



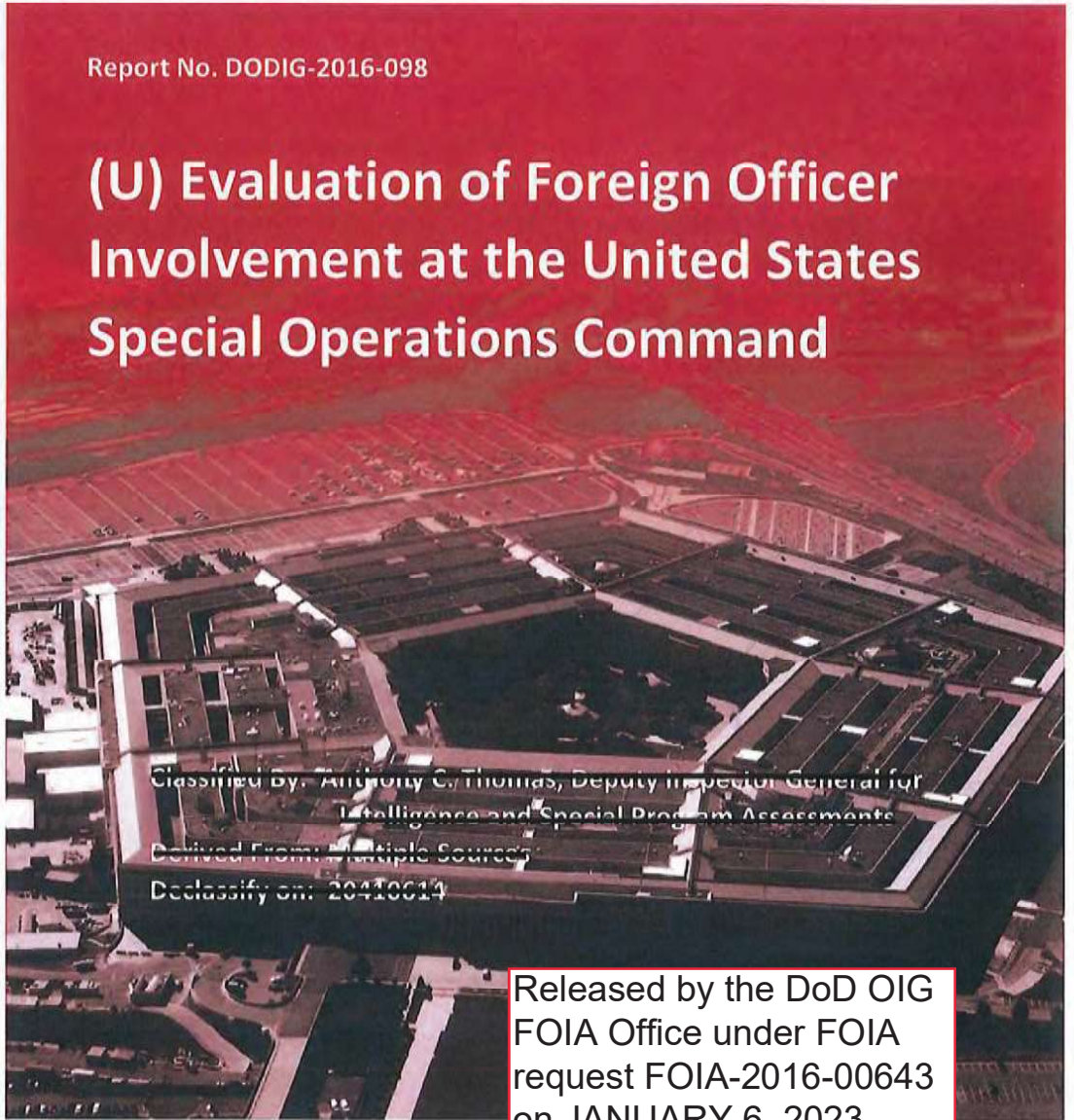
INSPECTOR GENERAL

Department of Defense

June 15, 2016

Report No. DODIG-2016-098

(U) Evaluation of Foreign Officer Involvement at the United States Special Operations Command



Classified by: Anthony C. Thomas, Deputy Inspector General for Intelligence and Special Program Assessments
Derived From: Multiple Sources
Declassify on: 20410014

Released by the DoD OIG FOIA Office under FOIA request FOIA-2016-00643 on JANUARY 6, 2023.

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department 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 and Abuse
HOTLINE
1.800.424.9098 • www.dodig.mil/hotline
.....

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



(U) Results in Brief

(U) Evaluation of Foreign Officer Involvement at the United States Special Operations Command

June 15, 2016

(U) Objective

(U) Our objective was to determine whether foreign officer involvement at the United States Special Operations Command (USSOCOM) was in compliance with U.S. laws and DoD directives.

(U) Findings

(S//NF) SOCOM (b)(1) 1.4(d)
[Redacted text block]

- (U) access to secure facilities and automated information systems by foreign officers;
- (U) possible improper disclosure of classified information to foreign officers; and

- (U) lack of processes by which foreign governments can reimburse the U.S. Government for expenses.

(U) Recommendations

(U//FOUO) We recommend that the Under Secretary of Defense for Policy update DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005, to include the establishment of criteria for granting exceptions to policy regarding the assignment of foreign officers preceding the establishment of an international agreement and clarification of guidance on the use of extended visit requests.

(U) We recommend that the USSOCOM Commander:

- (U//FOUO) ensure international agreements are in compliance with applicable laws and directives;
- (U//FOUO) identify and staff the number of foreign disclosure officers required to manage the disclosure program; and
- (U//FOUO) obtain the required automated information systems accreditation.

(U//FOUO) We recommend that the Defense Intelligence Agency Director establish policies concerning the integration of foreign officers into Secure Compartmented Information Facilities.

(U) Management Comments

(U) The Office of the Under Secretary of Defense for Policy concurred and addressed Recommendation A.1.



