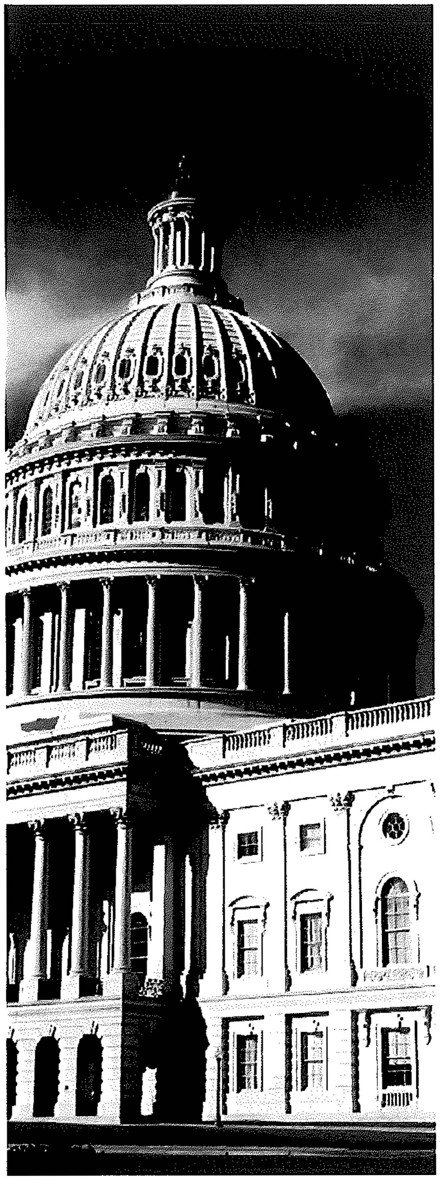
Report No. DODIG-2016-032

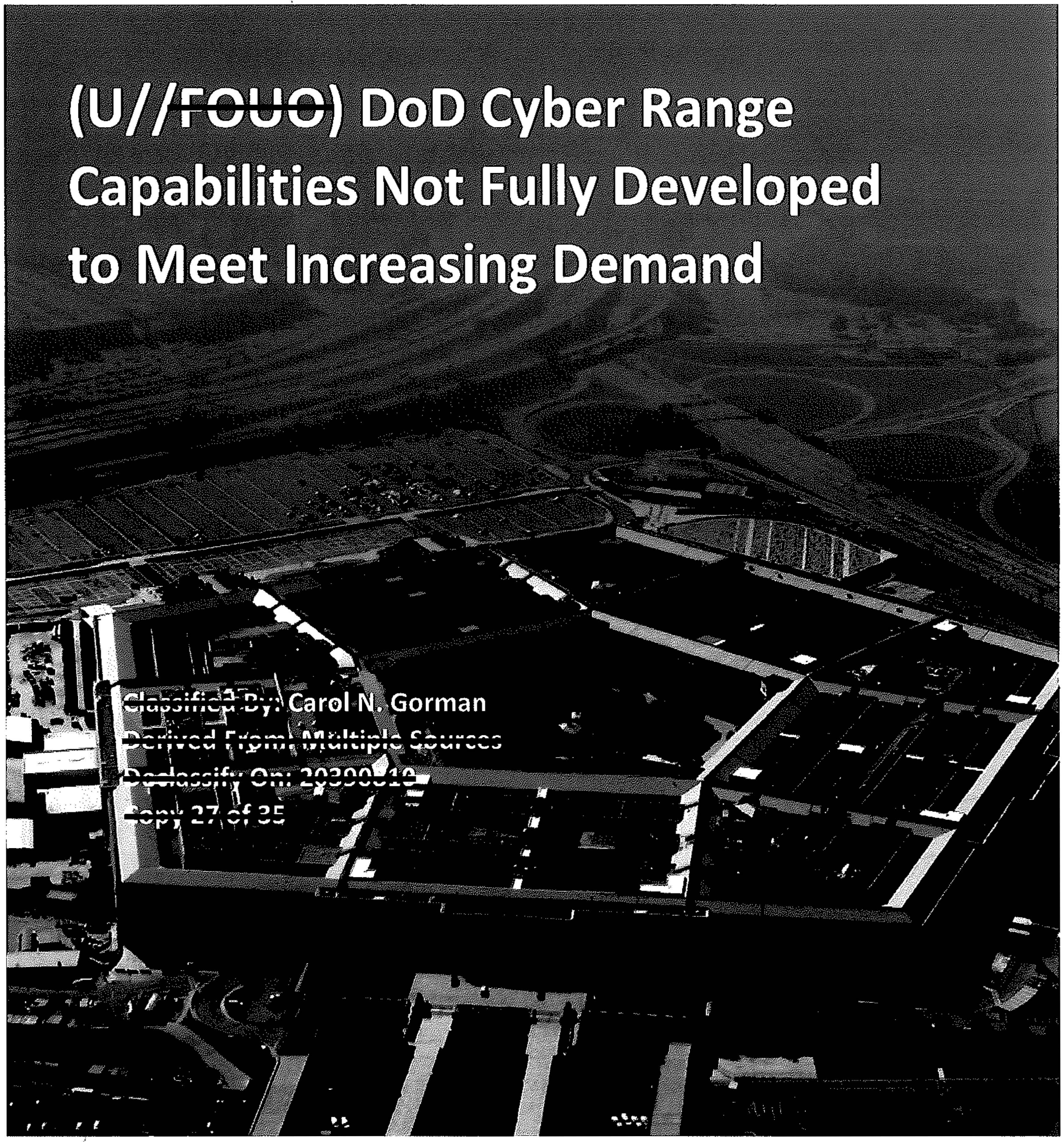
~~SECRET//NOFORN~~

INSPECTOR GENERAL

U.S. Department of Defense

December 18, 2015





(U//~~FOUO~~) DoD Cyber Range Capabilities Not Fully Developed to Meet Increasing Demand

~~Classified By:~~ Carol N. Gorman
~~Derived From: Multiple Sources~~
~~Declassify On: 20390919~~
~~Copy 27 of 35~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~SECRET//NOFORN~~

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|800.424.9098

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

Results in Brief

(U//~~FOUO~~) DoD Cyber Range Capabilities Not Fully Developed to Meet Increasing Demand

December 18, 2015

(U) Objective

(U) To determine whether DoD developed sufficient cyber range capabilities to satisfy the demand for cyber exercises.

(U) Finding

(U//~~FOUO~~) DoD is experiencing an increase in the demand for its cyber range capabilities from the Cyber Mission Force and the acquisition community. However, capabilities and capacity at the four DoD Enterprise Cyber Range Environment (DECRE) cyber ranges have not been fully developed to meet the increasing DoD demand. This occurred because:

- (U//~~FOUO~~) U.S. Cyber Command (USCYBERCOM) and DECRE cyber range officials had not effectively collaborated to define Cyber Environment Requirements for the Cyber Mission Force, and
- (U//~~FOUO~~) DECRE Senior Steering Group had not developed a comprehensive plan of action and milestones (POA&M) to prioritize and address increasing demands from the Cyber Mission Force and the acquisition community.

(~~S//REL TO FVEY~~) As a result, the Cyber Mission Force teams may not achieve full operational capability negatively impacting (~~S//REL TO FVEY~~) the DoD operational cyber mission. In addition, new equipment and systems going through the acquisition process may not receive timely test and evaluation, which may increase acquisition program costs and place quality at risk.

(U//~~FOUO~~) On April 17, 2015, the DECRE Requirements Working Group issued a report based on their assessment of USCYBERCOM's functional Cyber Environment Requirements to determine the timeframes and resources needed to fulfill them. Additionally, the DECRE Requirements Working Group will publish biannual reports reevaluating DECRE's status in fulfilling USCYBERCOM's Cyber Environment Requirements. Therefore, we are not making recommendations to USCYBERCOM and DECRE on the need to further collaborate on requirements.

(U) Recommendation

(U//~~FOUO~~) We recommend that the Chairman of the DECRE Senior Steering Group develop and implement a comprehensive POA&M that would fulfill and prioritize the user requirements collected from the Requirements Management Process. Specifically, this POA&M should address the capability and capacity needs of the DoD cyber range user community and de-conflict competing user requirements. In addition, the POA&M would address the delivery of fully developed cyber range capabilities and capacity to the Cyber Mission Force and the acquisition community in a timely manner.

(U) Management Comments and Our Response

(U//~~FOUO~~) The Chairman of the DECRE Senior Steering Group agreed to develop and implement a POA&M and included one in his response. However, the POA&M only partially addressed the recommendation. Therefore, we request that the Chairman of the DECRE Senior Steering Group provide comments on the final report by January 19, 2016. Please see the Recommendation Table on the next page.

(U) Recommendation Table

Management	Recommendation Requiring Comment
(U) DoD Enterprise Cyber Range Environment Senior Steering Group	Yes

(U) Provide management comments by January 19, 2016.

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

December 18, 2015

MEMORANDUM FOR COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, JOINT STAFF
DIRECTOR, TEST RESOURCE MANAGEMENT CENTER

SUBJECT: (U//~~FOUO~~) DoD Cyber Range Capabilities Not Fully Developed to Meet Increasing Demand (Report No. DODIG-2016-032)

(U//~~FOUO~~) We are providing this report for your review and comment. DoD is experiencing an increase in the demand for its cyber range capabilities from the Cyber Mission Force and the acquisition community. However, capabilities and capacity at the four DoD Enterprise Cyber Range Environment (DECRE) cyber ranges have not been fully developed to meet the increasing DoD demand. We conducted this audit in accordance with generally accepted government auditing standards.

(U) We considered management comments on a draft of this report when preparing the final report. Comments from the Chairman of the DECRE Senior Steering Group partially addressed the recommendation. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, we request that the Chairman of the DECRE Senior Steering Group provide comments on the final report by January 19, 2016. Comments provided on the final report must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01.

(U) Please send a portable document format (PDF) file containing your comments to DoD OIG (b)(6) Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

(U) If you consider any matters to be exempt from public release, you should mark them clearly for Inspector General consideration. We appreciate the courtesies extended to the staff. Please direct questions to me at DoD OIG (b)(6)

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) Contents

(U) Introduction

(U) Objective

(U) Our audit objective was to determine whether DoD has developed sufficient cyber range capabilities[1] to satisfy the demand for cyber exercises. For the purposes of this audit, we focused on the four DoD Enterprise Cyber Range Environment (DECRE) cyber ranges. See Appendix A for a discussion of our scope and methodology.

(U) Background

(U/~~FOUO~~) The DoD Test Resource Management Center, Cyber Range Interoperability Standards Working Group defines a cyber range as a designated set of capabilities to create the environment[2] needed to conduct a cyberspace exercise. Multiple cyber ranges can connect to create one environment for a cyberspace exercise.

(U) The Senate Report 112-173, June 4, 2012, that accompanied the National Defense Authorization Act (NDAA) for FY 2013, identified DoD's need to invest in cyber range capabilities. The Senate Report also stated that despite the importance of cyber range capabilities, comprehensive oversight and strategic planning for DoD cyber ranges did not exist.

(U) The following year, the NDAA for FY 2014,[3] Public Law 113-66, December 26, 2013, required the Secretary of Defense to establish a Principal Cyber Advisor to supervise cyber operations and serve as the principal advisor on military cyber forces and activities. In addition, the NDAA for FY 2014, stated the Principal Cyber Advisor would provide oversight of cyber activities related to offensive missions and oversight of policy and operational considerations, resources, personnel, and acquisition and technology.

(U) Further, the NDAA for FY 2014, required the Secretary of Defense to review existing cyber ranges and adapt one or more such ranges to support the training and exercises of cyber units. In February 2014, the Assistant Secretary of Defense for Homeland Defense testified to the Senate Armed Services Committee that the DECRE governance body would review and oversee DoD cyber range activities. In March 2014, the DECRE Governance Charter was finalized. The charter described the DECRE governance body

[1] (U) The Cyber Range Interoperability Standards Working Group defines a capability as a service, technique, or asset(s) that addresses a specific need. Capabilities can be integrated with other capabilities to create an environment.

[2] (U) U.S. Cyber Command defines an environment as the capability and capacity needed to accomplish either test and evaluation or training and exercise activities.

[3] (U) Section 932, Page 830

(U) as DoD's principal forum established to unify DoD cyber range capabilities, reduce duplication of efforts, and optimize use of limited resources. The DECRE governance body is comprised of the Senior Steering Group (SSG) and separate Working Groups (WG). The DECRE SSG and WGs are made up of the following voting members: U.S. Strategic Command; Joint Staff (JS) Force Development (J7); JS Command, Control, Communications, and Computers (C4) Cyber Directorate (J6); Office of the Director, Test Resource Management Center; and the Office of the Director, Defense Information Systems Agency. The DECRE SSG and WGs also have 17 non-voting members.

(U) On July 17, 2014, the Secretary of Defense designated the Assistant Secretary of Defense for Homeland Defense as the Principal Cyber Advisor.[4]

(U) DECRE Cyber Ranges and Cyber Range Users

(U//~~FOUO~~) The DECRE Governance Charter identifies the following four cyber ranges as part of the initial DECRE enterprise architecture: 1) Joint Information Operations Range (JIOR); Norfolk, Virginia; 2) DoD Cyber Security Range (CSR), DoD OIG (b)(7)(E) [redacted] 3) National Cyber Range (NCR), Orlando, Florida; 4) Command, Control, Communications, and Computers Assessment Division (C4AD), Suffolk, Virginia. Although other DoD-sponsored cyber ranges exist, DECRE selected these four cyber ranges[5] to deliver unified capabilities to the joint DoD community. According to the "Resource Management Decisions for the FY 2014 Budget Request," April 10, 2013, DoD planned to invest in the four DECRE cyber ranges to increase cyber capability development, assessments, and training. Specifically, from FY 2014 through 2018, DoD budgeted an additional $172.3 million in the four ranges to support additional cyber events, transition NCR[6] capabilities for continued DoD use, and to fund civilian billets.

[4] (U) Secretary of Defense Memorandum, "Designation of the DoD Principal Cyber Advisor," July 17, 2014.

[5] (U//~~FOUO~~) Each DECRE cyber range has a unique functional capability or the ability to develop a functional capability according to customer requirements. For example, JIOR's primary functional capability is a secure, accredited closed-loop network. DoD CSR's primary functional capability is the replication of the DoD Information Network. C4AD's primary functional capability is the command and control and cyber environment. NCR's functional capabilities are created and developed according to customer requirements. All of these functional capabilities combined together may form an environment for an exercise or test & evaluation event.

[6] (U//~~FOUO~~) The Defense Advanced Research Projects Agency transferred the NCR to the Test Resource Management Center in FY 2012.

~~(S//REL TO USA, FVEY)~~ The major DECRE cyber range users include the DoD Cyber Mission Force (CMF) and the acquisition community. The CMF uses cyber range environments to: 1) conduct mission rehearsals; 2) conduct test and evaluation of cyber capabilities; 3) train and exercise the 133 CMF teams. The acquisition community uses cyber ranges to conduct developmental and operational testing of systems going through the acquisition process.

(U) Cyber Mission Force Teams

~~(S//REL TO USA, FVEY)~~ On March 6, 2013, USCYBERCOM issued Task Order 13-0244, "Establishment and Presentation of Cyber Mission Force in FY 2013," establishing the CMF. According to the USCYBERCOM's Task Order 13-0244, The CMF's mission is to defend the nation in response to foreign hostile action or imminent threats in cyberspace. When fully staffed, the CMF will be composed of 6,187 cyber personnel in 133 different teams:

- ~~(S//REL TO USA, FVEY)~~ 13 National Mission Teams;
- ~~(S//REL TO USA, FVEY)~~ 68 Cyber Protection Teams;
- ~~(S//REL TO USA, FVEY)~~ 27 Combat Mission Teams;
- ~~(S//REL TO USA, FVEY)~~ 8 National Support Teams; and
- ~~(S//REL TO USA, FVEY)~~ 17 Combat Support Teams.

~~(S//REL TO USA, FVEY)~~ According to the "Execute Order to Implement Cyberspace Operations Command and Control Framework," June 21, 2013, issued by the Chairman of the Joint Chief of Staff, the CMF is expected to achieve full operational capability (FOC) by the end of FY 2016.[7]

~~(S//REL TO USA, FVEY)~~ To achieve certification and FOC status, the CMF teams are required to participate in joint cyber exercises (e.g. Cyber Flag, Cyber Guard, Cyber Knight or similar exercises) and complete other training requirements.

[7] (U/~~FOUO~~) See section on Recent Initiatives Impacting Cyber Ranges that identifies a new FOC date of FY 2018.

(U) Review of Internal Controls

(U//~~FOUO~~) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We found that DECRE cyber range capabilities and capacity were not fully developed to meet the increasing demand from the CMF and the acquisition community. However, during the audit timeframe, USCYBERCOM and DECRE cyber range officials collaborated to assess DECRE's capabilities to meet USCYBERCOM's requirements. Also, USCYBERCOM and DECRE are pursuing solutions to ensure there is adequate cyber range capacity to meet the concurrent demands from the CMFs and the acquisition community. As a result of USCYBERCOM and DECRE's current actions and plans, we are not identifying the deficiencies in this report as internal control weaknesses.

(U) Finding

(U//~~FOUO~~) DoD Cyber Range Capabilities and Capacity Not Fully Developed to Meet Increasing DoD Demand

(U//~~FOUO~~) DoD is experiencing an increase in the demand for its cyber range capabilities from the CMF teams and the acquisition community. However, capabilities and capacity at the four DECRE cyber ranges have not been fully developed to meet the increasing DoD demand. This occurred because:

- (U//~~FOUO~~) USCYBERCOM and DECRE cyber range officials did not effectively collaborate to define Cyber Environment Requirements (CER) for the CMFs, and

- (U//~~FOUO~~) DECRE Senior Steering Group did not develop a comprehensive plan of action and milestones (POA&M) to prioritize and address increasing demands from the CMF and the acquisition community.

~~(S//REL TO USA, FVEY)~~ As a result, there may not be sufficient opportunity for the DoD CMF teams to achieve FOC by the end of FY 2016,[8] which will negatively impact the DoD operational cyber mission. In addition, new equipment and systems going through the acquisition process may not receive timely test and evaluation (T&E), which may increase acquisition program costs and place quality at risk.

(U//~~FOUO~~) CMF's Increasing Demand for Cyber Range Capabilities

~~(S//REL TO USA, FVEY)~~ The demand for cyber range capabilities from the CMF teams is significantly increasing. On December 11, 2012, the Deputy's Management Action Group[9] approved the Cyberspace Force Presentation Model, which established the DoD CMF. By FY 2016, the Services plan to field 133 CMF teams comprised of 6,187 cyber warriors. The CMF teams began forming and training in March 2013.

