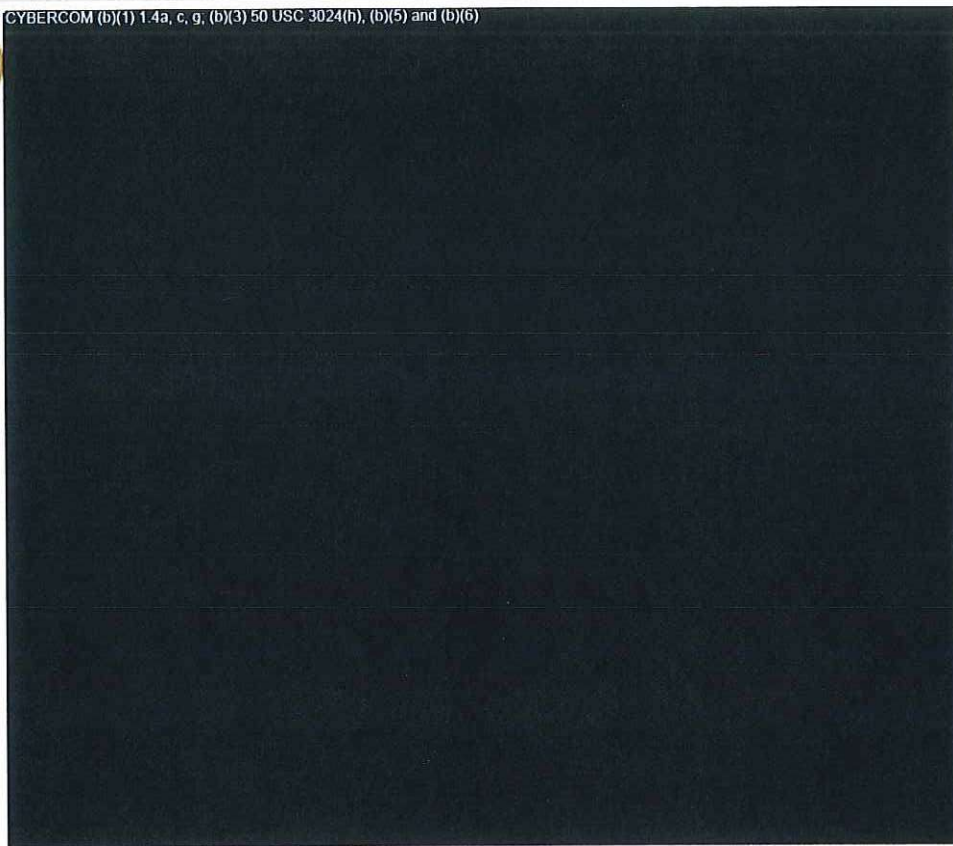
CYBERCOM (b)(3) 50 USC 3024(h) and (b)(5)



(U) Management Comments

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h), (b)(5) and (b)(6)