(U) Results in Brief

(U) Evaluation of Foreign Officer Involvement at the United States Special Operations Command

(U) The Defense Intelligence Agency concurred with Recommendation B.2.a and Recommendation B.2.b. DIA recommended that B.2.c be redirected to USSOCOM for action.

(U) USSOCOM did not concur with Recommendation A.2.a, Recommendation B.1.a, and Recommendation C.1. USSOCOM concurred with comment on all other recommendations.

(U) Recommendations Table

(U) Management	(U) Recommendations Requiring Comment	(U) No Additional Comment Required
Under Secretary of Defense for Policy	A.1	
Director, Defense Intelligence Agency	B.2.a, B.2.b, B.2.c	
Commander, United States Special Operations Command	A.2.b, A.2.c, A.2.e, A.2.f, B.1.a C.1, C.2, C.3, C.4, C.5 D.1, D.2, D.3	A.2.a, A.2.d, A.2.g, A.2.h, A.2.i B.1.b, B.1.c

(U) THIS PAGE INTENTIONALLY BLANK



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

June 15, 2016


MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY
COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND
DIRECTOR, DEFENSE INTELLIGENCE AGENCY

SUBJECT: Evaluation of Foreign Officer Involvement at the United States Special Operations
Command (Report No. D2016-098) (U)

(U) We are providing this final report for your information and use. We evaluated the United States Special Operations Command's (USSOCOM's) compliance with U.S. laws and DoD directives relating to foreign officer involvement at USSOCOM. This report was conducted in accordance with Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation.

(U) We considered management comments on the draft report. The Office of the Under Secretary of Defense for Policy concurred with and addressed all specifics for Recommendation A.1 in their Management Comments and we consider them responsive. The Defense Intelligence Agency concurred with and addressed Recommendation B.2.a and B.2.b. The Defense Intelligence Agency recommended that we redirect Recommendation B.2.c to USSOCOM. USSOCOM did not concur with Recommendation A.2.a, Recommendation B.1.a, and Recommendation C.1. USSOCOM concurred with comment on all other recommendations. Overall, we considered the Management Comments responsive to our recommendations; however, we have requested additional information from the Office of the Under Secretary of Defense for Policy, Defense Intelligence Agency, and USSOCOM.

(U//~~FOUO~~) We appreciate the courtesies extended to the staff. Please direct questions to me at
(b) (6)


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

(U) Contents

(U) Introduction	1
(U) Objective	1
(U) Background	1
(U) History of USSOCOM's International Special Operation Force Coordination Center	3
(U) Criteria.....	10
(U) Review of Internal Controls.....	15
(U) Finding A.....	16
(U) Foreign Officers Were Assigned to USSOCOM and Subordinate Commands Before the Conclusion of Formal International Agreements.....	16
(U) Criteria.....	17
(U) Status of International Agreements from 2011 to 2014	19
(U) Exception to Policy	21
(U) Assignment of Foreign Officers	22
(U) Foreign Intelligence Officers at USSOCOM.....	25
(U) Temporary Assignment of Foreign Officers to USSOCOM	27
(U) Employment of Foreign Officers at USSOCOM	28
(U) Service Components and Subordinate Commands	31
(U) Air Force Special Operations Command.....	32
(U) Naval Special Warfare Command	32
(U) United States Army Special Operations Command	33
(U) Special Operations Command – Pacific.....	34
(U) Special Operations Command – Africa	35
(U) Joint Special Operations Command	37
(U) Special Operation Command Forces – Central.....	38
(U) International Visits Program	40
(U) Funding the Integration of Foreign Officers.....	41
(U) Conclusion.....	42
(U) Recommendations, Management Comments, and Our Response.....	45
(U) Finding B.....	52
(U) USSOCOM Did Not Fully Comply With SCIF Requirements	52
(U) Criteria.....	52
(U) Physical Security, Access, and Counterintelligence	53
(U) Physical Security of the SCIF	53

(U) J3-International Spaces (Non-SCIF)54
(U) Foreign Officer Access to USSOCOM's SCIFs.....58
(U) Reoccurring Access for Foreign Officers58
(U) FVEY Partners Swipe Access.....59
(U) Special Operations Research Development and Acquisition Center60
(U) Conclusion.....60
(U) Recommendations, Management Comments, and Our Response.....62
(U) Finding C. 66
(U) USSOCOM Improperly Disclosed Classified Information to Foreign Officers66
(U) Criteria.....66
(U) Foreign Disclosure Program68
(U) Disclosure of Classified Information to Foreign Officers69
(U) Special Operations Command – Africa.....72
(U) Special Operations Command – Central73
(U) Foreign Disclosure Office Staffing Shortages73
(U) Lack of Foreign Disclosure Education74
(U) Conclusion.....75
(U) Recommendations, Management Comments, and Our Response.....76
(U) Finding D..... 80
(U) USSOCOM Did Not Fully Comply With Automated Information System Requirements.....80
(U) Criteria.....80
(U) Information Security Responsibilities.....81
(U) Foreign Officer Access to Automation Systems82
(U) Improper Installation of Foreign National Secure Communication Systems.....82
(U) Inability to Verify Accreditation of USSOCOM SCIF for Automated Information Systems83
(U) Risk to Information Security.....83
(U) Possible Data Spillage.....84
(U) Lack of Training.....84
(U) Conclusion.....85
(U) Recommendations, Management Comments, and Our Response.....87
(U) Appendix A 91
(U) Scope and Methodology91
(U) Use of Computer-Processed Data91
(U) Prior Coverage91

(U) Appendix B 92

(U//~~FOUO~~) Foreign Officers Assigned to USSOCOM Headquarters, Subordinate Commands, and Service Components (2011-2014).....92

(U) Appendix C 103

(U) Response to House Armed Services Committee and Other Relevant Information.....103

1. (U) What was the USSOCOM Commander's authority and intent in the ISCC?103

2. (U) Did USSOCOM have the appropriate authority and approval to implement a foreign liaison officer program and defense exchange program at USSOCOM?104