[8] (U//~~FOUO~~) See section on Recent Initiatives Impacting Cyber Ranges that identifies a new FOC date of FY 2018.

[9] ~~(S//REL TO AUS, CAN, NZL, GBR, USA)~~ Chairman of the Joint Chiefs of Staff, "Execute Order to Implement Cyberspace Operations Command and Control Framework," June 21, 2013.

(U//~~FOUO~~) The CMF teams are trained under the CMF Training Model described in USCYBERCOM's "Cyber Force Concept of Operations & Employment," Annex C, March 31, 2014. The CMF Training Model has four phases: Phase I (Feeder Training); Phase II (Foundation Training); Phase III (Collective Training); and Phase IV (Sustainment). Phase III (Collective Training) requires each CMF team to complete a joint cyber exercise such as Cyber Flag, Cyber Guard, Cyber Knight or similar exercises for certification leading to FOC. After the initial certification, CMF teams are required to be annually re-certified in their skills and abilities under Phase IV (Sustainment). To be re-certified, CMF teams are required at a minimum to complete another annual joint cyber exercise.

(U//~~FOUO~~) According to JS J7's JIOR CMF Cyber Environment Enhancement Issue Paper, September 2014, the requirement to annually certify and re-certify 133 teams will cause the number of joint cyber exercises to increase to a steady state of 133 exercises per year in FY 2017, a 71 percent increase in training requirements from FY 2013.

(U//~~FOUO~~) Acquisition Community's Increasing Demand for Cyber Range Capabilities

(U//~~FOUO~~) The increasing demand for cyber range capabilities from the acquisition community comes from three main sources: 1) developmental testing, 2) operational testing, and 3) Combatant Command cyber assessments.

(U//~~FOUO~~) Based on the Office of the Deputy Assistant Secretary Defense (DASD) for Communications, Command and Control, and Cyber Business (C3CB)'s estimate,[10] the three sources of demand will increase from [redacted] events to [redacted] events ([redacted] percent) beginning in FY 2015 through 2019 (See Table 1).

(U//~~FOUO~~) The three sources of demand will increase from [redacted] events to [redacted] events ([redacted] percent) beginning in FY 2015 through 2019.

[10] (U//~~FOUO~~) Office of the DASD C3CB's Data Collection, Modeling & Analysis, September 2, 2014.

Table 1: (U//~~FOUO~~) Projected Acquisition Community Demand for Cyber T&E

U//~~FOUO~~	# of Cyber Assessment Events					
	FY 2015	**FY 2016**	**FY 2017**	**FY 2018**	**FY 2019**	**Total**
Developmental Testing	DoD OIG: (b) (5) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Operational Testing	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Combatant Command Cyber Assessments	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
						U//~~FOUO~~

Source: (U) Draft – Data Collection, Modeling & Analysis for DECRE Working Group Briefing, September 2, 2014 ~~(S//NF)~~

(U//~~FOUO~~) Developmental testing requires cyber range capabilities to conduct vulnerability assessments, and operational testing uses cyber range capabilities to conduct tests for connectivity, risk reduction, pilot testing, and other types of tests. Combatant Command cyber assessments require cyber range capabilities to demonstrate their ability to accomplish critical missions in contested cyber environments.

(U//~~FOUO~~) The increasing demand for acquisition program T&E events is being driven by DoD Instruction 8510.01, "Risk Management Framework (RMF)[11] for DoD Information Technology," March 12, 2014. DoD Instruction 8510.01 states that the RMF applies to the acquisition processes for all DoD information technology systems that receive, process, store, display, or transmit DoD information. DoD Instruction 8510.01 requires RMF testing activities to be initiated as early as possible in the DoD acquisition processes to increase security and decrease cost. Because these tests are required earlier in the acquisition process, the amount of testing needed for DoD acquisition programs has increased.

(U//~~FOUO~~) The increase in Combatant Command cyber assessments is driven by Congressional directives and DoD guidance. On June 25, 2002, the House of Representatives' Committee on Appropriations directed[12] each Combatant Command and Service to evaluate interoperability and information assurance during major

[11] (U) Committee on National Security Systems Instruction 4009, "National Information Assurance Glossary," April 26, 2010, defines the RMF as a structured approach used to oversee and manage risk for an enterprise.

[12] (U) House of Representatives, Committee on Appropriations, Report 107-532, "Report of the Committee on Appropriations," June 25, 2002, Title IV., "Information Assurance Testing", Page 317.

(U//~~FOUO~~) exercises. On February 11, 2011, the Chairman of the Joint Chiefs of Staff's "Execute Order to Incorporate Realistic Cyberspace Conditions Into Major DoD Exercises," required Combatant Commands to incorporate realistic cyberspace conditions into major exercises. In accordance with these requirements, the Office of the Director for Operational T&E stated[13] they plan to DoD OIG (b)(5) [redacted] An official from the Office of the Director for Operational T&E also confirmed DoD OIG (b)(5) [redacted] of Combatant Command cyber assessments from FY 2015 through FY 2019.

(U//~~FOUO~~) Based on the requirement to train, certify and re-certify 133 CMF teams and the need to support the increase in events from the acquisition community, the DECRE cyber range capabilities and capacity will be exceeded and are not fully developed to meet this demand.

(U//~~FOUO~~) DECRE Cyber Range Capabilities and Capacity Not Fully Developed

(U//~~FOUO~~) The four DECRE cyber ranges do not have the capability and the capacity to meet the demand from the CMF and the acquisition community from FY 2015 through DoD OIG (b) [redacted]. Specifically, the DECRE Requirements Working Group (DRWG)[14] identified several needed capabilities and refinements to support USCYBERCOM's training and exercise priorities. Also, the DECRE cyber ranges confirmed their need for additional capacity to meet the increasing demand from the CMF and the acquisition community.

(U//~~FOUO~~) The four DECRE cyber ranges do not have the capability and the capacity to meet the demand from the CMF and the acquisition community from FY 2015 through DoD OIG (b)(5) [redacted]

(U//~~FOUO~~) DECRE Cyber Range Capabilities Not Fully Developed to Support USCYBERCOM

(U//~~FOUO~~) Specific capabilities are not fully developed to support USCYBERCOM's training and exercise priorities. For example, the DRWG's Assessment of USCYBERCOM Cyber Range Environment Requirements[15] reported the need to develop more realistic

[13] (U//~~FOUO~~) Director, Operational T&E, "Cyber Assessment Issue Paper," Submitted in FY 2014.

[14] (U//~~FOUO~~) The DECRE implemented the DRWG to address and respond to requirements from the cyber range user community.

[15] (U//~~FOUO~~) DECRE Requirement Report, "Assessment of USCYBERCOM Cyber Range Environment Requirements," issued April 17, 2015.

(U/~~/FOUO~~) cyber range environments including greater increased content and volume of traffic generation. The DRWG also stated that automated or semi-automated replications of opposing forces are needed to support the CMF training demand. Further, the DECRE cyber ranges lack the ability to create and store environment templates for rapid use and re-use through a common enterprise process. Lastly, the report stated additional functionality is required to rapidly provide, configure, and re-configure cyber range environments to support different scenarios for multiple training events in a short period of time with the ability to rapidly reset and restore the environment during an event.

(U/~~/FOUO~~) NCR officials also expressed specific challenges in developing blue, red, and gray environments[16] which were confirmed by DRWG's Assessment. Additionally, NCR officials confirmed that DoD OIG (b)(5) [redacted]

(U//~~FOUO~~) DECRE Cyber Range Capacity Cannot Support Increasing Demand

~~(S//REL TO USA, FVEY)~~ DECRE cyber ranges do not have sufficient capacity to satisfy the growing demand to train, certify, and re-certify the CMF and the acquisition community. To execute a joint cyber exercise, USCYBERCOM generally requires support from one or more of the four DECRE cyber ranges. We reviewed three Cyber Guard and three Cyber Flag joint cyber exercises from FY 2012 through 2014.

~~(S)~~ Of the exercises reviewed, two or more ranges provided support in five of the six cyber exercises. Specifically, the DECRE cyber ranges[17] provided hardware, software, and personnel to support each joint cyber exercise.

~~(S)~~ DECRE cyber range capacity is impacted by the length of a joint cyber exercise. According to a USCYBERCOM official, planning between USCYBERCOM, DECRE cyber range officials and other participants can range from 8 to 12 months for a major joint cyber exercise (such as Cyber Flag, Cyber Guard, Cyber Knight or similar exercises). Depending on the complexity of a joint cyber exercise, planning can take as much as 18 months until execution. For example, a USCYBERCOM official stated that Cyber Guard 14-1 took 10 months from planning to execution. The official also stated that Cyber Guard 14-1, like most joint cyber exercises, required detailed planning around exercise

[16] (U) The blue environment represents the DoD Information Network and US critical infrastructures. The red environment represents the potential adversary's network. The gray environment represents the internet including internet traffic and websites.

[17] (U/~~/FOUO~~) C4AD did not support Cyber Guard and Cyber Flag joint cyber exercises because USCYBERCOM did not request C4AD's command and control capabilities until FY 2015.

~~(S)~~ participants and their locations to develop exercise scenarios that were realistic to meet joint cyber exercise objectives.

(U//~~FOUO~~) According to the Cyber Flag 15-1[18] After Action Report, the requirement for CMF collective training far exceeds the number and scope of training events USCYBERCOM and the Services currently deliver. The After Action Report also states that the current USCYBERCOM exercise environment is unstable and unreliable for major exercises and sustained collective training. In addition, an exercise such as Cyber Flag is one of the few venues where CMF teams can come together and conduct collective training. During informal polling of the Cyber Flag 15-1 training audience, observer-controllers found few teams had the opportunity to conduct collective training prior to Cyber Flag 15-1. Further, large-scale exercises like Cyber Flag or Cyber Guard are too infrequent and often lack sufficient capacity and capability to satisfy the growing demand for CMF training.

(U//~~FOUO~~) With respect to the acquisition community, officials from the Office of the DASD for Developmental T&E stated that the length of a T&E event varies depending on the complexity of the event. The "T&E Management Guide," December 2012, describes the T&E process for testing events. Each T&E event begins with identifying critical issues and data requirements. Afterwards, the pre-test analysis determines specific aspects of the event including how to set up the test environment. Tests are then planned and executed to obtain sufficient data to support analysis. In the last stages of the T&E process, the data is analyzed to form conclusions, which help decide a proper course of action. If additional requirements for test data are identified, then the T&E process is repeated. DASD for Developmental T&E officials stated that this process can take anywhere from weeks to months.

(U//~~FOUO~~) DECRE cyber range officials confirmed the lack of capacity to support the increasing demand from the CMF and the acquisition community. Specifically, JIOR officials stated that based on the increasing CMF training timeline and requirements, existing JIOR capacity will not be able to meet the increased demand. In addition, NCR officials stated the increasing demand from CMF and the acquisition community will outstrip their existing resources for both capability and capacity in the near future, and that their existing capacity will be exceeded in FY 2015 and significantly exceeded in FY 2016.

[18] (U//~~FOUO~~) Cyber Flag 15-1 was executed between October 27, 2014, and November 7, 2014, at Nellis Air Force Base in Nevada.

(U//~~FOUO~~) Lack of Collaboration and a POA&M

(U//~~FOUO~~) Capabilities and capacity at the four DECRE cyber ranges have not been fully developed to meet the increasing DoD demand because of ineffective collaboration between USCYBERCOM and DECRE and the lack of a POA&M to prioritize and address competing demands.

(U//~~FOUO~~) Capabilities and capacity at the four DECRE cyber ranges have not been fully developed to meet the increasing DoD demand because of ineffective collaboration between USCYBERCOM and DECRE and the lack of a POA&M to prioritize and address competing demands.

(U//~~FOUO~~) USCYBERCOM and DECRE Cyber Range Officials Did Not Effectively Collaborate

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Collaboration between USCYBERCOM and DECRE cyber range officials to develop USCYBERCOM's CER was ineffective. USCYBERCOM's CER is a document listing USCYBERCOM's requirements for a cyber range environment to conduct multiple types of events including mission rehearsals, Tactics, Techniques, and Procedure development, training and exercises for the CMF, T&E, and science and technology activities. In a June 5, 2014 e-mail, USCYBERCOM asked DECRE cyber range officials for input on the May 15, 2014 CER draft. Additionally, USCYBERCOM required input by June 11, 2014 from DECRE[19] cyber range officials. However, only C4AD provided a response in that time frame.

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ JIOR officials stated that they did not respond because they believed the intent of USCYBERCOM's input request was "to ensure the requirements were generally worded appropriately" and "the requirements actually applied to the cyber environments that the DECRE, and its members are responsible for maintaining and improving." Included in their input, C4AD suggested the requirements should be categorized to support further analysis and decrease redundancies. Also, C4AD officials made recommendations for three additional command and control requirements to be added. As a result, comments from only one of the DECRE cyber ranges were included in the August 8, 2014 release of the CER.

(U//~~FOUO~~) Previous collaboration between USCYBERCOM and DECRE cyber range officials for joint cyber exercises from FY 2012 through 2014 resulted in coordinated capabilities. For example, from FY 2012 through 2014, USCYBERCOM and DECRE cyber range officials participated in regular planning conferences to define exercise

[19] (U//~~FOUO~~) DECRE was established in March 2014, three months from when USCYBERCOM first requested official input from the DECRE cyber ranges about the May 2015 draft of the CER.

(U//~~FOUO~~) requirements for Cyber Guard, Cyber Flag or similar exercises. As a result, DECRE cyber range officials developed cyber range capabilities for each joint cyber exercises (See Appendix B for joint cyber exercises from FY 2012 through 2014). Understanding USCYBERCOM's functional capability and capacity requirements earlier may have enabled the DECRE cyber range officials to start developing their capabilities sooner and to better plan for the increasing demand. The importance of the USCYBERCOM's CER called for a greater need to identify, plan and develop the requirements ahead of time in coordination with the DECRE cyber range officials.

(U//~~FOUO~~) During our audit, USCYBERCOM and DRWG began to fully collaborate and analyze USCYBERCOM's August 2014 version of the CER. The DRWG developed Requests for Information to help build USCYBERCOM's network and supporting infrastructure. The DRWG coordinated with USCYBERCOM's subject matter experts in late January 2015 to ensure agreed understanding of the requirements so DECRE could request additional resources.

(U//~~FOUO~~) As of April 17, 2015, the DRWG issued a report based on their assessment of USCYBERCOM's functional CER and responses from USCYBERCOM on DECRE's Requests for Information. The report categorized the requirements and assessed which requirements could be fulfilled now, which could be developed in a relatively short period, and which would require substantial new resources to develop. The DECRE Chairman sent the report to USCYBERCOM initiating discussion on how to proceed with fulfilling USCYBERCOM's CER. Finally, the DRWG plans to develop biannual follow-up reports reevaluating the status of the DECRE cyber ranges in developing their capabilities to meet USCYBERCOM's CER. We commend USCYBERCOM and DECRE for taking these actions and therefore, we are not making recommendations to USCYBERCOM and DECRE on the need to further collaborate on requirements.

(U//~~FOUO~~) DECRE Started Initiatives But Lacks Comprehensive POA&M

~~(S//NF)~~ Per OSD/JS: (b) (1), 1.4(a) [redacted]

~~(S//NF)~~ Per OSD/JS: (b) (1), 1.4(a) [redacted]

~~(S//NF)~~ Per OSD/JS: (b)(1), 1.4(a) [redacted]

Figure 1: (U//~~FOUO~~) DECRE Requirements Management Process

(U//~~FOUO~~)

DoD OIG: (b)(7)(E) [redacted]

(U//~~FOUO~~)

Source: (U//~~FOUO~~) DECRE Senior Steering Group Briefing, November 19, 2014 ~~(S//NF)~~

~~(S//NF)~~ Per OSD/JS: (b)(1), 1.4(a) [redacted]

[20] ~~(S//NF)~~ Per OSD/JS: (b)(1), 1.4(a) [redacted]

(U//~~FOUO~~) Despite these initiatives, DECRE does not have a comprehensive plan of action to prioritize increasing demands from the CMF and the acquisition community. According to a DECRE official, the RMP is a part of the formalized plan to address the increasing demand from multiple DoD communities. Additionally, the results of the Evaluation of Alternatives will help DECRE officials identify and address cyber range capability and capacity gaps. However, the RMP does not specifically explain how DECRE will prioritize and meet user needs. The Evaluation of Alternatives may address how to prioritize cyber range capabilities and capacity, but as of August 2015, the final report had not been issued.

~~(S//REL TO USA, FVEY)~~ Per OSD:JS: (b)(1), 1.4(a) [redacted]

(U//~~FOUO~~) DoD Cyber Mission and Acquisition Events May Be Negatively Impacted

~~(S//REL TO USA, FVEY)~~ Without the fully developed cyber range capabilities and capacity to meet the increasing DoD CMF and acquisition program demands, the CMF teams may not be able to complete certification events leading to FOC by FY 2016 (see Recent Initiatives Impacting Cyber Ranges) and acquisition events may be negatively impacted.

~~(S//REL TO USA, FVEY)~~ If the CMFs do not attain FOC, then USCYBERCOM's mission to protect the DoD Information Network, provide support to combatant commands, and to defend our nation, may be negatively impacted.

(U//~~FOUO~~) The lack of fully developed cyber range capabilities may also hinder timely test and evaluation for new equipment and systems going through the acquisition process, which may increase acquisition program costs and place quality at risk. The purpose of increased acquisition program testing is to identify cybersecurity weaknesses as early as possible in the acquisition process. This will allow for acquisition decisions to be made earlier in the process preventing acquisition decision delays. In addition, early testing identification will allow for improved mitigation of cybersecurity weaknesses avoiding costly redesigns which usually happen later in the

(U//~~FOUO~~) acquisition process. Further, mitigating cybersecurity weaknesses earlier will reduce exploitation risk. DoD OIG (b)(7)(E) [redacted] According to the Director for Operational T&E, the cybersecurity weaknesses could have been identified earlier in the acquisition process avoiding costly redesigns and acquisition decision delays caused by the mitigation of the cybersecurity weaknesses and retesting of the acquisition program.

(U) Recent Initiatives Impacting Cyber Ranges

(U//~~FOUO~~) The CMF teams are now expected to achieve FOC by FY 2018. According to the Honorable Eric Rosenbach's testimony before the U.S. Senate Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities on April 14, 2015, Mr. Rosenbach stated that once fully manned, trained, and equipped in FY 2018, these 133 teams will execute their missions with nearly 6, 200 military and civilian personnel.