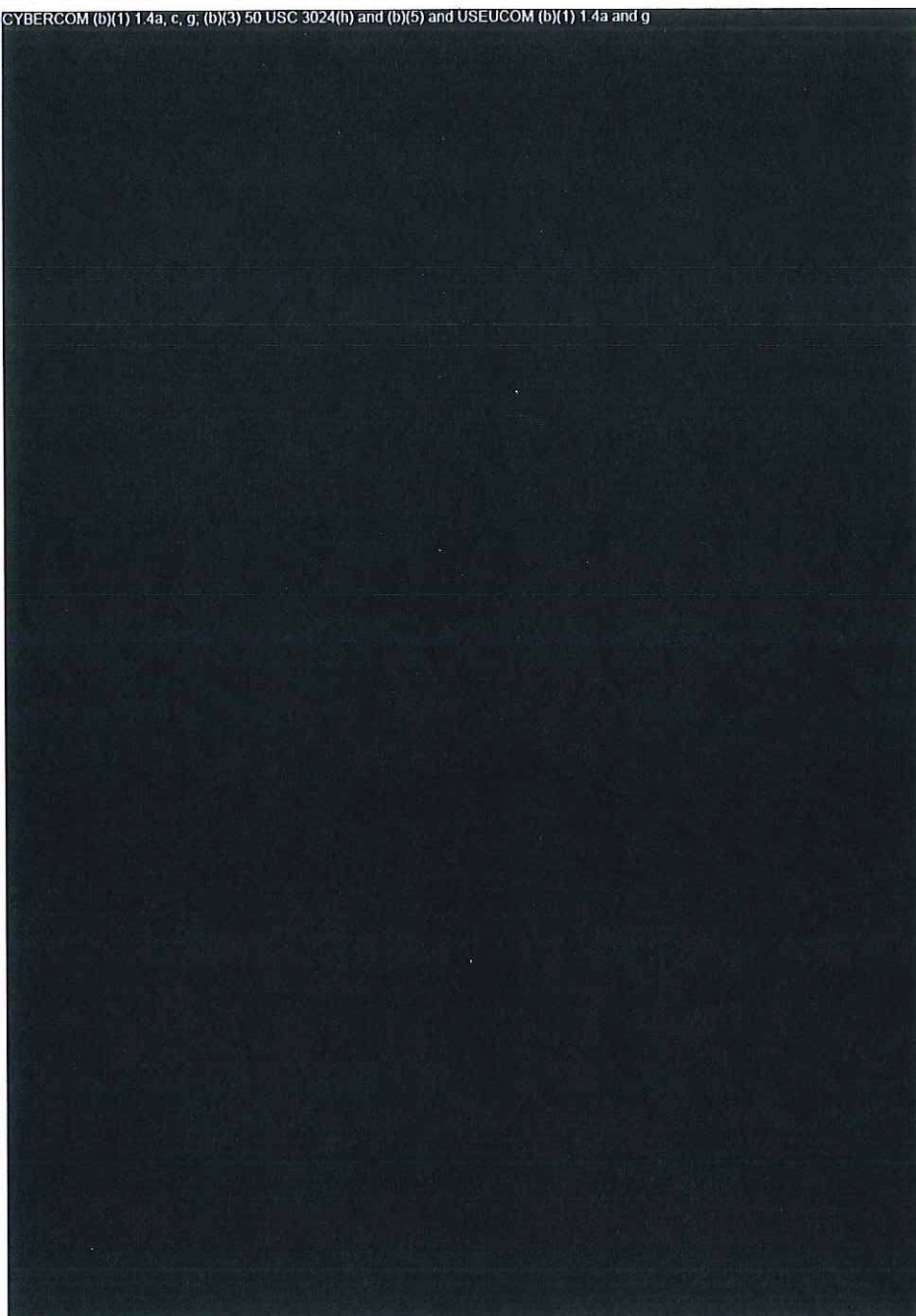
(U)



(U) Management Comments

CYBERCOM (b)(1) 1.4a, c, g, (b)(3) 50 USC 3024(h) and (b)(5) and USEUCOM (b)(1) 1.4a and g

(U)