3. (U) What was USSOCOM's authority and use of foreign officers within USSOCOM's staff?105

4. (U) Was USSOCOM in compliance with SCIF regulations?.....105

5. (U) What funding sources did USSOCOM use for the construction and renovation to USSOCOM HQ's SCIF?106

(U) Appendix D 109

(U) Counterintelligence Risks.....109

(U) Foreign Officer Misconduct111

(U) Appendix E..... 113

(U) Benefits of Foreign Officer Assignment to the USSOCOM Enterprise.....113

(U) Appendix F..... 117

(U) Office of the Under Secretary of Defense for Policy Comments.....117

(U) Defense Intelligence Agency Comments118

(U) United States Special Operations Command Comments120

(U) Acronyms and Abbreviations..... 130

(U) Introduction

(U) Objective

(U) Our objective was to determine whether foreign officer involvement at the United States Special Operations Command (USSOCOM) was in compliance with U.S. laws and DoD directives. Specifically, we reviewed the establishment of the International Special Operation Forces (SOF) Coordination Center (ISCC), as well as its processes, use, and security.

(U) Background

(U) On August 4, 2014, representatives from the DoD Office of Inspector General met with a senior congressional staffer from the House Appropriation Committee for Defense to discuss the committee's evaluation requirements regarding foreign officer involvement at USSOCOM. During the meeting the staffer asked:

- (U) What was USSOCOM Commander's authority and intent in the establishment of the ISCC?
- (U) Did the USSOCOM Commander have the appropriate authority and approval to implement a foreign liaison officer (FLO) program and defense exchange program at USSOCOM?
- (U) What was USSOCOM's authority and use of foreign officers within USSOCOM's staff?
- (U) Was USSOCOM in compliance with Sensitive Compartmental Information (SCI) Facility (SCIF) security regulations?
- (U) What funding sources did USSOCOM use for the construction and renovations made to the USSOCOM headquarter SCIF?

(U) Based on the discussion, the DoD Office of Inspector General team decided to conduct an evaluation of legal and regulatory guidelines governing USSOCOM's assignment and employment of foreign officers, the physical structure and security of

the infrastructure, affiliated counterintelligence risks, USSOCOM's disclosure of information to foreign officers, and other relevant matters.

(S//NF) SOCOM (b)(1) 1.4(a) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]:

- (S//NF) SOCOM (b)(1) 1.4(a) [REDACTED]
- (S//NF) SOCOM (b)(1) 1.4(a) [REDACTED]
[REDACTED]
- (S//NF) SOCOM (b)(1) 1.4(a) [REDACTED]
[REDACTED]
- (S//NF) SOCOM (b)(1) 1.4(a) [REDACTED]
[REDACTED]
- (U) SOCOM (b)(1) 1.4(a) [REDACTED]

(U) See Appendix A for the scope and methodology of this report and prior evaluation coverage. See Appendix B for a summary of the foreign officers assigned to USSOCOM Headquarters, Service Component and Subordinate Unified Commands. See Appendix C for the response to questions from a senior congressional staffer, House Appropriation Committee for Defense and other relevant information. See Appendix D for a discussion on the counterintelligence risks posed by foreign officer integration. See Appendix E for a discussion on the benefits of foreign officers to the USSOCOM enterprise.

(U) History of USSOCOM's International Special Operation Force Coordination Center

(U//~~FOUO~~) The integration of foreign officers within USSOCOM from 2011 to 2014 was not new. Five Eye (FVEY)¹ partners were assigned to the United States Army Special Operations Command (USASOC) as early as 1976 and to USSOCOM as early as 2009. In September 2011, Admiral William McRaven, then USSOCOM Commander, announced his vision to expand USSOCOM's support to the Global SOF Network (GSN) by including partner nations' SOF representatives into USSOCOM and providing them with the greatest possible access to USSOCOM's facilities, communications, and information sharing systems.

(U//~~FOUO~~) As one USSOCOM senior staff official told us, Admiral McRaven viewed the building of additional partnerships with foreign SOF elements as an expansion of what was already in existence at USSOCOM. The USSOCOM senior staff official stated that USSOCOM derived its requirement to build partnership capacity through the words echoed in national policy, the National Defense Strategy, and presidential speeches such as President Obama's "West Point"² speech that mentioned "partnerships" more than 30 times. The senior official stated that "partnerships" was mentioned approximately 40 times in the 2012 National Defense Strategy and approximately 200 times in the current Quadrennial Defense Review.

(U//~~FOUO~~) According to the USSOCOM senior official, building partnerships should include foreign officers at the headquarters because that was where planning took place. The USSOCOM Commander was more explicit about his vision in an e-mail to his senior staff providing guidance on how they should proceed:

(U) the future, as I see it, is about expanding the SOCOM network globally. You will hear me talk about 'taking SOCOM global.' This means

¹ (U) Five Eye - International intelligence sharing network that includes the United States, Australia, Canada, New Zealand, and the United Kingdom.

² (U) President Barack Obama's speech to the United States Army Military Academy, West Point was delivered as part of the commencement ceremony for the class of 2014 on May 28, 2014.

thickening our SOF, IA, and allied networks around the world. It also means having the authorities to move forces globally in order to resolve problems which the POTUS [President of the United States], SECDEF [Secretary of Defense] or GCC(s) [Geographic Combatant Commands] need resolved.

- ADM McRaven, Purple Note, 14 Sep 2011

(U//~~FOUO~~) The DoD Inspector General provided Admiral McRaven the opportunity for a face-to-face or telephonic interview. However, his assistant advised that he declined because of his busy schedule as Chancellor, University of Texas. In spite of not interviewing Admiral McRaven, we believe the extensive documentation and testimony that we collected provided us with necessary information to develop an accurate picture of his vision.