(U//~~FOUO~~) The DECRE SSG's ability to prioritize cyber range capabilities will be impacted by the appointments of the Executive Agents for Training and T&E. According to the NDAA for FY 2015,[21] the Secretary of Defense, in consultation with the Principal Cyber Advisor, shall designate senior DoD officials to act as the Executive Agents for Training and T&E. The Training Executive Agent and T&E Executive Agent will be responsible for establishing the priorities for cyber ranges to meet Department objectives and ensure the cyber ranges meet requirements specified by USCYBERCOM, the training community, and the research, development, testing, and evaluation community. In addition, these Executive Agents will influence DECRE's cyber range investment strategies and funding of DECRE cyber range capabilities for the training and T&E communities. As of October 2015, the Secretary of Defense has not designated appointees for the Training Executive Agent and T&E Executive Agent positions.

[21] (U) Public Law 113-291, "Carl Levin and Howard P. 'Buck' McKeon NDAA for FY 2015," December 19, 2014.

(U) Management Comments on the Finding and Our Response

(U) Chairman of the DECRE SSG Comments

(U//~~FOUO~~) The Chairman, DECRE SSG, disagreed with the Finding stating specifically that he disagreed "with the content and context of the report along with the interpretation of the scope of the DECRE governance charter." The Chairman also provided line-by-line comments on the draft report to be considered as part of his official response. Please see Appendix C for his comments and our responses.

(U//~~FOUO~~) In his response, the Chairman stated that DECRE has implemented effective business processes since its stand up in March 2014 and that its working groups have had excellent participation from multiple DoD stakeholders. He also stated the DECRE charter had only been signed six months prior to the start of the audit and that, since that time, sub-working groups have been assigned to address gaps and shortfalls.

(U//~~FOUO~~) The Chairman reiterated that DECRE cyber ranges have "met every capability development, test, training, readiness, or mission rehearsal event requirement brought to the DECRE ranges – no one has been turned away." He provided a list of the entities in which DECRE has collaborated with to include, the Deputy Secretary of Defense for Developmental Test and Evaluation, the Under Secretary of Defense for AT&L, Office of the Secretary of Defense for Policy, among others.

(U//~~FOUO~~) The Chairman stated that the report's premise was that "collaboration between USCYBERCOM and DECRE was ineffective when in fact, collaboration and active participation was occurring across the Department." The Chairman specifically addressed the CMF requirement, stating that the CMF training needs cannot be met by the cyber ranges alone but require facilities, curriculum, and scenario capabilities as identified in the USCYBERCOM Persistent Training Environment vision. The Chairman added that DECRE requirements for those needs were provided to the DoD higher level cyber investment governance boards but that the DECRE requirements had not been funded to date. The Chairman offered that collaboration must go beyond USCYBERCOM and DECRE to meet CMF training requirements and that funding must be provided.

(U//~~FOUO~~) The Chairman stated that, as directed and funded by the Deputy Secretary of Defense, USCYBERCOM and the Joint Staff achieved an initial PTE capability in FY 2015 and USCYBERCOM had collaborated with the Joint Staff Suffolk facility to meet the near term CMF training needs. Further, the Chairman added that, although DECRE has identified and provided FY 2016 and FY 2017 resource issues, "funding

(U/~~/FOUO)~~ necessary to meet the DECRE validated requirements has not been identified or allocated."

(U/~~/FOUO)~~ The Chairman requested that the information he provided in response to the draft report be used to update the report, to include acknowledging the additional stakeholders who can influence DoD capabilities. Lastly, the Chairman requested that a comment adjudication session be conducted before the final report is published.

(U) Our Response

(U/~~/FOUO)~~ Although the Chairman, DECRE SSG, disagreed with the Finding's content and context, he reiterated the primary message of our audit report, which is that with the increase in the demand for cyber range capabilities, there may not be sufficient opportunity for the DoD CMF teams to timely achieve FOC or that new equipment and systems may not receive timely test and evaluation. For example, the Chairman stated that DECRE requirements for the CMF teams have been submitted but have not been funded to date and that although DECRE submitted FY 2016 and FY 2017 validated requirements that the "funding necessary to meet those requirements had not been identified or allocated." We acknowledge that the lack of funding directly impacts the ability for DECRE to meet the increasing DoD demand for cyber range capabilities and capacity from the CMF teams and the acquisition community.

(U/~~/FOUO)~~ With respect to the DECRE governance charter, the information we include in the report comes directly from the March 2014 charter. The charter states that the DECRE SSG and its separate WGs are DoD's principal forum established to unify DoD cyber range capabilities, reduce duplication of efforts, and optimize use of limited resources. Accordingly, in the report, we acknowledged that DECRE implemented the DRWG to address and respond to requirements from the cyber range user community. We further stated that the DRWG identified several needed capabilities and refinements to support USCYBERCOM's training and exercise priorities.

(U/~~/FOUO)~~ Regarding DECRE fulfilling requirements, we stated that DECRE cyber range officials met the CMF training needs with sufficiently developed capabilities for USCYBERCOM's joint cyber exercises from FY 2012 through 2014.

(U/~~/FOUO)~~ With respect to collaboration, our initial discussion spoke to the lack of collaboration between USCYBERCOM and DECRE during the development of USCYBERCOM's CER. However, we credit USCYBERCOM and DECRE for collaborating to clearly define USCYBERCOM's CER as of April 2015. Because USCYBERCOM and DECRE took those actions during the audit, we did not issue a recommendation to USCYBERCOM and DECRE concerning collaboration. In fact, we commend USCYBERCOM and DECRE in the report.

(U/~~/FOUO~~) We conducted a comment adjudication session with the Chairman on October 9, 2015, and discussed technical changes to the report in response to his comments. As a result of that meeting, we made certain revisions to the report that are included in Appendix C.

(U) USCYBERCOM Comments

(U/~~/FOUO~~) Although not required to comment, the Chief of Staff, USCYBERCOM agreed that USCYBERCOM and DECRE cyber range officials had not effectively collaborated to define Cyber Environment Requirements for the CMF.

(U) Recommendation, Management Comments and Our Response

(U) Recommendation

(U/~~/FOUO~~) We recommend the Chairman of the DoD Enterprise Cyber Range Environment Senior Steering Group develop and implement a comprehensive plan of action and milestones that would fulfill and prioritize the user requirements collected from the Requirements Management Process. Specifically, this plan of action and milestones should address the capability and capacity needs of the DoD cyber range user community and de-conflict competing user requirements. In addition, the plan of action and milestones would address the delivery of fully developed cyber range capabilities and capacity to the Cyber Mission Force and the acquisition community in a timely manner.

(U) Chairman of the DECRE Senior Steering Group Comments

(U/~~/FOUO~~) The Chairman, DECRE SSG agreed to develop a POA&M and included one in his response. The Chairman's POA&M is a one-page pictorial timeline of DECRE's collaboration with USCYBERCOM to define the Cyber Environment Requirements and DECRE's efforts to obtain funding through the Program Objective Memorandum cycle for FY 2017 and 2018. The POA&M also identifies short and long-term cyber range capability gaps that DECRE plans to develop from FY 2017 through 2021.

(U) Our Response

(U/~~/FOUO~~) Comments from the Chairman only partially addressed the intent of the recommendation. We commend the Chairman for developing a POA&M. However, the POA&M does not address the full intent of the recommendation. Specifically, the Chairman did not identify how the DECRE SSG plans to prioritize and de-conflict user requirements collected from the Requirements Management Process to address

(U//~~FOUO~~) capability and capacity needs of the DoD cyber range user community. In addition, the Chairman did not establish specific milestones addressing the delivery of fully developed cyber range capabilities and capacity to the CMF and the acquisition community. Therefore, we ask that the Chairman provide additional comments in response to the final report.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from April 2014 through August 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) To determine whether DoD had developed sufficient cyber range capabilities to satisfy the demand for cyber exercises, we interviewed officials and reviewed policies and procedures from the following organizations:

- (U) U.S. Strategic Command
- (U) USCYBERCOM
- (U) Office of the USD for Policy; DASD for Cyber Policy
- (U) Office of the USD for AT&L; DASD for Developmental T&E
- (U) Office of the Director of Operational T&E
- (U) Office of the USD for AT&L; DASD for C3CB
- (U) Army Cyber Command
- (U) Fleet Cyber Command

(U) Additionally, we interviewed personnel and reviewed policies and procedures from the four DECRE cyber ranges: DoD CSR, JIOR, C4AD, and NCR to determine:

- (U) processes to conduct joint cyber exercises;
- (U) their overall roles and responsibilities;
- (U) unique cyber range capabilities;

- (U) challenges and concerns; and
- (U) budgeting and funding processes for capability development and conducting joint cyber exercises.

(U/~~/FOUO)~~ We obtained and analyzed DoD Cyber Range assessments and reports to support conclusions made about the four DECRE cyber ranges' ability to meet the demands of the user community.

(U/~~/FOUO)~~ We determined whether DECRE cyber range capabilities were sufficient to meet USCYBERCOM's capability needs during Cyber Flag and Cyber Guard exercises for FY's 2012 through 2014. In addition, we determined what capability each DECRE cyber range provided Cyber Flag and Cyber Guard from FY's 2012 through 2014. Specifically, we analyzed Interconnection Security Agreements and After-Action Reports to verify and confirm what capability each cyber range provided.

~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ We also reviewed the following USCYBERCOM guidance to determine whether USCYBERCOM had included input from the DECRE cyber ranges on USCYBERCOM's CER:

- ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ USCYBERCOM "Cyber Environment Requirements", Initial Release 1–Draft, May 15, 2014, Version 0.2
- ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ USCYBERCOM "Cyber Environment Requirements", Initial Release 1, August 8, 2014, Version 0.5

(U) Use of Computer-Processed Data

(U/~~/FOUO)~~ We did not use computer-processed data for this report.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General (DoD IG) issued three reports related to DoD cyber range capabilities. Unrestricted GAO reports can be accessed at http://www/gao.gov, DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

(U) GAO

(U) Report No. GAO-11-75, "Defense Department Cyber Efforts: DoD Faces Challenges In Its Cyber Activities," July 2011

(U) Report No. GAO-11-421, "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 2011

(U) DoD OIG

~~(S//NF)~~ Report No. DODIG-2015-117, "U.S. Cyber Command and Military Services Need to Reassess Processes for Fielding Cyber Mission Force Teams," April 30, 2015

(U) Appendix B

(U//~~FOUO~~) DECRE Cyber Range Officials Sufficiently Developed Capabilities for USCYBERCOM's Joint Cyber Exercises From FY 2012-2014

(U//~~FOUO~~) From FY 2012 through 2014, DECRE cyber range officials sufficiently developed cyber range capabilities to satisfy USCYBERCOM's requirements for joint cyber exercises. For joint cyber exercises in which USCYBERCOM requested capabilities from the DECRE cyber ranges, two or more of the DECRE cyber ranges provided capabilities for five out of six joint cyber exercises. Additonally, three of the four DECRE cyber ranges supported USCYBERCOM's annual joint cyber exercises by providing hardware, software, or personnel support. The fourth cyber range, C4AD, did not participate in USCYBERCOM's joint cyber exercises from FY 2012 through 2014, because USCYBERCOM did not request C4AD's command and control capabilities until FY 2015 (Table 2).

(U//~~FOUO~~) Table 2. Cyber range capability support provided for joint cyber exercises

U//~~FOUO~~

(U) Joint Cyber Exercise	(U) NCR	(U) JIOR	(U) DoD CSR
(U) Cyber Flag 12-1		X	X
(U) Cyber Flag 13-1		X	X
(U) Cyber Flag 14-1	X	X	X
(U) Cyber Guard 12-1		X	X
(U) Cyber Guard 13-1	X	X	X
(U) Cyber Guard 14-1		X	

U//~~FOUO~~

(U) Appendix C

(U//~~FOUO~~) Additional Comments on the Report and Our Response

(U//~~FOUO~~) The Chairman of the DECRE SSG provided 26 additional comments on the draft report as part of his official response. We added reference numbers IG-1 through IG-26 for reference purposes on the right side of his comments. See Page 34. A summary of the Chairman's comments by reference number and our response follows.

(U) Management Comments on the Definition of a Cyber Range

(U//~~FOUO~~) Comment IG-1: The Chairman recommended we replace the "cyber range" definition used in the report with the description identified in the memorandum from the Under Secretary of Defense for AT&L, "Acquisition Oversight and Integration of Department of Defense Cyber Range Infrastructure," May 8, 2015. The memorandum describes a cyber range as the "DoD cyberspace range infrastructure supporting T&E, training, exercises, experimentation, mission rehearsals, science and technology, and research and development."

(U) Our Response

(U//~~FOUO~~) During the audit, DECRE cyber range officials provided the definition from the DoD Test Resource Management Center, Cyber Range Interoperability Standards Working Group, which defines a "cyber range" as a designated set of capabilities to create the environment needed to conduct a cyberspace exercise. The memorandum from the Under Secretary of Defense for AT&L, "Acquisition Oversight and Integration of Department of Defense Cyber Range Infrastructure," May 8, 2015, describes the missions that cyber ranges will support. However, the memorandum does not define a cyber range. Therefore, we did not revise the report.

(U) Management Comments on DECRE's Background

(U//~~FOUO~~) Comment IG-2: The Chairman recommended we add the following information to our report: "In response to the Fiscal Year 2011 NDAA, Section 933, the Department established the Cyber Investment Management Board to facilitate alignment of Department cyber activities across science and technology, requirements, acquisition, development, T&E, and sustainment. As an advisory board to key senior level Department decision-making bodies, the Cyber Investment Management Board serves to ensure cyber investments are effectively planned, executed, and coordinated across the Department."

(U) Our Response

(U//~~FOUO~~) Our report referred to the fact that as early as the NDAA for FY 2013, Congress identified the need to invest in cyber range capabilities. The Chairman's comment addressed a timeframe before the NDAA for FY 2013 and confirmed the identified need. Therefore, we did not revise the report.

(U) Management Comments on DECRE's Background

(U//~~FOUO~~) Comment IG-3: The Chairman recommended we add that the DECRE governance construct was formed as a result of an October 2012 Deputy's Management Action Group that recognized resource challenges and shortfalls to cyber range efficiency and effectiveness across DoD. The Chairman explained that adding the information would show that internal DoD stakeholders were aware of the need to synchronize and potentially integrate joint cyber range capabilities to support growing cyber training and test requirements throughout DoD.

(U) Our Response

(U//~~FOUO~~) Our report identifies that according to Senate Report 112-173, June 4, 2012, DoD identified the need to invest in cyber range capabilities. Therefore, we did not revise the report.

(U) Management Comments on DECRE's Responsibilities

(U//~~FOUO~~) Comment IG-4: The Chairman recommended we delete the statement "In February 2014, the Assistant Secretary of Defense for Homeland Defense testified to the Senate Armed Services Committee that the DECRE governance body would review and oversee DoD cyber range activities." He stated that the testimony was Mr. Rosenbach's prepared statement and was included in his responses to Chairman Levin before the hearing. The original question, "From your position as DASD for Cyber Policy, how do you expect the Department will implement the NDAA legislation?" and Mr. Rosenbach's response was:

> (U//~~FOUO~~) "The Department is working to establish the DECRE governance body to oversee Cyber Range issues. DECRE is currently working on establishing a persistent test and training environment intended to meet the demand of the CMF teams that are being fielded by providing on demand environments for training in both offensive and defensive cyberspace operations. The Department is also conducting an assessment to determine if we have the required cyber range capacity and capability to

> (U//~~FOUO~~) support CMF. This assessment is expected to be completed by October 2014."

(U//~~FOUO~~) The Chairman stated that at the time of this response the DECRE signatories were still working on the roles and responsibilities of the DECRE. The finalized charter states:

> (U//~~FOUO~~) "DECRE SSG ...shall serve as the principal forum within the Department of Defense to inform, coordinate, and resolve DECRE requirements regarding the emulation of the cyberspace domain. This governance construct will synchronize efforts to promote effective and efficient utilization of secure, operationally realistic, and technically representative replications of the cyberspace domain."

(U) Our Response

(U//~~FOUO~~) The context of our statement in the report was to emphasize that DECRE would review and oversee DoD cyber range activities as required by NDAA FY 2014. With respect to DECRE's responsibilities, our statement that the DECRE governance body was established to unify DoD cyber range capabilities, reduce duplication of efforts, and optimize use of limited resources aligns with the Chairman's comment and is in accordance with the DECRE Governance Charter. Therefore, we did not revise the report.

(U) Management Comments on DECRE's Governance Contruct

(U//~~FOUO~~) Comment IG-5: The Chairman recommended we add "construct and its" between governance and charter in the background of the report to provide clarity to the organization's constraints.

(U) Our Response

(U//~~FOUO~~) To meet plain language requirements, we used the term "body" instead of "construct." Therefore, we did not revise the report.

(U) Management Comments on DECRE's Responsibilities

(U//~~FOUO~~) Comments IG-6 and IG-19: The Chairman recommended we add "...and optimize use of limited resources" and "Ranges and organizations are responsible for their respective budgets and event scheduling processes, independent of this governance construct" to provide the limitations of the DECRE.

(U) Our Response

(U/~~FOUO~~) We revised the final report to include "...and optimize use of limited resources." Adding that the ranges and organization are responsible for their respective budgets and events scheduling is unnecessary because in the report background we discuss DoD's budgeting for the four cyber ranges from FY 2014 through 2016. See Page 2.

(U) Management Comments on DECRE Governance Construct and Members

(U/~~FOUO~~) Comments IG-7 and IG-8: The Chairman recommended we identify the voting and non-voting members and specific working groups to show DECRE's organization construct and members.

(U) Our Response

(U/~~FOUO~~) We revised the report to identify that DECRE also has non-voting members. In addition, we added that all members are part of DECRE's Senior Steering Group and separate Working Groups. See Page 2.

(U) Management Comments on DoD Cyberspace Stakeholders and Their Responsibilities

(U/~~FOUO~~) Comments IG-9 and IG-10: The Chairman recommended we add information on the roles and responsibilities and alignment of DoD cyberspace stakeholders as established in the memorandum from the Deputy Secretary of Defense, "Guidance Regarding Cyberspace Roles, Responsibilities, Functions, and Governance within the Department of Defense," June 9, 2014, and the memorandum from the Under Secretary of Defense for AT&L, "Coordination Request on Assignment of T&E and Training Cyber Range Focal Point," November 24, 2014.