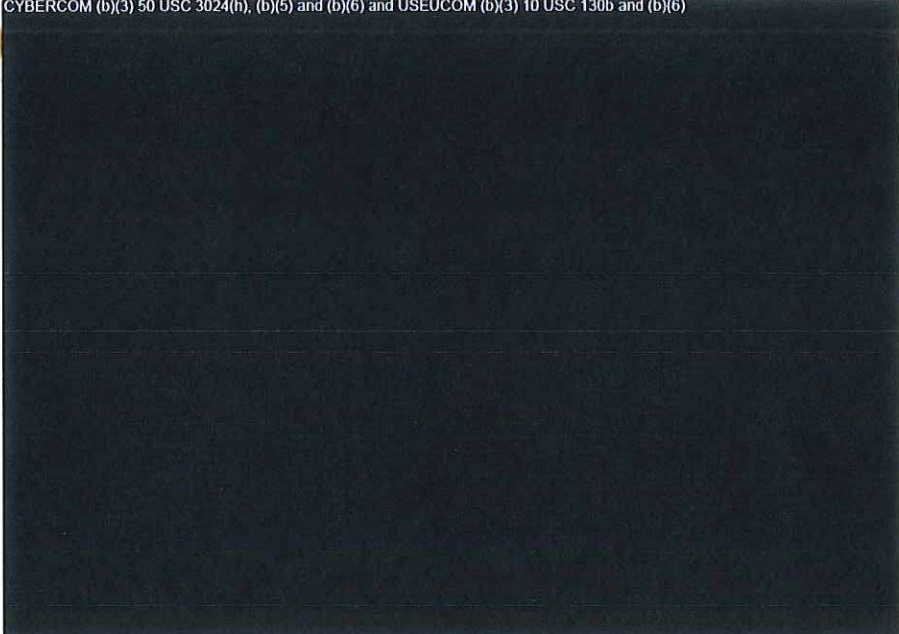


~~SECRET~~

(U) Management Comments

(U)

CYBERCOM (b)(3) 50 USC 3024(h), (b)(5) and (b)(6) and USEUCOM (b)(3) 10 USC 130b and (b)(6)



~~SECRET~~

(U) Management Comments

(U) Joint Staff Deputy Director for Global Operations, J-39



THE JOINT STAFF  
WASHINGTON, DC 20318

Reply Zip Code:  
20318-3000

12 Apr 2024

## MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

**SUBJECT:** Response to the Department of Defense Evaluation of Combatant Command Joint Military Deception Planning Report

1. (U) The Joint Staff J39 Deputy Director for Global Operations (DDGO) concurs the Department of Defense Inspector General Report's four recommendations with the following amplifying information:

a. ~~(S)~~ **Recommendation 1.** The DoDI S-3694.1 is currently in staffing at action officer level coordination. It clarifies the roles and responsibilities of the Defense Deception Activities (DDA) Office of Primary Responsibility (OPR), assigning that role to the Influence and Perception Management Office (IPMO). This addresses the entirety of recommendation number 1.

b. (S) **Recommendation 2.** A Deception Capabilities Joint Doctrine, Organization, Training, materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) Change Recommendation (DCR) has been in the staffing process. This Joint DCR is sponsored by the Joint Staff Directorate for Force Structure, Resources, and Assessments, Deputy Directorate for Force Protection (J-8). The Joint DCR already makes similar recommendations that fall in line with Inspector General Report Recommendation 2.

c. (U) **Recommendation 3.** Concur with this recommendation in its entirety.

d. (b)(1) **Recommendation 4.** The Joint DCR mentioned in paragraph 2 also makes similar recommendations. IPMO, in coordination with the Joint Staff J-39 DDGO will identify any recommendations not addressed by the DCR, and will work with the OPR to have them included. IPMO and the DDGO will assess the feasibility of implementing the remaining recommendations, and then develop a plan action and milestones.

2. (U) The Joint Staff POC is DOWOIG (b)(6)

DOWOI  
G (b)(6)

20

THOMAS A. DONOVAN, RDML, USN  
Deputy Director for Global Operations, J-39

[illegible]

Controlled By: N/A  
CUICategory: N/A  
LIC: N/A  
POC: N/A

**GLI**

(U) Acronyms and Abbreviations

## (U) Acronyms and Abbreviations

(U)