(U) According to the Special Operations Forces 2020 (SOF 2020) paper, "A History of the Global SOF Network Operational Plan Team," March 2014, the USSOCOM Commander established the GSN operational planning team (OPT) in September 2011. The purpose of the GSN OPT was to enhance the SOF collaboration with the GCC, the interagency and international partners through a network designed to build relationships and support mutual objectives. The USSOCOM Commander tasked the GSN OPT with looking into how USSOCOM could build allied relationships and establish a NATO-like SOF Headquarters organization in selective regional areas called "Regional SOF Coordination Centers (RSCC)."³

(U) The USSOCOM Commander assigned a U.S. Army Colonel to lead the GSN OPT. The Colonel reported directly to the USSOCOM Commander, but coordinated through the USSOCOM Chief of Staff to ensure the headquarters staff could provide input. The

³ (U//~~FOUO~~) RSCCs were intended to be venues for promoting interoperability, exchanging information, and collaborating to address regional challenges. RSCC's focus and structure would be dictated by regional concerns and participating nations. However, in the summer of 2013, legislative restrictions were imposed upon the RSCC initiative. The House Armed Service Committee (H.R.1960) stated that "none of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2014 for DOD may be obligated or expended to plan, prepare, establish, or implement any...RSCC or similar regional coordination entities."

USSOCOM Commander directed the GSN OPT to provide an initial assessment on how to take USSOCOM global no later than November 4, 2011.

(U) As of late 2011, liaison officers from Australia, Canada, and the United Kingdom were already assisting the GSN OPT with developing a plan to carry out the USSOCOM Commander's vision to establish RSCCs. According to an April 2012 memorandum to the Office of the Under Secretary of Defense for Policy (OUSDP), Defense Technology Security Administration (DTSA), the Chief of Staff, USSOCOM, stated that the GSN OPT was key to achieving the USSOCOM Commander's vision of a GSN.

(U) In early 2012, the GSN OPT concluded that USSOCOM lacked the ability to integrate, and organize the variety of information generated by the GSN that would enable strategic decision-making by USSOCOM leadership. The GSN OPT also concluded that the command was not prepared to integrate partner nation SOF officers or to operate as a global functional command. In the spring of 2012, GSN OPT leadership initiated an effort to ~~SOCOM Section 1.7(e) for 1.4(g)~~ to consolidate the foreign partners and U.S. partners under one roof in what would become the ISCC.

(U//~~FOUO~~) In 2012, the ISCC renovation costs were estimated at \$500,000 to \$700,000. Later, the estimated costs doubled. Security upgrades were added to meet regulations and engineering requirements. USSOCOM's renovations were not budgeted items. The Office of Integration Center for Financial Management was tasked with resourcing the expanded support to the GSN and the reconstruction associated with the integration of partner nation representatives into USSOCOM. According to a USSOCOM financial management official, USSOCOM did not view the renovation to ~~SOCOM Section 1.7(e)~~, but viewed it as a modification to an existing facility. Additionally, USSOCOM did not view partner nation's integration efforts as a "new start." Therefore, USSOCOM did not seek congressional authorization.

⁴ (U) De-SCIF, De-accreditation or DIA's termination of a SCIF's accreditation.

(U//~~FOUO~~) The first two non-FVEY officers were from France, arriving at USSOCOM in March and June 2012 respectively. They worked in Building 143, along with foreign officers from Australia, Canada, and the United Kingdom ~~SOCOM Section 1.7(e) for 1.4(g)~~.

(U//~~FOUO~~) In May 2012, USSOCOM hosted the first International SOF Week in conjunction with the annual SOF Industry Conference. More than 90 nations participated and the event offered a venue in which the USSOCOM Commander introduced his GSN concept to the world's SOF leaders.

(U//~~FOUO~~) In September 2012, the USSOCOM Commander laid out the following requirements for the GSN OPT: [Establish] (1) ~~SOCOM Section 1.7(e) for 1.4(g)~~

The GSN OPT submitted a \$5.9 million Military Interdepartmental Purchase Request to the Navy Research Lab to develop system specifications for a ~~SOCOM Section 1.7(e) for 1.4(g)~~

roadmap and resourcing documentation. ~~SOCOM Section 1.7(e) for 1.4(g)~~ was envisioned as the centerpiece for the forthcoming ISCC common operating picture. Less than a year later, ~~SOCOM Section 1.7(e) for 1.4(g)~~

(U) On March 6, 2013, the USSOCOM Commander testified to the House Armed Services Committee that, "USSOCOM is enhancing its global network of SOF to support our

⁵ (U) TSOCs are the Subordinate Unified Commands (Special Operations Command-Pacific, Special Operations Command-Central Command, Special Operations Command-Africa, Special Operations Command-Europe, Special Operations Command-South, Special Operations Command-Korea, and Special Operations Command-North).

worked to break down barriers to information sharing so that partners could be fully integrated into the staff.

(U//~~FOUO~~) The ISCC Information Paper reported that the ~~SOCOM Section 1.7(e) for 1.4(g)~~
~~_____~~
~~_____~~
levels. As shared opportunities (or crises) emerged, the ~~SOCOM Section 1.7(e) for _____~~ As a result of this enhanced SOF capability and interoperability across the GSN, the ISCC ~~SOCOM Section 1.7(e) for _____~~. The ISCC would also ~~SO~~ information, intelligence, and requirements among GSN members to support and strengthen the network.

(U//~~FOUO~~) According to the ISCC information progress report, September 4, 2013, the USSOCOM Commander stated:

(U//~~FOUO~~) to achieve my vision of including Partner Nation SOF Representatives into the SOCOM Headquarters, we will provide the ~~SOCOM Section 1.7(e) for 1.4(d)~~
~~_____~~
~~_____~~
~~_____~~
~~_____~~.

(U//~~FOUO~~) On September 20, 2013, the USSOCOM Commander briefed his vision to the SECDEF, the USD(P), and the CJCS.

(U//~~FOUO~~) ~~SOCOM Section 1.7(e) for 1.4(g)~~
~~_____~~
~~_____~~.

⁶ (U) TEMPEST is a short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. The aim is to minimize the likelihood that these emanations will ever be intercepted by adversaries of the United States.