(U) Our Response

(U/~~FOUO~~) The scope of the audit was DoD's ability to develop cyber range capabilities to conduct joint cyber exercises. Specifically, we focused on the four DECRE cyber ranges. As stated in the report, the DECRE's mission is to provide a collective strategy and forum to unify DoD cyber range capabilities, mitigate duplication of effort, and optimize use of limited resources according to the DECRE Governance Charter. Therefore, we did not revise the report.

(U) Management Comments on the Updated FOC Year

(U/~~FOUO~~) Comments IG-11, IG-12, IG-13, IG-16, IG-18, and IG-21: The Chairman recommended updating the FOC date for the CMF teams to FY 2018 in reference to the

(U//~~FOUO~~) Mission Analysis for Cyber Operations of DoD, submitted in compliance with the reporting requirement contained in the FY 2014 NDAA, Section 933(d), Public Law 113-66, August 21, 2014.

(U) Our Response

(U//~~FOUO~~) We revised the report to indicate the new FOC date in the "Recent Initiatives Impacting Cyber Ranges" section by referencing the Honorable Eric Rosenbach's testimony before the U.S. Senate Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities on April 14, 2015. Mr. Rosenbach stated that once fully manned, trained, and equipped in FY 2018, 133 Cyber Mission Force teams would execute their missions with nearly 6, 200 military and civilian personnel. See Page 15.

(U) Management Comments on the CMF Teams

(U//~~FOUO~~) Comments IG-11, IG-16, and IG-21: The Chairman recommended we add USCYBERCOM's Task Order 15-0124, "Establishment and Presentation of CMF teams in FY 2015 and FY 2016," which tasks the service cyber components to execute building the CMF teams within FY 2015 and FY 2016 and applies key tasks.

(U) Our Response

(U//~~FOUO~~) We disagree that the report should include the service cyber components' responsibility to build the CMF teams, because the report's focus is the development of cyber range capabilities for joint cyber exercises. USCYBERCOM executes these joint cyber exercises for CMF teams to complete for certification leading to FOC. Therefore, we did not revise the report.

(U) Management Comments on Review of Internal Controls

(U//~~FOUO~~) Comment IG-14: The Chairman recommended we add that the "DRWG developed 7 categories and 40 sub-categories to ensure assessments were properly aligned with the capabilities of the four DECRE cyber ranges" from the DECRE Requirements Report.

(U) Our Response

(U//~~FOUO~~) We acknowledge that DECRE developed 7 categories and 40 sub-categories to understand, assess, and manage USCYBERCOM's Cyber Environment Requirements in the DECRE Requirements Report. However, we disagree that this information should be included in the report, because we confirmed that USCYBERCOM and DECRE cyber range officials collaborated to assess DECRE's capabilities to meet USCYBERCOM's requirements. Also, USCYBERCOM and DECRE are pursuing solutions to ensure there is

(U/~~/FOUO)~~ adequate cyber range capacity to meet the concurrent demands from the CMFs and the acquisition community. Therefore, we did not revise the report.

(U) Management Comments on Fulfilled Requirements

(U/~~/FOUO)~~ Comments IG-15, IG-20, IG-22, and IG-24: The Chairman stated, "To date the DECRE ranges have met every capability development, test, training, readiness, or mission rehearsal event requirement brought to the DECRE ranges" and "no one has been turned away."

(U) Our Response

(U/~~/FOUO)~~ We agree with the Chairman and identified that DECRE cyber range officials sufficiently developed cyber range capabilities to satisfy USCYBERCOM's requirements for joint cyber exercises from FY 2012 through 2014 (See Appendix B). Therefore, we did not revise the report.

(U) Management Comments on DECRE's Responsibilities

(U/~~/FOUO)~~ Comment IG-17: The Chairman recommended we add the various responsibilities of the DECRE Working Group, Senior Steering Group, and the Chairman according to the DECRE Governance Charter to thoroughly explain all of DECRE's responsibilities.

(U) Our Response

(U/~~/FOUO)~~ We stated in the report that the DECRE governance body was comprised of the Senior Steering Group and separate Working Groups. In addition, we list the voting members and identify the number of non-voting members in the DECRE Senior Steering Group and Working Groups. Therefore, we did not revise the report.

(U) Management Comments on Unfunded Requirements

(U/~~/FOUO)~~ Comment IG-23: The Chairman stated that despite DECRE's efforts to submit requirements to the Cyber Coordination Team and the AT&L chaired Cyber Investment Management Board, DECRE's requirements have not been funded to date. As a result, the CMF training needs cannot be met by collaboration between USCYBERCOM and DECRE alone or a collaboration that involves either DECRE or cyber ranges at large.

(U) Our Response

(U/~~/FOUO)~~ We agree with the Chairman. In the report we stated, "We acknowledge that the lack of funding directly impacts the ability for DECRE to meet the increasing

(U//~~FOUO~~) DoD demand for cyber range capabilities and capacity from the CMF teams and the acquisition community." Therefore, we did not revise the report.

(U) Management Comments on the DRWG Report

(U//~~FOUO~~) Comment IG-25: The Chairman recommended stating that the DRWG issued a report about their assessment of USCYBERCOM's Cyber Environment Requirements to distinguish this assessment from other DRWG reports.

(U) Our Response

(U//~~FOUO~~) In the report, we stated "The DECRE Requirements Working Group issued a report based on their assessment of USCYBERCOM's functional Cyber Environment Requirements." Therefore, we did not revise the report.

(U) Management Comments on the Report

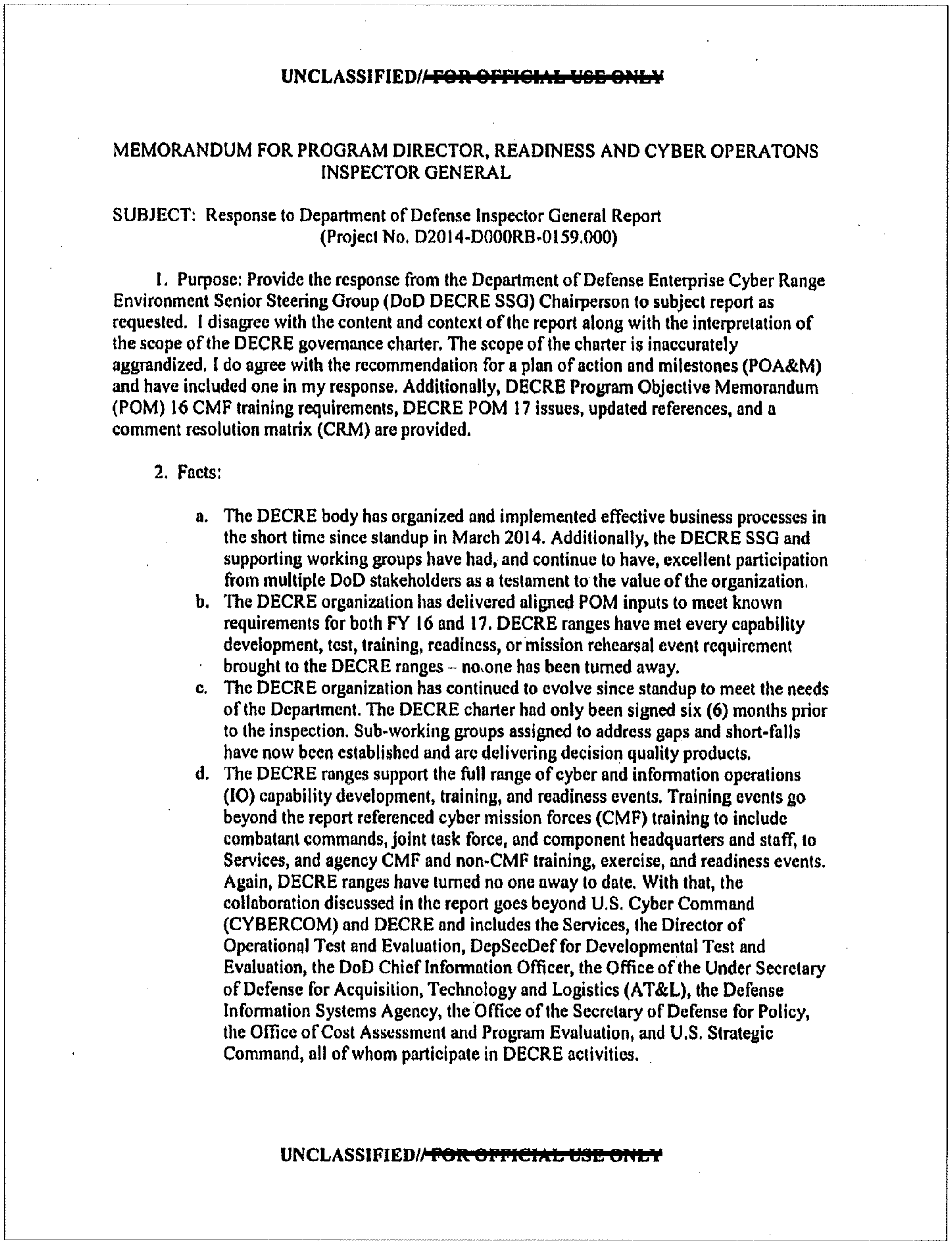
(U//~~FOUO~~) Comment IG-26: The Chairman stated that comments IG-1 through IG-25 apply to the remainder of the report.

(U) Our Response

(U//~~FOUO~~) Please see our responses for comments IG-1 through IG-25.

(U) Management Comments

(U) Chairman of the DECRE Senior Steering Group



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

MEMORANDUM FOR PROGRAM DIRECTOR, READINESS AND CYBER OPERATONS
INSPECTOR GENERAL

SUBJECT: Response to Department of Defense Inspector General Report
(Project No. D2014-D000RB-0159.000)

1. Purpose: Provide the response from the Department of Defense Enterprise Cyber Range Environment Senior Steering Group (DoD DECRE SSG) Chairperson to subject report as requested. I disagree with the content and context of the report along with the interpretation of the scope of the DECRE governance charter. The scope of the charter is inaccurately aggrandized. I do agree with the recommendation for a plan of action and milestones (POA&M) and have included one in my response. Additionally, DECRE Program Objective Memorandum (POM) 16 CMF training requirements, DECRE POM 17 issues, updated references, and a comment resolution matrix (CRM) are provided.

2. Facts:

a. The DECRE body has organized and implemented effective business processes in the short time since standup in March 2014. Additionally, the DECRE SSG and supporting working groups have had, and continue to have, excellent participation from multiple DoD stakeholders as a testament to the value of the organization.

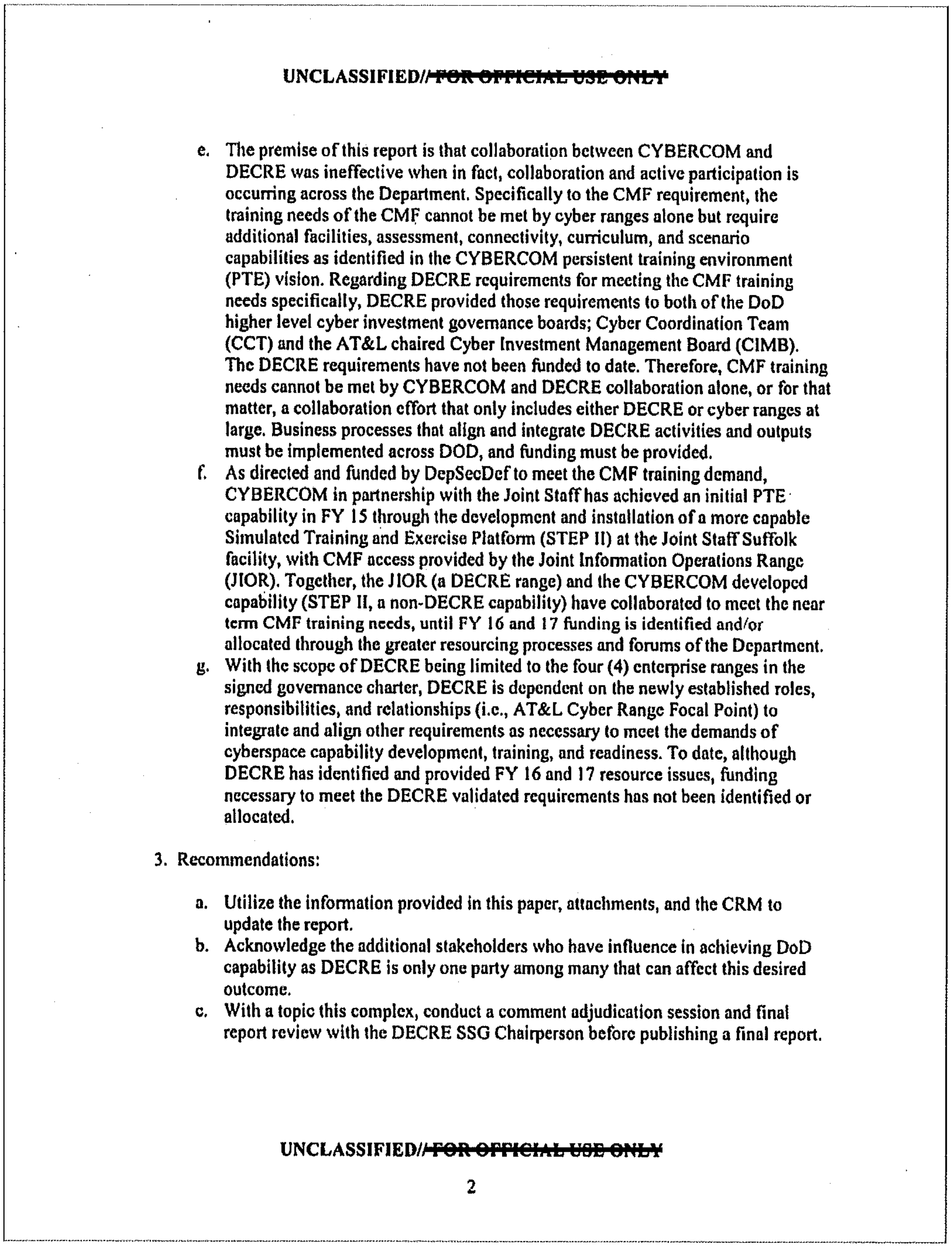
b. The DECRE organization has delivered aligned POM inputs to meet known requirements for both FY 16 and 17. DECRE ranges have met every capability development, test, training, readiness, or mission rehearsal event requirement brought to the DECRE ranges – no one has been turned away.

c. The DECRE organization has continued to evolve since standup to meet the needs of the Department. The DECRE charter had only been signed six (6) months prior to the inspection. Sub-working groups assigned to address gaps and short-falls have now been established and are delivering decision quality products.

d. The DECRE ranges support the full range of cyber and information operations (IO) capability development, training, and readiness events. Training events go beyond the report referenced cyber mission forces (CMF) training to include combatant commands, joint task force, and component headquarters and staff, to Services, and agency CMF and non-CMF training, exercise, and readiness events. Again, DECRE ranges have turned no one away to date. With that, the collaboration discussed in the report goes beyond U.S. Cyber Command (CYBERCOM) and DECRE and includes the Services, the Director of Operational Test and Evaluation, DepSecDef for Developmental Test and Evaluation, the DoD Chief Information Officer, the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (AT&L), the Defense Information Systems Agency, the Office of the Secretary of Defense for Policy, the Office of Cost Assessment and Program Evaluation, and U.S. Strategic Command, all of whom participate in DECRE activities.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Chairman of the DECRE Senior Steering Group (cont'd)



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

e. The premise of this report is that collaboration between CYBERCOM and DECRE was ineffective when in fact, collaboration and active participation is occurring across the Department. Specifically to the CMF requirement, the training needs of the CMF cannot be met by cyber ranges alone but require additional facilities, assessment, connectivity, curriculum, and scenario capabilities as identified in the CYBERCOM persistent training environment (PTE) vision. Regarding DECRE requirements for meeting the CMF training needs specifically, DECRE provided those requirements to both of the DoD higher level cyber investment governance boards; Cyber Coordination Team (CCT) and the AT&L chaired Cyber Investment Management Board (CIMB). The DECRE requirements have not been funded to date. Therefore, CMF training needs cannot be met by CYBERCOM and DECRE collaboration alone, or for that matter, a collaboration effort that only includes either DECRE or cyber ranges at large. Business processes that align and integrate DECRE activities and outputs must be implemented across DOD, and funding must be provided.

f. As directed and funded by DepSecDef to meet the CMF training demand, CYBERCOM in partnership with the Joint Staff has achieved an initial PTE capability in FY 15 through the development and installation of a more capable Simulated Training and Exercise Platform (STEP II) at the Joint Staff Suffolk facility, with CMF access provided by the Joint Information Operations Range (JIOR). Together, the JIOR (a DECRE range) and the CYBERCOM developed capability (STEP II, a non-DECRE capability) have collaborated to meet the near term CMF training needs, until FY 16 and 17 funding is identified and/or allocated through the greater resourcing processes and forums of the Department.

g. With the scope of DECRE being limited to the four (4) enterprise ranges in the signed governance charter, DECRE is dependent on the newly established roles, responsibilities, and relationships (i.e., AT&L Cyber Range Focal Point) to integrate and align other requirements as necessary to meet the demands of cyberspace capability development, training, and readiness. To date, although DECRE has identified and provided FY 16 and 17 resource issues, funding necessary to meet the DECRE validated requirements has not been identified or allocated.

3. Recommendations:

a. Utilize the information provided in this paper, attachments, and the CRM to update the report.