|                                |                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------|
| ACCM                           | Alternative Compensatory Control Measures                                                               |
| CCMD                           | Combatant Command                                                                                       |
| CJCSI                          | Chairman of the Joint Chiefs of Staff Instruction                                                       |
| CMDO                           | Command MILDEC Officer                                                                                  |
| CONOP                          | Concept of the Operation                                                                                |
| DDGO                           | Deputy Director for Global Operations                                                                   |
| DISO                           | Deception in Support of Operations Security                                                             |
| DOTmLPF-P                      | doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy |
| EXORD                          | Execute Order                                                                                           |
| CYBERCOM (b)(3) 50 USC 3024(h) |                                                                                                         |
| DOWOIG (b)(1) 1.4(a) and (g)   |                                                                                                         |
| (a Joint MILDEC plan)          |                                                                                                         |
| JMXRB                          | Joint MILDEC Execution Review Board                                                                     |
| JS                             | Joint Staff                                                                                             |
| MILDEC                         | Military Deception                                                                                      |
| MISO                           | Military Information Support Operations                                                                 |
| MOE                            | Measures of Effectiveness                                                                               |
| MOP                            | Measures of Performance                                                                                 |
| OUUSD(I&S)                     | Office of the Under Secretary for Defense (Intelligence & Security)                                     |
| OUUSD(P)                       | Office of the Under Secretary for Defense (Policy)                                                      |
| CYBERCOM (b)(3) 50 USC 3024(h) |                                                                                                         |
| PM                             | Program Manager                                                                                         |
| RAP                            | Review and Approval Process                                                                             |
| SecDef                         | Secretary of Defense                                                                                    |
| TAC-D                          | Tactical Deception                                                                                      |

CYBERCOM (b)(3) 50 USC 3024(h)

(U)

## **Whistleblower Protection**

### **U.S. DEPARTMENT OF DEFENSE**

*Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto:Whistleblowerprotectioncoordinator@dodig.mil)*

## **For more information about DoD OIG reports or activities, please contact us:**

### **Congressional Liaison**

703.604.8324

### **Media Contact**

[public.affairs@dodig.mil](mailto:public.affairs@dodig.mil); 703.604.8324

### **DoD OIG Mailing Lists**

[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)



[www.twitter.com/DoD\\_IG](https://www.twitter.com/DoD_IG)

### **LinkedIn**

<https://www.linkedin.com/company/dod-inspector-general/>

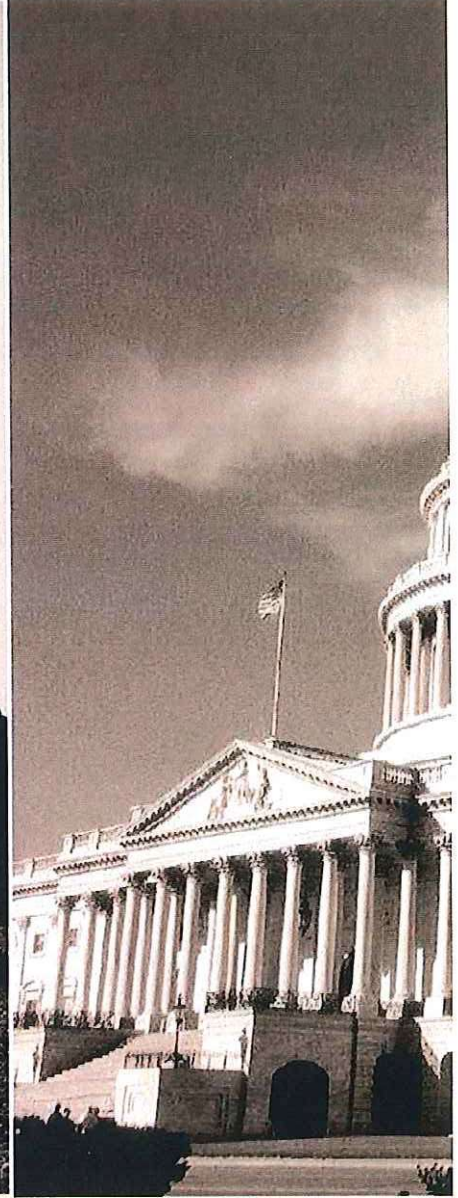
### **DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)

~~TOP SECRET//ACCM-~~

DOWOIG (b)(1) 1.4(a) and (g)

~~//NOFORN~~



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
DoD Hotline 1.800.424.9098

DOWOIG (b)(1) 1.4(a) and (g)

~~TOP SECRET//ACCM-~~

~~//NOFORN~~