(U//~~FOUO~~) From 2012 to 2014, the GSN OPT integrated 11 partner nations into the USSOCOM's battle rhythm: Australia, Canada, Denmark, France, Germany, the Netherlands, New Zealand, Norway, Spain, Sweden, and the United Kingdom. An additional five nations, Italy, Lithuania, Poland, Singapore, and Romania, had contact with the GSN OPT on matters concerning the GSN, but were resident at the United States Central Command (USCENTCOM). Additionally, the GSN OPT facilitated the installation of three partner nation secure national systems (France, Germany, and Spain) at USSOCOM.

(U//~~FOUO~~) According to a February 7, 2014, briefing to the USSOCOM Deputy Commander, the Director, ISCC, reported that the ISCC workspace was expected to open on April 11, 2014. The updated cost estimate for the project was more than \$7.2 million. An acquisition officer associated with the reconstruction project stated that the construction and renovation was funded with Operations and Maintenance (O&M) funds. There was no need for military construction funding because USSOCOM was not constructing a new building or changing the purpose of ~~SOCOM~~. According to the acquisition official, O&M funding limits for building renovation were based on a percentage of the original building cost and the purpose of the building.

(U//~~FOUO~~) As of mid-2014, the ISCC project cost USSOCOM approximately \$7.125 million. These costs included approximately \$2.4 million in renovation costs, and approximately \$4.7 million in collateral requirements, such as furniture, information technology installation, and security requirements. USSOCOM used \$2.48 million in procurement funds and \$4.64 million in O&M funds.

(U//~~FOUO~~) On May 7, 2014, the USSOCOM Commander renamed the ISCC the J3-International (J3-I). ~~SOCOM Section 1.7(e) for 1.4(g)~~. This action effectively completed the "operational role" of the GSN OPT and ISCC and transitioned the GSN OPT to ~~SOCOM Section 1.7(e)~~.

(U//~~FOUO~~) In May 2014, the Chief of Staff, USSOCOM, declared the ISCC/J3-I spaces and the ~~SOCOM Section 1.7(e) for 1.4(g)~~. That decision officially integrated J3-I partner nations into the USSOCOM headquarters.

(U) Criteria

(U) The authority to negotiate and conclude international agreements comes from the Constitution and includes those agreements that are not treaties made pursuant to the Constitutional authority of the President. The relevant sources of that authority for international agreements pertaining to DoD include the President's authority as Chief Executive to represent the nation in foreign affairs, and the President's authority as Commander-in-Chief. DoD negotiates and concludes international agreements pursuant to that authority, executed on behalf of the President.

(U) U.S. Department of State Foreign Affairs Manual Volume 11, Political Affairs, Section 720 (11 FAM 720) "Negotiation and Conclusion", September 25, 2006. Section 11 FAM 720 states that authority to negotiate and conclude international agreements for Defense Personal Exchange Personnel is executed subject to the Case Act, which provides that the Secretary of State must transmit the texts of all international agreements to Congress "as soon as practicable, but in no event later than sixty days thereafter." In addition, the Act provides that an international agreement may not be signed or otherwise concluded on behalf of the United States without prior consultation with the Secretary of State. The Secretary of State implements this law, among others in 11 FAM 720, and provides consultation for initiation and conclusion.

(U) 11 FAM 721 "Circular 175 Procedure", December 13, 1955. The Department of State (DoS) issued Circular 175 Procedure, "Authority to Negotiate and Conclude Non-Reciprocal International Defense Personnel Exchange Agreements," October 20, 2011, and "Authority to Negotiate and Conclude Foreign Liaison Assignments," October 17, 2011, to the Department of Defense. These Circular 175 Procedures authorized DoD to negotiate and conclude international agreements, based

on pre-approved DoS template agreements, with North Atlantic Treaty Organization (NATO) allies and other specified countries or their ministries.

(U) These template agreements included template annexes, whereby prospective foreign liaison or exchange personnel certified their understanding of, and agreement with, the terms and conditions governing their status, and provided a detailed description of each foreign liaison or exchange position. The templates standardized definitions and established the duties and responsibilities of the "host" and "parent" organizations as well as the assigned personnel. They also included the allocation of associated expenses, protection of classified and other sensitive information, settlement or waiver of claims, disciplinary authority, and other terms and conditions related to the assignment of such personnel.

(U) The process for negotiating and concluding international agreements pertaining to an exchange officer is prescribed in the applicable DoD publications, and includes a notice requirement to the Assistant Advisor for Treaty Affairs at the DoS. Circular 175 Procedure ensures compliance by the executive branch with the Case Act and makes certain that Congress is kept fully informed of the international agreements. DoD defines the approval authority and procedures for international agreements, and implements the Case Act, in DoD Directive 5530.3, "International Agreements."

(U) DoD Directive 5530.3, "International Agreements," June 11, 1987.

DoDD 5530.3, paragraph 4.2, assigns USD(P) the task of authorizing the negotiation and conclusion for all categories of international agreements, unless this directive or other authorizing regulations for specific categories of agreements delegate this authority to another official within DoD. The Directive also granted the Director, DIA, the authority to negotiate and conclude international agreements for the collection and exchange of military intelligence information (except signals intelligence agreements). Paragraph 6.1 designated the Communications Management Division, OUSD(P), as the single office of record for receiving requests for the authority to negotiate or conclude an international agreement. The Communications Management Division delegated this authority to DTSA. According to paragraphs 8.2 and 8.3, DoD personnel must not

initiate, negotiate, nor conclude an international agreement without prior written approval by the OUSD(P) or designated official. Paragraph 11 stated that it was DoD policy to maintain awareness of compliance with the terms of international agreements. The paragraph also stated that DoD Components must oversee compliance with international agreements for those agreements for which the DoD Component was responsible. In addition, paragraph 11 stated that DoD Components must keep the DoD Office of General Counsel currently and completely informed on compliance with all international agreements in force for which they were responsible.