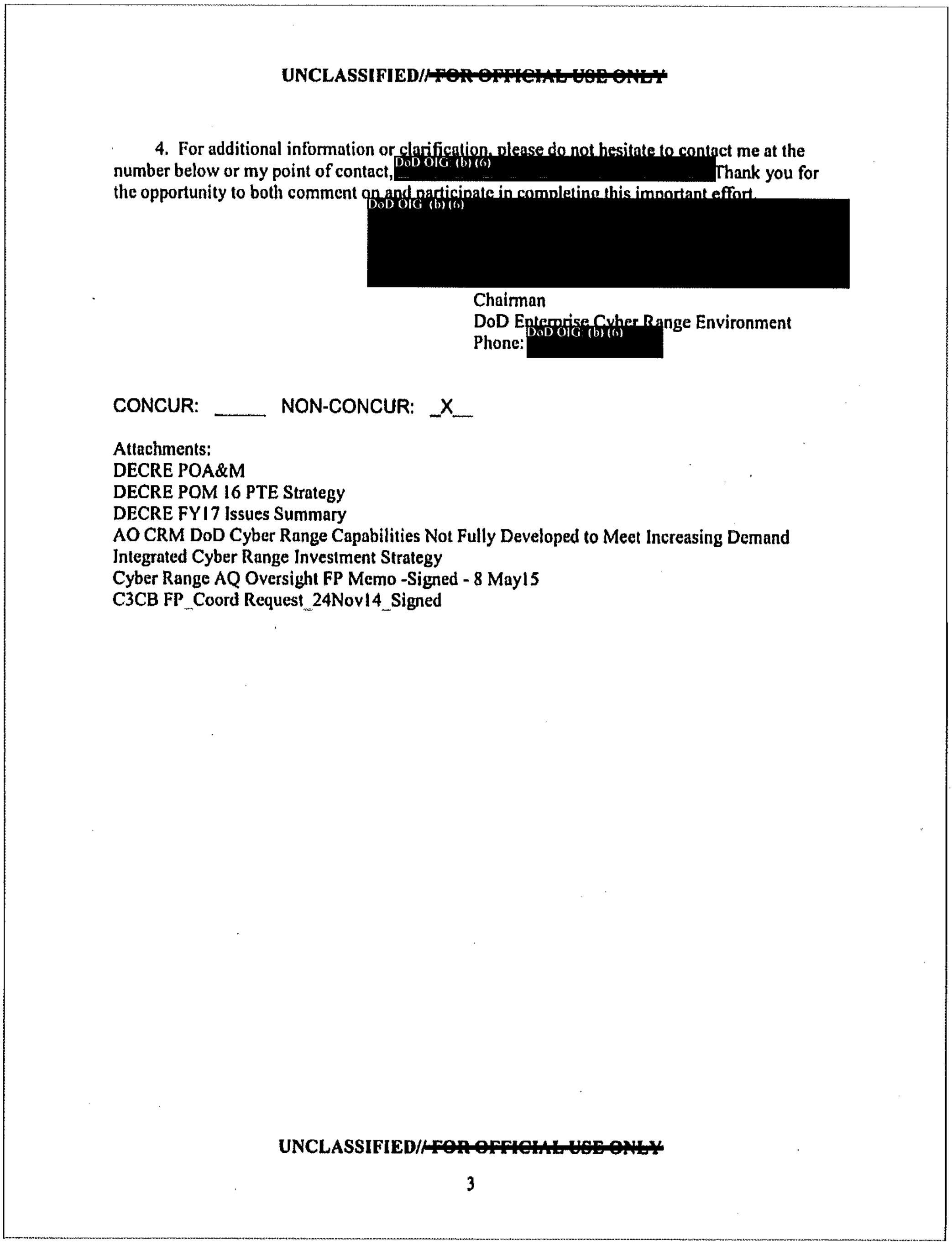
b. Acknowledge the additional stakeholders who have influence in achieving DoD capability as DECRE is only one party among many that can affect this desired outcome.

c. With a topic this complex, conduct a comment adjudication session and final report review with the DECRE SSG Chairperson before publishing a final report.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

2

(U) Chairman of the DECRE Senior Steering Group (cont'd)



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

4. For additional information or clarification, please do not hesitate to contact me at the number below or my point of contact, DoD OIG (b)(6) Thank you for the opportunity to both comment on and participate in completing this important effort.

DoD OIG (b)(6)

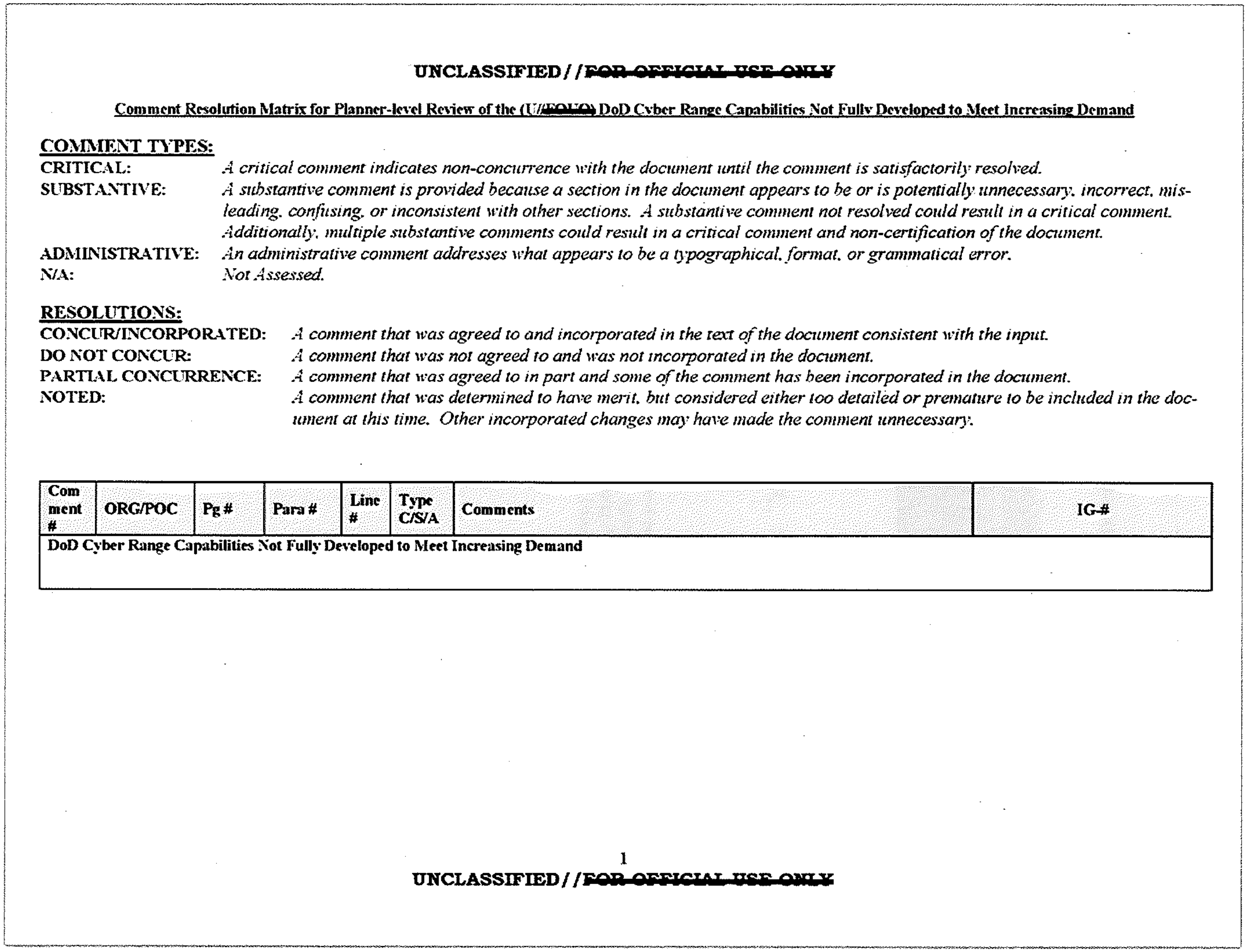
Chairman
DoD Enterprise Cyber Range Environment
Phone: DoD OIG (b)(6)

CONCUR: _____ NON-CONCUR: _X__

Attachments:
DECRE POA&M
DECRE POM 16 PTE Strategy
DECRE FY17 Issues Summary
AO CRM DoD Cyber Range Capabilities Not Fully Developed to Meet Increasing Demand
Integrated Cyber Range Investment Strategy
Cyber Range AQ Oversight FP Memo -Signed - 8 May15
C3CB FP_Coord Request_24Nov14_Signed

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

3



Comment Resolution Matrix for Planner-level Review of the (U//~~FOUO~~) DoD Cyber Range Capabilities Not Fully Developed to Meet Increasing Demand

COMMENT TYPES:

CRITICAL: *A critical comment indicates non-concurrence with the document until the comment is satisfactorily resolved.*

SUBSTANTIVE: *A substantive comment is provided because a section in the document appears to be or is potentially unnecessary, incorrect, misleading, confusing, or inconsistent with other sections. A substantive comment not resolved could result in a critical comment. Additionally, multiple substantive comments could result in a critical comment and non-certification of the document.*

ADMINISTRATIVE: *An administrative comment addresses what appears to be a typographical, format, or grammatical error.*

N/A: *Not Assessed.*

RESOLUTIONS:

CONCUR/INCORPORATED: *A comment that was agreed to and incorporated in the text of the document consistent with the input.*

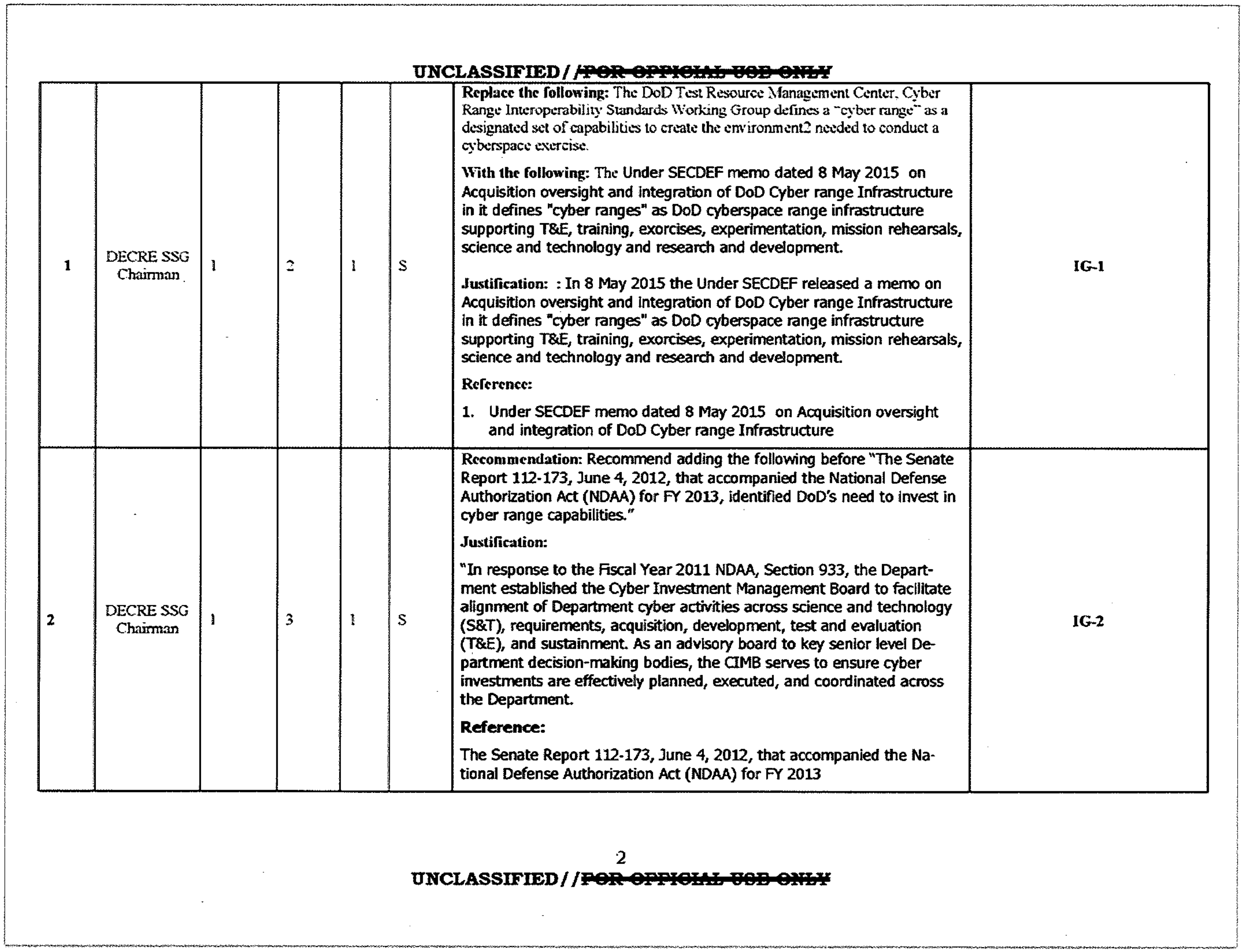
DO NOT CONCUR: *A comment that was not agreed to and was not incorporated in the document.*

PARTIAL CONCURRENCE: *A comment that was agreed to in part and some of the comment has been incorporated in the document.*

NOTED: *A comment that was determined to have merit, but considered either too detailed or premature to be included in the document at this time. Other incorporated changes may have made the comment unnecessary.*

Comment #	ORG/POC	Pg #	Para #	Line #	Type C/S/A	Comments	IG-#
DoD Cyber Range Capabilities Not Fully Developed to Meet Increasing Demand							

(U) Comment Resolution Matrix (cont'd)



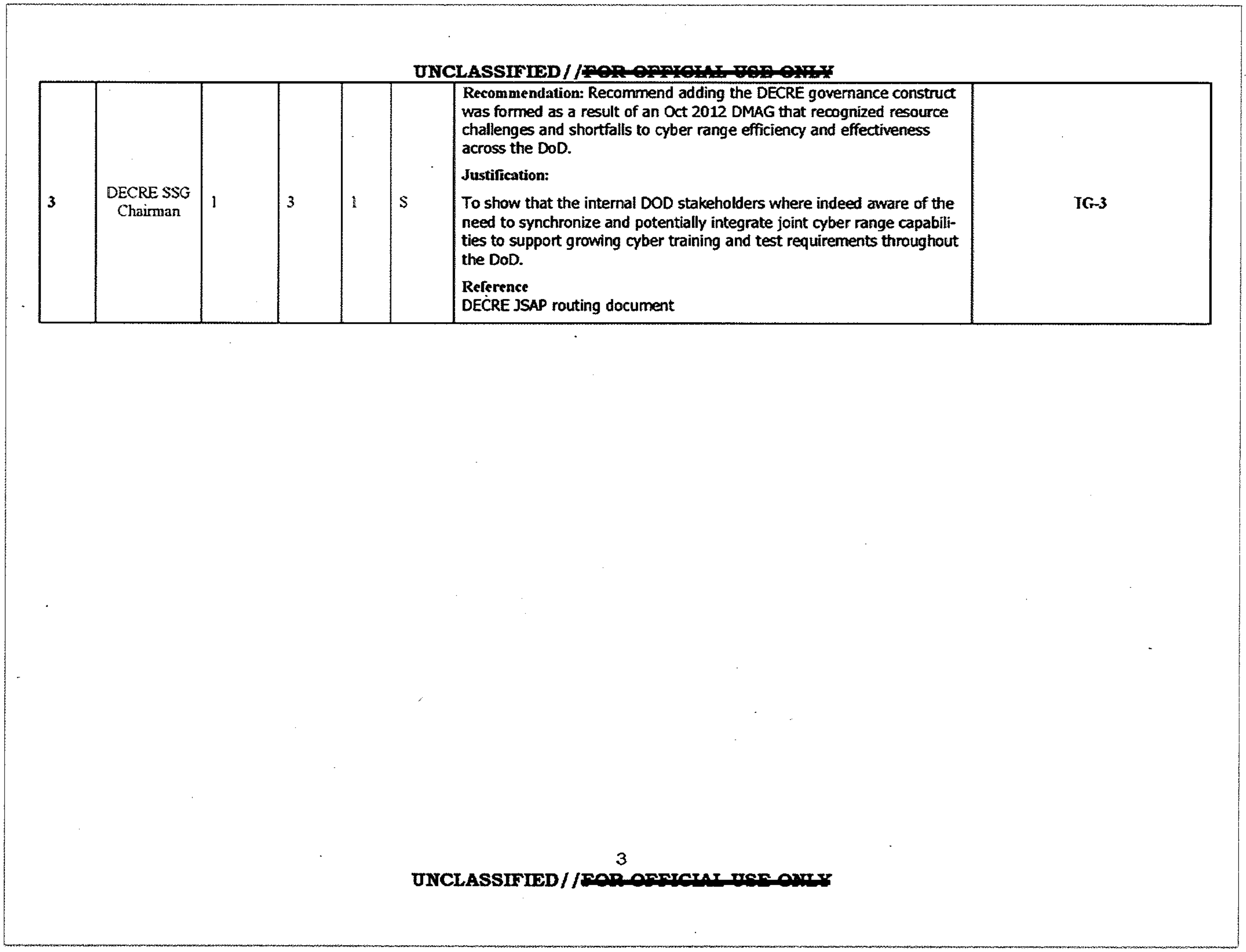
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

1	DECRE SSG Chairman	1	2	1	S	**Replace the following:** The DoD Test Resource Management Center, Cyber Range Interoperability Standards Working Group defines a "cyber range" as a designated set of capabilities to create the environment2 needed to conduct a cyberspace exercise. **With the following:** The Under SECDEF memo dated 8 May 2015 on Acquisition oversight and integration of DoD Cyber range Infrastructure in it defines "cyber ranges" as DoD cyberspace range infrastructure supporting T&E, training, exorcises, experimentation, mission rehearsals, science and technology and research and development. **Justification:** : In 8 May 2015 the Under SECDEF released a memo on Acquisition oversight and integration of DoD Cyber range Infrastructure in it defines "cyber ranges" as DoD cyberspace range infrastructure supporting T&E, training, exorcises, experimentation, mission rehearsals, science and technology and research and development. **Reference:** 1. Under SECDEF memo dated 8 May 2015 on Acquisition oversight and integration of DoD Cyber range Infrastructure	IG-1
2	DECRE SSG Chairman	1	3	1	S	**Recommendation:** Recommend adding the following before "The Senate Report 112-173, June 4, 2012, that accompanied the National Defense Authorization Act (NDAA) for FY 2013, identified DoD's need to invest in cyber range capabilities." **Justification:** "In response to the Fiscal Year 2011 NDAA, Section 933, the Department established the Cyber Investment Management Board to facilitate alignment of Department cyber activities across science and technology (S&T), requirements, acquisition, development, test and evaluation (T&E), and sustainment. As an advisory board to key senior level Department decision-making bodies, the CIMB serves to ensure cyber investments are effectively planned, executed, and coordinated across the Department. **Reference:** The Senate Report 112-173, June 4, 2012, that accompanied the National Defense Authorization Act (NDAA) for FY 2013	IG-2

2

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Comment Resolution Matrix (cont'd)