(U) Deputy Secretary of Defense Memorandum "Accountability of Department of Defense Sponsored Foreign Personnel in the United States," May 18, 2004. The Deputy Secretary of Defense's memorandum specifies that DoD Components must document the arrival and departure of foreign personnel from their assigned duty. The Deputy Secretary of Defense's memorandum also states that DoD Components must establish a central, automated accounting capability that captures the planned and actual itineraries of DoD sponsored foreign personnel where possible, leveraging the DoD Foreign Visit System and Foreign Visit System Confirmation Module.

(U) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005. DoD Directive 5230.20 governs the DoD International Visits Program, the Foreign Liaison Officer Program, the Defense Personnel Exchange Program (DPEP), the Cooperative Program Personnel Program, and foreign personnel arrangements pursuant to Section 2608(a) of title 10, United States Code. DoDD 5230.20 requires that the terms and conditions for all assignments of foreign nationals to the DoD Components must be established in a legally binding international agreement, or an annex to such agreement, which must be negotiated pursuant to DoD Directive 5530.3 According to DoDD 5230.20, DoD Components must also account for DoD sponsored foreign personnel in the United States as specified by Deputy Secretary of Defense Memorandum, May 18, 2004.

(U) The National Defense Authorization Act, 2010, (Public Law 111-84). Public Law 111-84 governed the assignment of defense exchange officers. Statutory authority

for military exchange programs is codified in 10 U.S.C. § 168. Section 1207 of the National Defense Authorization Act (NDAA) for Fiscal Year 2010 expanded the types of DoD exchange programs to include non-reimbursable exchange officers. According to Sec 1207(c), (d):

(U) (c) PAYMENT OF PERSONNEL COST.

(U) (1) The foreign government with which the United States has entered into a non-reciprocal international defense personnel exchange agreement must pay the salary, per diem, cost of living, travel costs, cost of language or other training, and other costs for its personnel under such agreement in accordance with the applicable laws and regulations of such government.

(U) (2) EXCLUDED COSTS.-Paragraph (1) does not apply to the following costs:

(U) (A) The cost of training programs conducted to familiarize, orient, or certify exchanged personnel regarding unique aspects of the assignments of the exchanged personnel.

(U) (B) Costs incident to the use of facilities of the United States Government in the performance of assigned duties.

(U) (C) The cost of temporary duty of the exchanged personnel directed by the United States Government.

(U) (d) PROHIBITED CONDITIONS. No personnel exchanged pursuant to a non-reciprocal agreement under this section may take or be required to take an oath of allegiance or to hold an official capacity in the government.

(U) SOCOM Section 1.7(e) for 1.4(g)

[REDACTED]

[REDACTED]

[REDACTED]

SOCOM Section 1.7(e) for 1.4(g)

(U) USSOCOM Policy Memorandum 13-16, "Permanent Assignment of Military Personnel Exchange Program and Foreign Liaison Officers to U.S. Special Operations Command," June 24, 2010. The memorandum establishes the USSOCOM policy and procedures for the assignment of FLOs to USSOCOM and components.

(U) USSOCOM Directive 550-2, "Disclosure of U.S. Classified Military Information to Foreign Governments and International Organizations," August 5, 2010. Directive 550-2 provides policy and guidance for disclosing and protecting SOF classified military information to foreign governments and international organizations. The directive provides USSOCOM foreign disclosure policy and procedures, delegated authority, and assigned responsibilities.

(U) USSOCOM Directive 550-3, "Foreign Visits and Requirements for Administering Visits by Foreign Government Representatives to U.S. Special Operations Command (USSOCOM)," April 29, 2013. Directive 550-3 provides policy and guidance, for visits, invitations, and assignments of foreign nationals to USSOCOM and its component and sub-unified commands.

(U) USSOCOM Directive 550-4, "Disclosure and Release of Classified and Controlled Unclassified Special Operations Tactics, Techniques, and Procedures to Foreign Nationals," February 7, 2012. Directive 550-4 provides USSOCOM's policy and procedures for the authorized disclosure of classified and controlled unclassified information activities and information related to SOF tactics, techniques, and procedures to foreign forces and nationals.

(U) Review of Internal Controls

(U//~~FOUO~~) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, required DoD organizations to implement a comprehensive system of internal controls to provide reasonable assurance that programs were operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses at USSOCOM. Although USSOCOM established sufficient written policies governing the visit and assignment of foreign officers and the disclosure of classified information to foreign nationals, each component command managed its own visits and assignment of foreign nationals and its own foreign disclosure management system with no evident oversight by USSOCOM. USSOCOM did not have adequate means for determining the overall efficacy of its directives and mandated processes. USSOCOM's disregard for its prescribed policies and DoD directives concerning the assignment of foreign officers and the lack of a formalized process for maintaining oversight of all foreign SOF officers (attached or assigned to each USSOCOM component) posed a significant weakness to USSOCOM's internal controls. We will provide a copy of this report to the senior officials responsible for internal controls at USSOCOM.

(U) Finding A.

(U) Foreign Officers Were Assigned to USSOCOM and Subordinate Commands Before the Conclusion of Formal International Agreements

(U//~~FOUO~~) Although the USSOCOM Commander initiated informal international agreements with foreign governments, those international agreements were not concluded in accordance with applicable laws and directives. USSOCOM also lacked oversight of the international agreements and appropriate annexes for which they had responsibility. Subordinate commands lacked accountability over foreign officers that they sponsored. This situation occurred because:

- (U//~~FOUO~~) The USSOCOM Commander initiated and negotiated informal international agreements with various foreign governments for FLOs and non-reciprocal exchange officers (NREOs), before the authorization of USD(P) or Office of General Counsel;
- (U//~~FOUO~~) USSOCOM and subordinate commands assigned FLOs and NREOs to their commands before the conclusion of an international agreement⁷ and had several international agreements that lacked required annexes, certifications, security assurances, and designated disclosure letters (DDL);
- (U//~~FOUO~~) USSOCOM initiated agreements for the exchange of military intelligence with foreign governments before gaining the approval of the DIA; and
- (U//~~FOUO~~) USSOCOM subordinate commands did not maintain records concerning the arrival, departure, or itinerary of foreign officers who

⁷ (U) Unless otherwise noted, international agreements are negotiated in accordance with DoDD 5530.03.

actually visited or were assigned to their command.