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

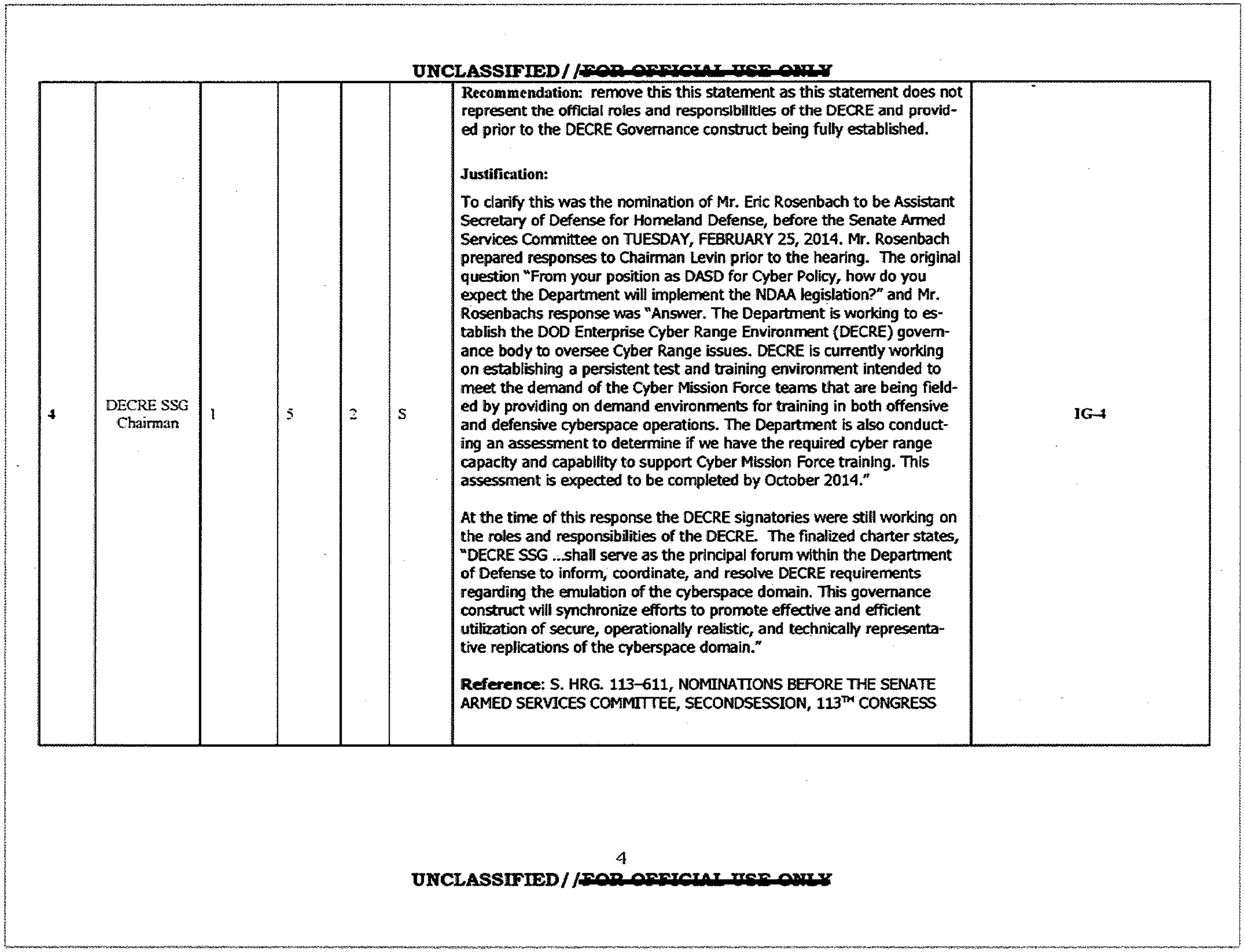
3	DECRE SSG Chairman	1	3	1	S	**Recommendation:** Recommend adding the DECRE governance construct was formed as a result of an Oct 2012 DMAG that recognized resource challenges and shortfalls to cyber range efficiency and effectiveness across the DoD. **Justification:** To show that the internal DOD stakeholders where indeed aware of the need to synchronize and potentially integrate joint cyber range capabilities to support growing cyber training and test requirements throughout the DoD. **Reference** DECRE JSAP routing document	IG-3

3

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

(U) Comment Resolution Matrix (cont'd)



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

4	DECRE SSG Chairman	1	5	2	S	**Recommendation:** remove this this statement as this statement does not represent the official roles and responsibilities of the DECRE and provided prior to the DECRE Governance construct being fully established. **Justification:** To clarify this was the nomination of Mr. Eric Rosenbach to be Assistant Secretary of Defense for Homeland Defense, before the Senate Armed Services Committee on TUESDAY, FEBRUARY 25, 2014. Mr. Rosenbach prepared responses to Chairman Levin prior to the hearing. The original question "From your position as DASD for Cyber Policy, how do you expect the Department will implement the NDAA legislation?" and Mr. Rosenbachs response was "Answer. The Department is working to establish the DOD Enterprise Cyber Range Environment (DECRE) governance body to oversee Cyber Range issues. DECRE is currently working on establishing a persistent test and training environment intended to meet the demand of the Cyber Mission Force teams that are being fielded by providing on demand environments for training in both offensive and defensive cyberspace operations. The Department is also conducting an assessment to determine if we have the required cyber range capacity and capability to support Cyber Mission Force training. This assessment is expected to be completed by October 2014." At the time of this response the DECRE signatories were still working on the roles and responsibilities of the DECRE. The finalized charter states, "DECRE SSG ...shall serve as the principal forum within the Department of Defense to inform, coordinate, and resolve DECRE requirements regarding the emulation of the cyberspace domain. This governance construct will synchronize efforts to promote effective and efficient utilization of secure, operationally realistic, and technically representative replications of the cyberspace domain." **Reference:** S. HRG. 113–611, NOMINATIONS BEFORE THE SENATE ARMED SERVICES COMMITTEE, SECONDSESSION, 113TH CONGRESS	IG-4

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Comment Resolution Matrix (cont'd)

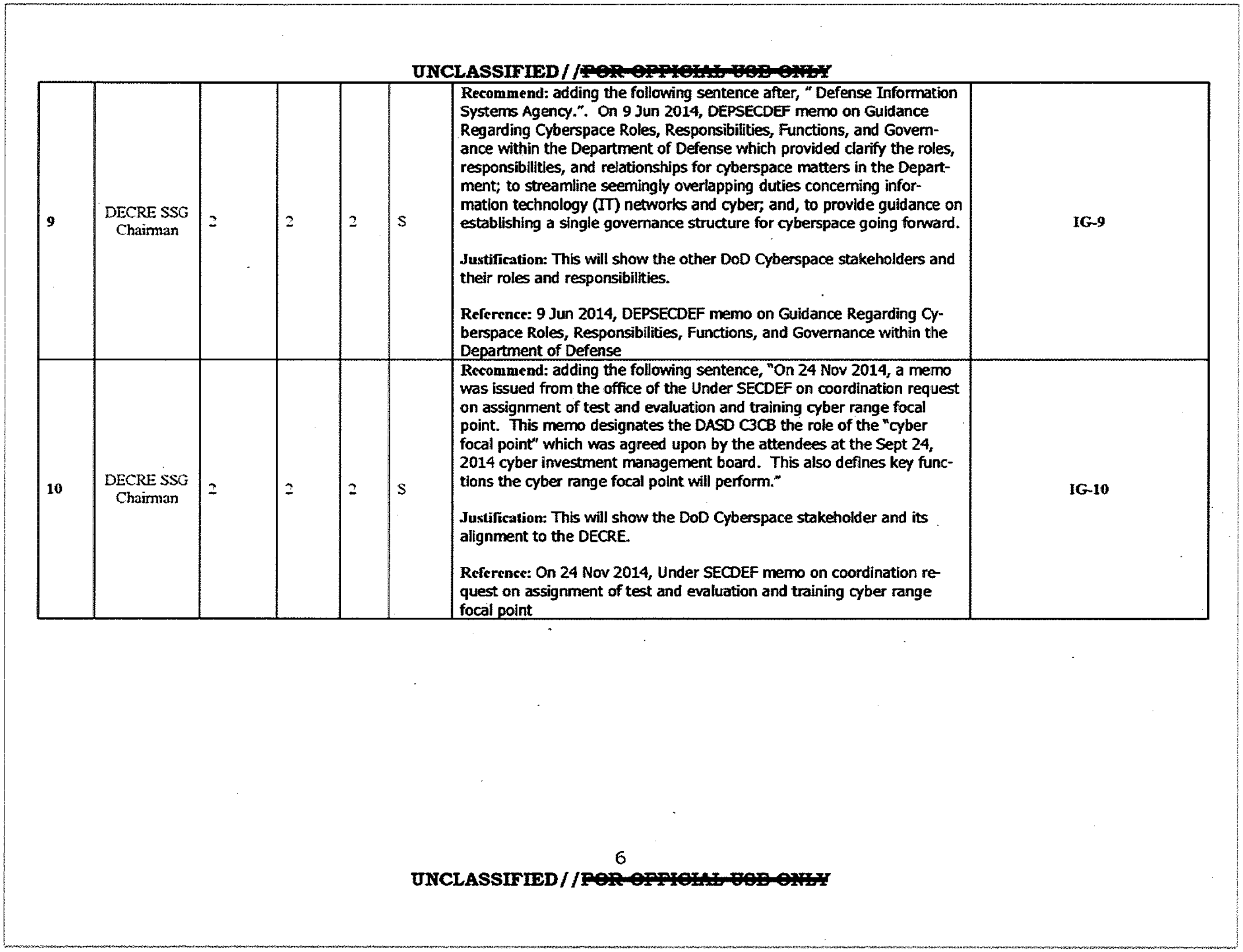
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

5	DECRE SSG Chairman	2	1	1	S	**Recommendation:** recommend adding "construct and its" between governance and charter **Justification:** to provide clarity to the organizations constraints. **Reference:** DECRE Charter	IG-5
6	DECRE SSG Chairman	2	1	1	S	**Recommend:** Adding after "…and optimize use of limited resources." "Ranges and organizations are responsible for their respective budgets and event scheduling processes, independent of this governance construct." **Justification:** This is provide the limitations of the DECRE **Reference:** DECRE Charter	IG-6 **Revised on page 2**
7	DECRE SSG Chairman	2	1	1	S	**Recommend:** recommend adding after "The DECRE governance body is made up of the following voting members", "for the DECRE SSG and the O6/GS15 WG", **Justification:** This will provide the organization construct DECRE **Reference:** DECRE Charter	IG-7 **Revised on page 2**
8	DECRE SSG Chairman	2	2	2	S	**Recommendation:** add the following sentence after "Defense Information Systems Agency." "DECRE is also comprised of 17 non-voting members: Headquarters, US Army; Headquarters, US Marine Corps; Headquarters, US Navy; Headquarters, US Air Force; National Guard Bureau; Office of the Director, Operational Test and Evaluation (DOT&E); Office of the Under Secretary of Defense for Personnel and Readiness; Office of the Under Secretary of Defense for Policy (OUSD(P)); Office of the Under Secretary of Defense, Intelligence (OUSD(I)); Office of the Director, Cost Assessment and Program Evaluation (CAPE); Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DOT&E); Office of the Deputy Assistant Secretary of Defense for C3 and Cyber (DASD C3CB); Joint Staff Operations Directorate (J3); National Security Agency (NSA); DoD Chief Information Office (DoD CIO); United States Cyber Command (USCC); United States Special Operations Command (USSOCOM)" **Justification:** This will show the completeness and makeup of the DECRE members. **Reference:** DECRE Charter	IG-8 **Revised on page 2**

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

(U) Comment Resolution Matrix (cont'd)

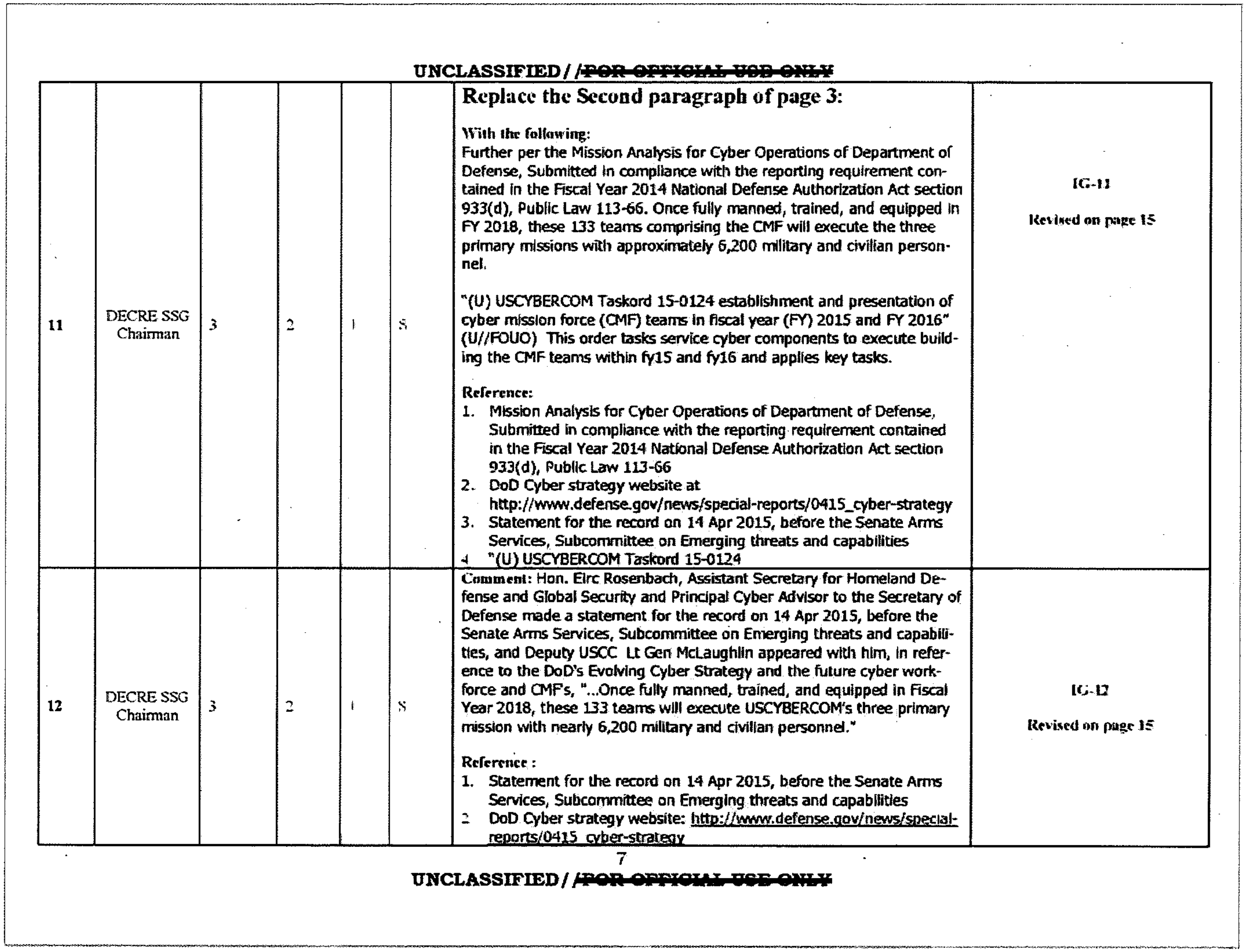


UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

9	DECRE SSG Chairman	2	2	2	S	**Recommend:** adding the following sentence after, " Defense Information Systems Agency.". On 9 Jun 2014, DEPSECDEF memo on Guidance Regarding Cyberspace Roles, Responsibilities, Functions, and Governance within the Department of Defense which provided clarify the roles, responsibilities, and relationships for cyberspace matters in the Department; to streamline seemingly overlapping duties concerning information technology (IT) networks and cyber; and, to provide guidance on establishing a single governance structure for cyberspace going forward. **Justification:** This will show the other DoD Cyberspace stakeholders and their roles and responsibilities. **Reference:** 9 Jun 2014, DEPSECDEF memo on Guidance Regarding Cyberspace Roles, Responsibilities, Functions, and Governance within the Department of Defense	IG-9
10	DECRE SSG Chairman	2	2	2	S	**Recommend:** adding the following sentence, "On 24 Nov 2014, a memo was issued from the office of the Under SECDEF on coordination request on assignment of test and evaluation and training cyber range focal point. This memo designates the DASD C3CB the role of the "cyber focal point" which was agreed upon by the attendees at the Sept 24, 2014 cyber investment management board. This also defines key functions the cyber range focal point will perform." **Justification:** This will show the DoD Cyberspace stakeholder and its alignment to the DECRE. **Reference:** On 24 Nov 2014, Under SECDEF memo on coordination request on assignment of test and evaluation and training cyber range focal point	IG-10

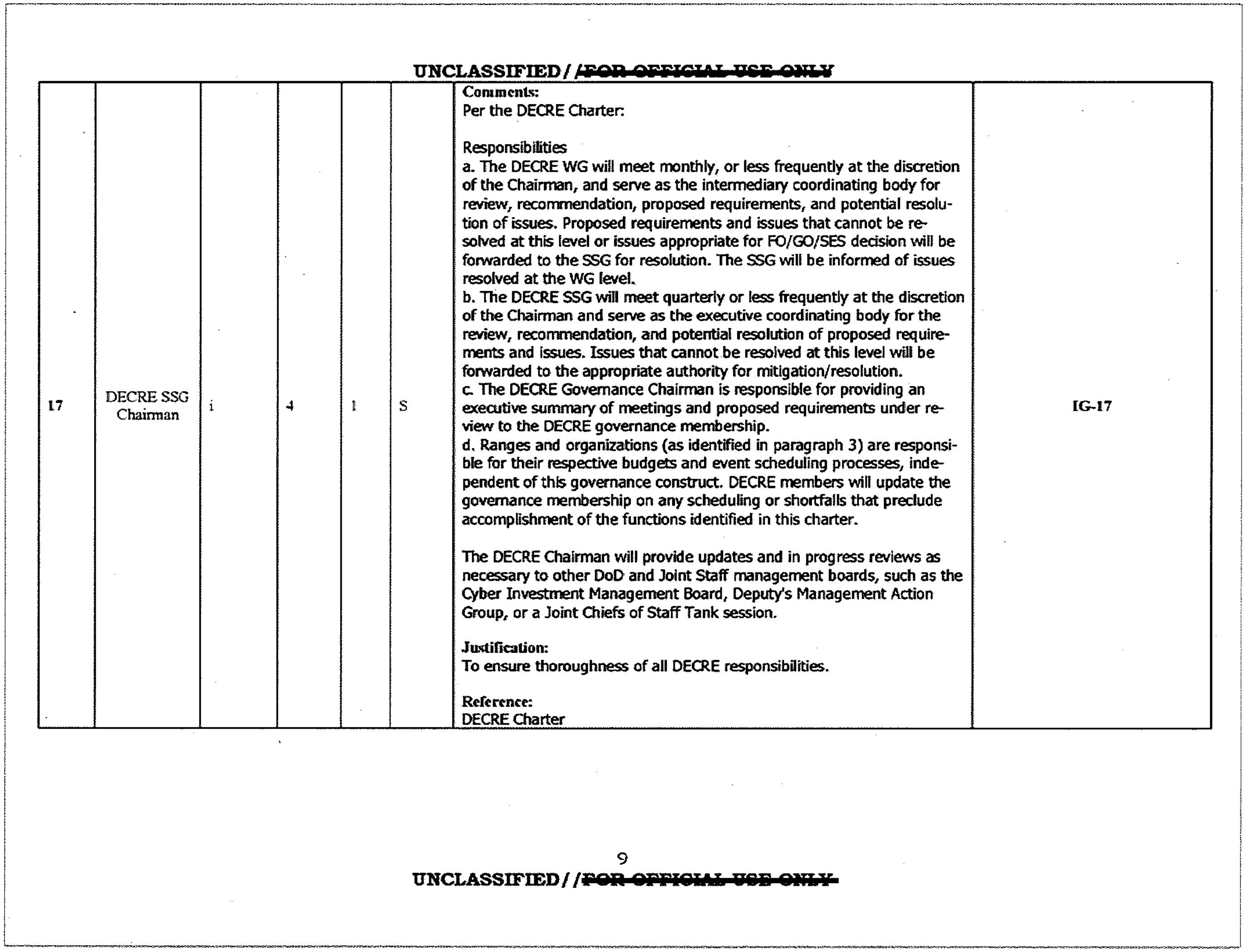
6

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



11	DECRE SSG Chairman	3	2	1	S	**Replace the Second paragraph of page 3:** **With the following:** Further per the Mission Analysis for Cyber Operations of Department of Defense, Submitted In compliance with the reporting requirement contained In the Fiscal Year 2014 National Defense Authorization Act section 933(d), Public Law 113-66. Once fully manned, trained, and equipped In FY 2018, these 133 teams comprising the CMF will execute the three primary missions with approximately 6,200 military and civilian personnel. "(U) USCYBERCOM Taskord 15-0124 establishment and presentation of cyber mission force (CMF) teams In fiscal year (FY) 2015 and FY 2016" (U//FOUO) This order tasks service cyber components to execute building the CMF teams within fy15 and fy16 and applies key tasks. **Reference:** 1. Mission Analysis for Cyber Operations of Department of Defense, Submitted in compliance with the reporting requirement contained in the Fiscal Year 2014 National Defense Authorization Act section 933(d), Public Law 113-66 2. DoD Cyber strategy website at http://www.defense.gov/news/special-reports/0415_cyber-strategy 3. Statement for the record on 14 Apr 2015, before the Senate Arms Services, Subcommittee on Emerging threats and capabilities 4 "(U) USCYBERCOM Taskord 15-0124	IG-11 Revised on page 15
12	DECRE SSG Chairman	3	2	1	S	**Comment:** Hon. Elrc Rosenbach, Assistant Secretary for Homeland Defense and Global Security and Principal Cyber Advisor to the Secretary of Defense made a statement for the record on 14 Apr 2015, before the Senate Arms Services, Subcommittee on Emerging threats and capabilities, and Deputy USCC Lt Gen McLaughlin appeared with him, In reference to the DoD's Evolving Cyber Strategy and the future cyber workforce and CMF's, "...Once fully manned, trained, and equipped In Fiscal Year 2018, these 133 teams will execute USCYBERCOM's three primary mission with nearly 6,200 military and civilian personnel." **Reference :** 1. Statement for the record on 14 Apr 2015, before the Senate Arms Services, Subcommittee on Emerging threats and capabilities 2 DoD Cyber strategy website: http://www.defense.gov/news/special-reports/0415_cyber-strategy	IG-12 Revised on page 15

13	DECRE SSG Chairman	3	3	1	S	**Comment:** It should be noted that this process can take 2 years as identified in the Hon. Eirc Rosenbach, Assistant Secretary for Homeland Defense and Global Security and Principal Cyber Advisor to the Secretary of Defense made a statement for the record on 14 Apr 2015, before the Senate Arms Services, Subcommittee on Emerging threats and capabilities **Reference:** 1. Statement for the record on 14 Apr 2015, before the Senate Arms Services, Subcommittee on Emerging threats and capabilities	IG-13 **Revised on page 15**
14	DECRE SSG Chairman	3	4	2	S	**Comment:** DRWG developed 7 categories and 40 sub-categories to ensure assessments where properly aligned with the capabilities of the 4 DECRE ranges. **Reference:** DECRE Requirements Report	IG-14
15	DECRE SSG Chairman	4	3	1	S	**Comment:** as of yet there has been no significant demand that has not been supported.	IG-15
16	DECRE SSG Chairman	4	5	2	S	**Comments:** refer to line item 11 **Reference:** . 1. Mission Analysis for Cyber Operations of Department of Defense, Submitted in compliance with the reporting requirement contained in the Fiscal Year 2014 National Defense Authorization Act section 933(d), Public Law 113-66 2. DoD Cyber strategy website at http://www.defense.gov/news/special-reports/0415_cyber-strategy 3. Statement for the record on 14 Apr 2015, before the Senate Arms Services, Subcommittee on Emerging threats and capabilities 4. (U) USCYBERCOM Taskord 15-0124	IG-16 **Revised on page 15**



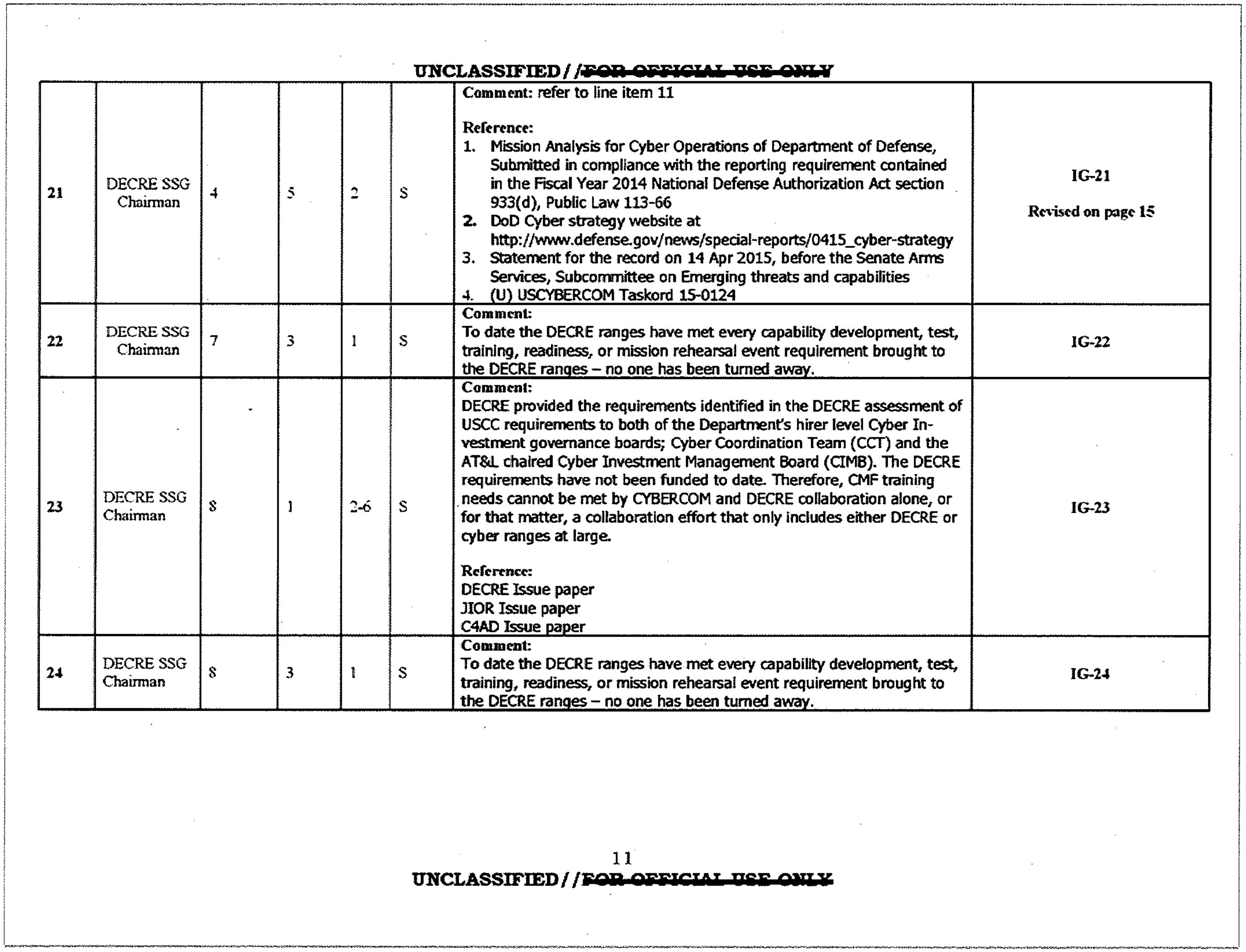
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

17	DECRE SSG Chairman	i	4	1	S	**Comments:** Per the DECRE Charter: Responsibilities a. The DECRE WG will meet monthly, or less frequently at the discretion of the Chairman, and serve as the intermediary coordinating body for review, recommendation, proposed requirements, and potential resolution of issues. Proposed requirements and issues that cannot be resolved at this level or issues appropriate for FO/GO/SES decision will be forwarded to the SSG for resolution. The SSG will be informed of issues resolved at the WG level. b. The DECRE SSG will meet quarterly or less frequently at the discretion of the Chairman and serve as the executive coordinating body for the review, recommendation, and potential resolution of proposed requirements and issues. Issues that cannot be resolved at this level will be forwarded to the appropriate authority for mitigation/resolution. c. The DECRE Governance Chairman is responsible for providing an executive summary of meetings and proposed requirements under review to the DECRE governance membership. d. Ranges and organizations (as identified in paragraph 3) are responsible for their respective budgets and event scheduling processes, independent of this governance construct. DECRE members will update the governance membership on any scheduling or shortfalls that preclude accomplishment of the functions identified in this charter. The DECRE Chairman will provide updates and in progress reviews as necessary to other DoD and Joint Staff management boards, such as the Cyber Investment Management Board, Deputy's Management Action Group, or a Joint Chiefs of Staff Tank session. **Justification:** To ensure thoroughness of all DECRE responsibilities. **Reference:** DECRE Charter	IG-17

9

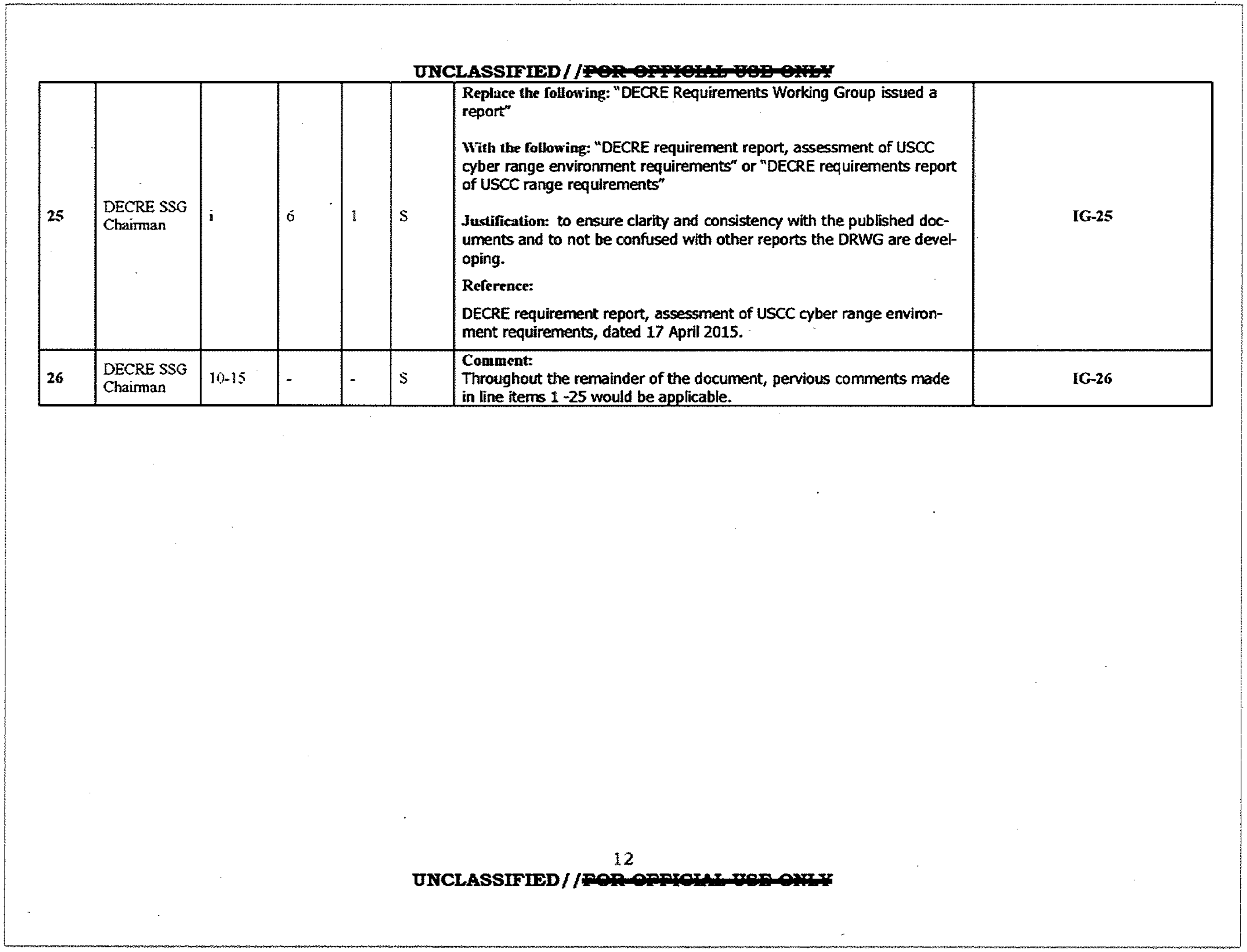
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Comment Resolution Matrix (cont'd)



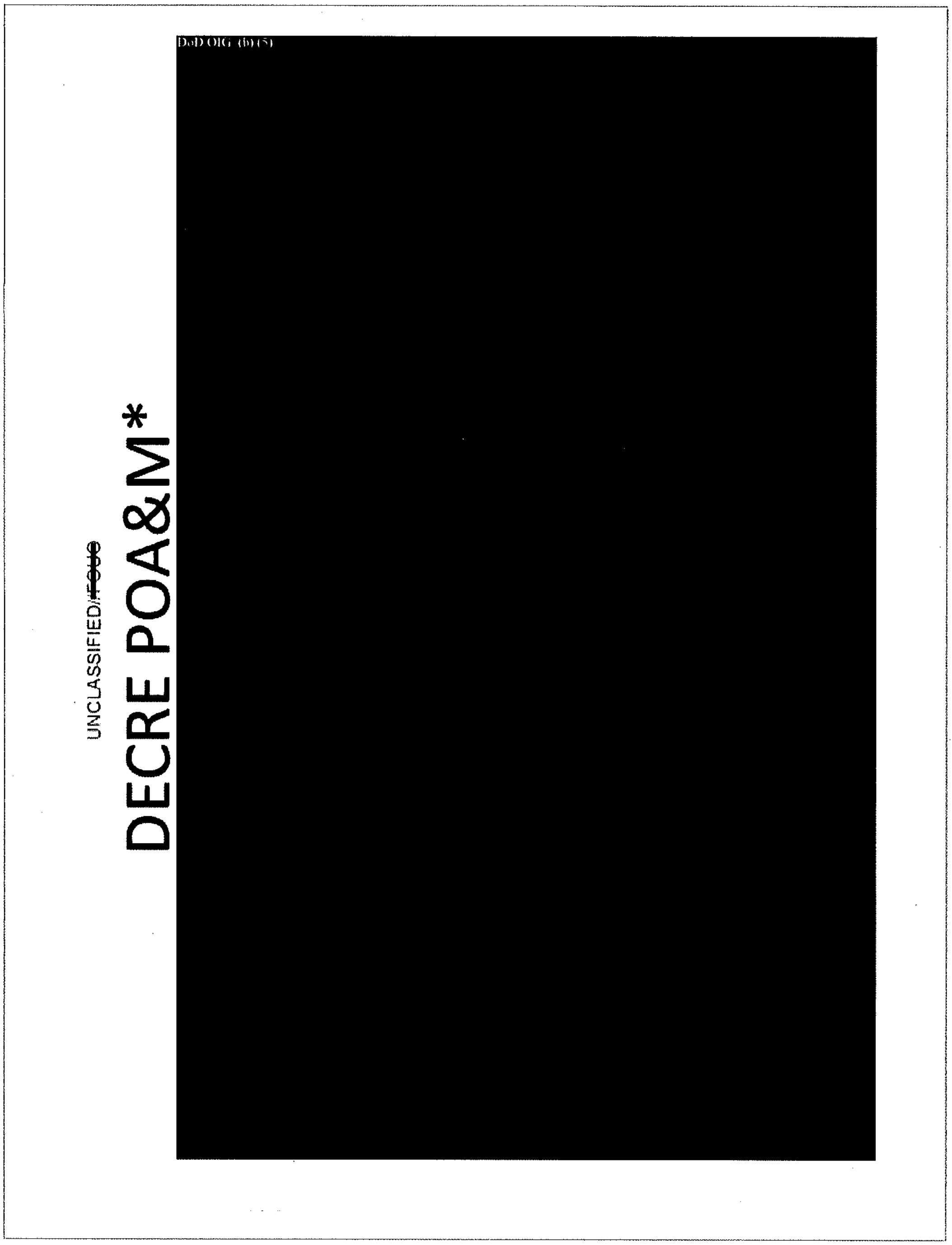
21	DECRE SSG Chairman	4	5	2	S	**Comment:** refer to line item 11 **Reference:** 1. Mission Analysis for Cyber Operations of Department of Defense, Submitted in compliance with the reporting requirement contained in the Fiscal Year 2014 National Defense Authorization Act section 933(d), Public Law 113-66 2. DoD Cyber strategy website at http://www.defense.gov/news/special-reports/0415_cyber-strategy 3. Statement for the record on 14 Apr 2015, before the Senate Arms Services, Subcommittee on Emerging threats and capabilities 4. (U) USCYBERCOM Taskord 15-0124	IG-21 **Revised on page 15**
22	DECRE SSG Chairman	7	3	1	S	**Comment:** To date the DECRE ranges have met every capability development, test, training, readiness, or mission rehearsal event requirement brought to the DECRE ranges – no one has been turned away.	IG-22
23	DECRE SSG Chairman	8	1	2-6	S	**Comment:** DECRE provided the requirements identified in the DECRE assessment of USCC requirements to both of the Department's hirer level Cyber Investment governance boards; Cyber Coordination Team (CCT) and the AT&L chaired Cyber Investment Management Board (CIMB). The DECRE requirements have not been funded to date. Therefore, CMF training needs cannot be met by CYBERCOM and DECRE collaboration alone, or for that matter, a collaboration effort that only includes either DECRE or cyber ranges at large. **Reference:** DECRE Issue paper JIOR Issue paper C4AD Issue paper	IG-23
24	DECRE SSG Chairman	8	3	1	S	**Comment:** To date the DECRE ranges have met every capability development, test, training, readiness, or mission rehearsal event requirement brought to the DECRE ranges – no one has been turned away.	IG-24