(U//~~FOUO~~) As a result, from 2011 to 2014, USSOCOM was not in full compliance with applicable laws and directives concerning the assignment and use of foreign officers. This potentially placed U.S. intelligence and military information and resources at risk based on the assignment and possible misuse of foreign officers.

(U) Criteria

(U) The National Defense Authorization Act, 2010, (Public Law 111-84), Section 1207. Section 1207(b) (1)(2) of the law states that pursuant to a non-reciprocal international defense personnel exchange agreement, personnel of the defense ministry of a foreign government may be assigned to positions in the DoD. An individual may not be assigned to a position pursuant to a non-reciprocal international defense personnel exchange agreement unless the assignment is acceptable to both governments. This law further prohibits personnel pursuant to a non-reciprocal agreement from holding an official capacity in the government.

(U) DoD Directive 5530.3, "International Agreements," June 11, 1987.

DoDD 5530.3 prohibits DoD personnel from initiating, negotiating, or concluding an international agreement without prior written approval by the OUSD(P) or designated official. The directive requires that all international agreements are implemented in accordance with DoD's delegated blanket DoS Circular 175 authority, as previously discussed. DoDD 5530.3 also requires DoD components to maintain oversight and compliance with the international agreements for which they are responsible, and to gain Director, DIA, authorization to negotiate agreements for the collection and exchange of military intelligence. Paragraph 13.4 states that "agreements for the collection and exchange of military intelligence information (except signals intelligence agreements): The Director, Defense Intelligence Agency (DIA) and ...[The Under

Security of Defense for Intelligence] must concur in all proposed agreements concerning intelligence and intelligence-related matters.”

(U//~~FOUO~~) DoD's delegated DoS Circular 175 authority required adherence to the DoS templates for all international agreements. In accordance with USSOCOM template memorandum of agreement for FLOs:

(U) the Host Participant will provide such office facilities, equipment, supplies, and services as may be necessary for the Liaison Officer to fulfill the purposes of this MOU, subject to reimbursement by the parent participant for the cost of the liaison officer's use of such facilities at rates determined by the Host Participant. When the U.S. is the host participant, reimbursement for such facilities, equipment, supplies, and services will be made through foreign military sales or use of an acquisition and cross-servicing agreement.

(U) DoDD 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005.

DoDD 5230.20 states that the terms and conditions for all assignments of foreign nationals to the DoD Components must be established in a legally binding international agreement, or an annex to such agreement, which must be negotiated pursuant to DoDD 5530.3. According to DoDD 5230.20, the requests for coordination and approval of DPEP, CPP, FLO, and foreign personnel arrangements must include a position description and a DDL⁸ or equivalent written disclosure guidance, and be submitted according to DoDD 5530.3. Paragraph 4.5 states that foreign nationals must have access only to information that does not exceed the level authorized under National Disclosure Policy (NDP)-1 for release to their governments. Exceptions to NDP-1 shall not be granted to accommodate the assignment of FLOs, DPEP, CPP, or foreign personnel arrangements.

⁸ DDL is a delegation of disclosure authority letter issued by the appropriate Principle Disclosure Authority or Designated Disclosure Authority describing the classification levels, categories, scope, and limitations related to information under a DoD Component's disclosure jurisdiction that may be disclosed to specific foreign governments or their nationals for a specified purpose.

(U) USSOCOM Policy Memorandum 13-16, "Permanent Assignment of Military Personnel Exchange Program and FLOs to U.S. Special Operations Command," June 24, 2010. The memorandum established the USSOCOM policy and procedures for the assignment of FLOs to USSOCOM and Components.

(U) Status of International Agreements from 2011 to 2014

(U//~~FOUO~~) 2011. Before 2011, USSOCOM concluded an international agreement with Australia concerning the assignment of liaison officers. By July 2011, USSOCOM had concluded an international agreement with Canada and began negotiating with France without the written approval of OUSD(P) as required by DoDD 5530.3. In June, OUSD(P) first granted USSOCOM the authority to negotiate and conclude an international agreement with the United Kingdom; in which USSOCOM later concluded.

(U//~~FOUO~~) 2012. OUSD(P) issued USSOCOM written authority to negotiate and conclude an international agreement with France. USSOCOM also began negotiating an agreement with Norway without OUSD(P)'s written approval.

(U//~~FOUO~~) 2013. USSOCOM began negotiating agreements with Denmark, Germany, and the Netherlands without OUSD(P)'s written approval. OUSD(P) later granted USSOCOM the authority to negotiate seven international agreements with Australia, Denmark, Germany, Jordan, the Netherlands, Norway, and Spain. In July, USSOCOM concluded its second international agreement with Australia and an international agreement with the United Kingdom with OUSD(P)'s written approval.

(U//~~FOUO~~) 2014. OUSD(P) granted USSOCOM the authority to negotiate 13 international agreements with the countries of Australia, Canada, Finland, Italy, Japan, South Korea, Lithuania, New Zealand, Peru, Poland, Singapore, Sweden, and United Arab Emirates. USSOCOM also concluded international agreements with New Zealand, Spain, Denmark, Jordan, and Canada with OUSD(P)'s written approval. In March, the pre-existing 2009 Memorandum of Understanding (MOU) for FLOs between USSOCOM and the Australian government expired. In June, without OUSD(P)'s

approval, the USSOCOM Commander extended the MOU to March 2019. DoD Office of General Counsel was aware of the exchange letters between the USSOCOM Commander and the Australian Government. By the end of the year, USSOCOM had concluded a second international agreement with Canada without OUSD(P)'s written approval.