(U) Comment Resolution Matrix (cont'd)



25	DECRE SSG Chairman	i	6	1	S	**Replace the following:** "DECRE Requirements Working Group issued a report" **With the following:** "DECRE requirement report, assessment of USCC cyber range environment requirements" or "DECRE requirements report of USCC range requirements" **Justification:** to ensure clarity and consistency with the published documents and to not be confused with other reports the DRWG are developing. **Reference:** DECRE requirement report, assessment of USCC cyber range environment requirements, dated 17 April 2015.	IG-25
26	DECRE SSG Chairman	10-15	-	-	S	**Comment:** Throughout the remainder of the document, pervious comments made in line items 1 -25 would be applicable.	IG-26

(U) DECRE Plan of Action and Milestones



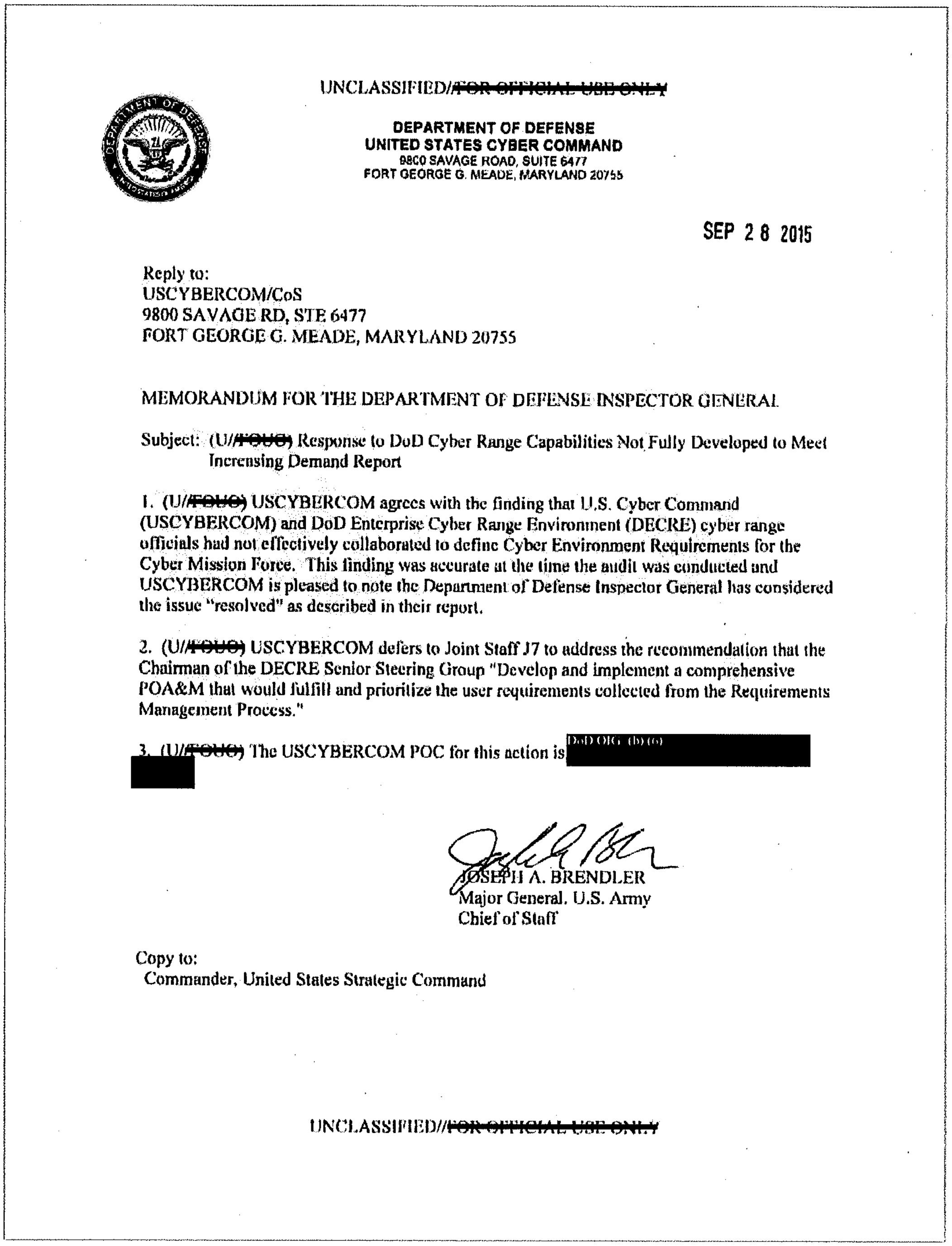
UNCLASSIFIED//~~FOUO~~

DECRE POA&M*

DoD OIG (b)(5)

[redacted]

(U) U.S. Cyber Command



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6477
FORT GEORGE G. MEADE, MARYLAND 20755

SEP 28 2015

Reply to:
USCYBERCOM/CoS
9800 SAVAGE RD, STE 6477
FORT GEORGE G. MEADE, MARYLAND 20755

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL

Subject: (U/~~FOUO~~) Response to DoD Cyber Range Capabilities Not Fully Developed to Meet Increasing Demand Report

1. (U/~~FOUO~~) USCYBERCOM agrees with the finding that U.S. Cyber Command (USCYBERCOM) and DoD Enterprise Cyber Range Environment (DECRE) cyber range officials had not effectively collaborated to define Cyber Environment Requirements for the Cyber Mission Force. This finding was accurate at the time the audit was conducted and USCYBERCOM is pleased to note the Department of Defense Inspector General has considered the issue "resolved" as described in their report.

2. (U/~~FOUO~~) USCYBERCOM defers to Joint Staff J7 to address the recommendation that the Chairman of the DECRE Senior Steering Group "Develop and implement a comprehensive POA&M that would fulfill and prioritize the user requirements collected from the Requirements Management Process."

3. (U/~~FOUO~~) The USCYBERCOM POC for this action is DoD OIG (b)(6) [redacted]

JOSEPH A. BRENDLER
Major General, U.S. Army
Chief of Staff

Copy to:
Commander, United States Strategic Command

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Sources of Classified Information

(U) The documents listed below are sources used to support information within this report.

Source 1: ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ USCYBERCOM Cyber Environment Requirements, Initial Release 1
Derived From: Multiple sources; dated 20140808
Declassify On: 20361001

Source 2: ~~(S//REL TO USA, FVEY)~~ Cyber Guard 14 JIOR Interconnection Security Agreement
Classified By: Per CYBERCOM (b)(3), 10 USC § 130b; Per DoD OIG (b)(6) [redacted]
Derived From: Multiple Sources
Declassify On: 20340424

Source 3: ~~(S//NF)~~ Per OSD/JS (b)(1), 1.4(a) [redacted]
Classified By: Multiple Sources
Declassify On: 20380410

Source 4: ~~(S//REL TO USA, FVEY)~~ USCYBERCOM Task Order 13-0244, "Establishment and Presentation of Cyber Mission Force Teams in FY 2013"; dated 20130306
Declassify On: 20380306

Source 5: ~~(S//REL TO USA, FVEY)~~ Cyber Force Concept of Operations & Employment
Classified By: Per CYBERCOM (b)(3), 10 USC § 130b, Per DoD OIG (b)(6) [redacted]
Derived from: USCYBERCOM Security Classification Guide; dated 20111011, and National Security Agency/Central Security Service Policy Manual 1-52; dated 20130930
Declassify On: 20390601

Source 6: ~~(S//REL TO USA, FVEY)~~ Cyber Flag Architecture Integrating Kinetic and Cyber Capabilities
Classified By: DoD OIG (b)(6) [redacted]
Derived From: Multiple Sources (CMF SCG; dated 20131126 and NSA/CSSM 1-52; dated 20140514)
Declassify On: 20390801

Source 7: ~~(S//REL TO USA, AUS, CAN, NZL, GBR)~~ Execute Order to Implement Cyberspace Operations Command and Control Framework
Classified By: DoD OIG (b)(6) [redacted]; dated 20130621
Declassify On: 20380622

Source 8: ~~(S//REL TO USA, FVEY)~~ Cyber Force Concept of Operations and Employment, Annex C
Classified by: Per CYBERCOM (b)(3), 10 USC § 130b, Per DoD OIG (b)(6) [redacted]
Derived from: USCYBERCOM Security Classification Guide; dated 20121116
Declassify On: 20381106

Source 9: ~~(S//NF)~~ Per OSD/JS (b)(1), 1.4(a) [redacted]
Derived from: Multiple Sources; dated 20140815
Declassify on: 20381120

Source 10: ~~(S//NF)~~ Per OSD/JS (b)(1), 1.4(a) [redacted]
Classified By: Multiple Sources; dated 20140902
Declassify On: 20390818

Source 11: ~~(S//REL TO USA, FVEY)~~ Cyber Flag 15-1 After-Action Report
Derived from: USCYBERCOM Security Classification Guide; dated 20131011, and National Security Agency/Central Security Service CNE Classification Guide; dated 20100301
Declassify On: 20400518

Source 12: ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ USCYBERCOM Cyber Environment Requirements, Initial Release 1- DRAFT Per CYBERCOM (b)(3), 10 USC § 130b, Per DoD OIG (b)(6) [redacted] [redacted] Input)
Derived From: Multiple Sources
Declassify On: 20361001

Source 13: ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ USCYBERCOM Cyber Environment Requirements, Initial Release – DRAFT
Derived From; Multiple Sources
Declassify On: 20361001

Source 14: ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Cyber Guard 13-1 After-Action Report
Derived From: USCYBERCOM SCG
Declassify On: 20390812

Source 15: ~~(S//NF)~~ Per OSD/JS (b)(1), 1.4(a) [redacted]
Classified By: Multiple Sources
Declassify For: Manual Review

Source 16: ~~(S//REL TO USA, FVEY)~~ Cyber Flag 13-1 JIOR Interconnection Security Agreement
Derived From: Multiple Sources
Declassify On: 20320911

Source 17: ~~(S//REL TO USA, FVEY)~~ Cyber Flag 14-1 JIOR Interconnection Security Agreement
Classified By Per CYBERCOM: (b)(3), 10 USC § 130b; Per DoD OIG: (b) [redacted]
Derived From: Multiple Sources
Declassify On: 20330912

Source 18: ~~(S//REL TO USA, FVEY)~~ Cyber Guard 13-1 JIOR Interconnection Security Agreement
Classified By: Per CYBERCOM: (b)(3), 10 USC § 130b; Per DoD OIG: (b)(6) [redacted]
Derived From: Multiple Sources
Declassify On: 20330611

Source 19: ~~(S//REL TO USA, AUS, CAN, GBR, NZL)~~ Per OSD/JS: (b)(1), 1.4(a) [redacted]
Derived From: Multiple Sources
Declassify On: 20350312

(U) Acronyms and Abbreviations

AT&L	Acquisition, Technology, and Logistics
CBA	Capability Based Assessment
C4AD	Command, Control, Communications, and Computers Assessment Division
C3CB	Communications, Command and Control, and Cyber Business
CER	Cyber Environment Requirements
CMF	Cyber Mission Force
DoD CSR	DoD Cyber Security Range
DECRE	DoD Enterprise Cyber Range Environment
DRWG	DoD Enterprise Cyber Range Environment Requirements Working Group
DASD	Deputy Assistant Secretary of Defense
EOA	Evaluation of Alternatives
FOC	Full Operational Capability
JIOR	Joint Information Operations Range
JS	Joint Staff
NCR	National Cyber Range
NDAA	National Defense Authorization Act
PTE	Persistent Training Environment
POA&M	Plan of Action and Milestones
RMP	Requirements Management Process
RMF	Risk Management Framework
T&E	Test and Evaluation
USD	Under Secretary of Defense
USCYBERCOM	U.S. Cyber Command

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

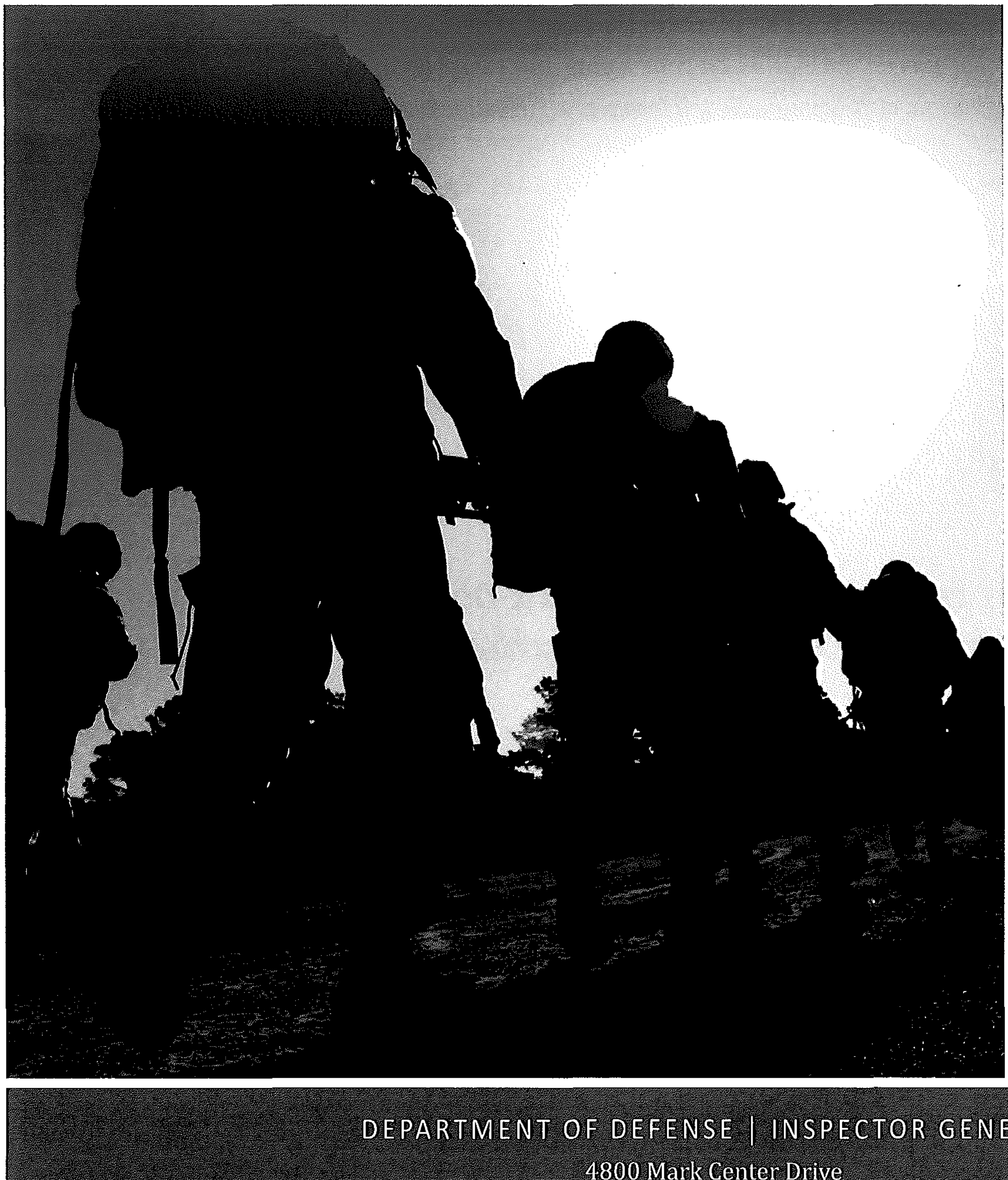
Media Contact
public.affairs@dodig.mil; 703.604.8324

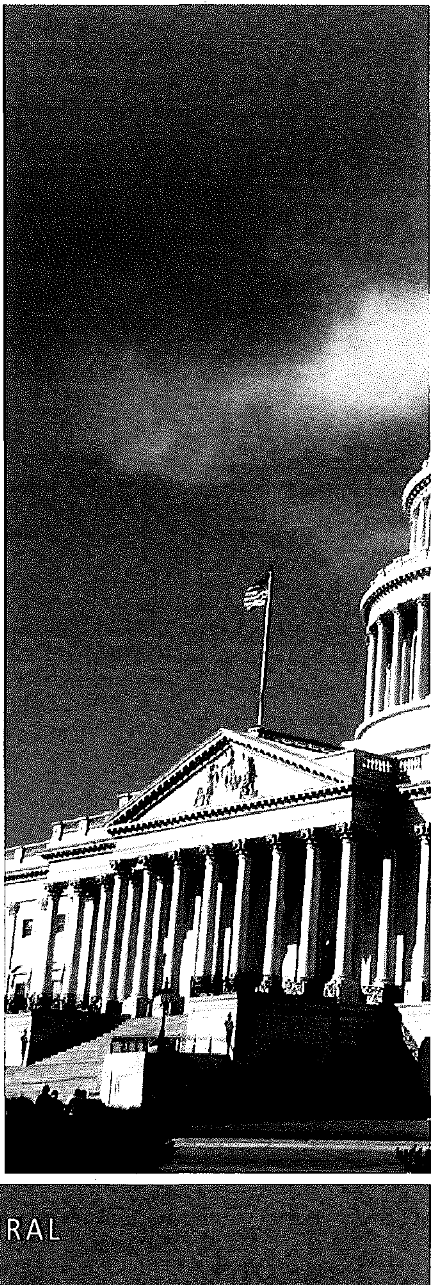
Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline





DEPARTMENT OF DEFENSE | INSPECTOR GENERAL
4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098