(U) As of December 2014, OUSD(P) granted USSOCOM the authority to concluded international agreements with seven countries on behalf of the United States. Of those seven countries, USSOCOM concluded nine international agreements (five FLO and four NREO agreements). In addition, OUSD(P) authorized USSOCOM to pursue the negotiation or conclusion of 15 international agreements.

(U) Table 1. USSOCOM's Authorized International Agreements and Authorities (as of December 2014)

USSOCOM's Concluded MOUs	Authorized to Conclude	Authorized to Negotiate
Australia (2) (2009, 2013)	Norway (2013)	Finland (2014)
Canada (2) (2011, 2014)	France (2012)	Japan (2014)
Denmark (2014)	Germany (2013)	Poland (2014)
Spain (2014)		Peru (2014)
Jordan (2014)		United Arab Emirates (2014)
New Zealand (2014)		Lithuania (2014)
United Kingdom (2013)		Netherlands (2014)
		South Korea (2014)
		Singapore (2014)
		Sweden (2014)
		Italy (2014)
		Australia (2014)

(U//FOUO)

(U) Exception to Policy

(U//~~FOUO~~) In May 2012, the Director, International Security Programs, OUSD(P), authorized USSOCOM to assign a French special operations exchange officer to USSOCOM before the establishment of a legally binding international agreement. OUSD(P) granted USSOCOM a temporary exception to policy (120 days) to allow the assignment of the first French officer. According to an OUSD(P) senior official, he was unaware of USSOCOM's specific justification for requesting an exception to policy, but the reason could have been "the foreign officer was already in the United States." The OUSD(P) senior official stated, "It's hard to go back to these countries and require an agreement for the person that was already in the [U.S]." OUSD(P) provided no written justification for the exception during our data calls. The temporary exception to policy, which allowed the assignment of the French officer to USSOCOM, expired in September 2012 and was reissued in July 2014.

(U//~~FOUO~~) According to the Director, DTSA, his office tried to mitigate USSOCOM's actions after the fact, because "no one was going to tell a four-star general, 'no', you cannot keep a foreign officer in place because the [USSOCOM] staff did not follow DoDD 5230.20." According to the OUSD(P) senior staff official, exchange officers without a concluded agreement would need an exception to policy. In July 2014, OUSD(P) extended an unlimited exception to policy (July 2014 - indefinite) to allow foreign officers from Australia, Germany, France, the Netherlands, Norway, and Sweden to remain at USSOCOM until formal international agreements were concluded.

(U//~~FOUO~~) According to the Director, DTSA, the DoD Office of General Counsel later advised OUSD(P) that the Joint Staff, not OUSD(P), should have approved USSOCOM's request for exceptions to policy for exchange officers.

(U//~~FOUO~~) An OUSD(P) official stated that he did not know why USSOCOM was allowed to remain non-compliant with the assignment of foreign officers from 2011 to 2014 or why there were no consequences for being non-compliant with Public Law 111-84 or DoDD 5230.20. The OUSD(P) official believed that as of December 2014 USSOCOM was

making an effort to come into compliance with the DoD regulations and USSOCOM policies. According to the OUSD(P) official, OUSD(P) was the office of primary responsibility for DoDD 5230.20 and should have oversight of DoDD 5230.20. The official further stated that the defense exchange program needed system oversight and [compliance] enforcement. Also according to the OUSD(P) official, DTSA did not have the authority to enforce DoDD 5230.20, which governs the assignment of and visits by foreign officers. According to an OUSD(P) senior staff official, reinforcing compliance of a directive or law would have to come from the Office of the President of the United States.

(U) Assignment of Foreign Officers

(U//~~FOUO~~) USSOCOM reported that there were 25 foreign officers assigned or attached to USSOCOM from 2011 to 2014. These foreign officers were assigned as FLOs and DPEP officers. They were subcategorized as permanent FLOs, temporary duty FLOs, intelligence FLOs, operational FLOs, Military Personnel Exchange Program (MPEP) officers, or NREO officers.

(U//~~FOUO~~) **2011.** Foreign officers from Australia, Canada, and the United Kingdom were already working with the GSN OPT on the USSOCOM Commander's vision for regional coordinating centers. The first international agreements between Australia and Canada were concluded without the OUSD(P)'s authority to conclude. In November, the USSOCOM Commander met with the Commander, French Special Operations Command, to discuss the establishment of a non-reciprocal French exchange position at USSOCOM to support the GSN OPT prior to OUSD(P)'s authority to negotiate. In December, USSOCOM senior staff members from the Foreign Disclosure (FD) Office and International Engagement Program (J5) advised the Officer-in-Charge of the GSN OPT of their concerns with the invitation, negotiation, and ultimate assignment of a French officer to USSOCOM. The USSOCOM senior staff members cited there were a number of rules regarding the assignment of foreign nationals to DoD facilities under the MPEP and the requirement to gain OUSD(P)'s approval. A senior staff officer offered an alternative recommendation to have the French officer reside in the USCENTCOM

Coalition Village⁹, with recurring visits to USSOCOM. According to the GSN OPT Officer-in-Charge, the USSOCOM Commander did not want liaison officers, but would rather have the non-U.S. officers in billets as active members of the USSOCOM team. According to official documentation, the Officer-in-Charge, GSN OPT, threatened "consequences" [to the staff component] if that course of action was briefed to the USSOCOM Commander.

(U//~~FOUO~~) **2012.** By 2012, foreign officers from France and Norway had joined the ranks of the GSN OPT without concluded international agreements. Since the Norwegian SOF FLO was already in the U.S., assigned to the USCENTCOM Coalition Village, USSOCOM issued him a permanent badge for USSOCOM. In March, the Deputy Director, International Security Programs Secretariat (ISPS), National Disclosure Policy Committee (NDPC), OUSD(P), provided a written email to a USSOCOM's senior staff official, advising that USSOCOM was not authorized to place foreign nationals on its staff until a MOU was concluded or an exception to policy was granted by the OUSD(P). The Deputy Director, ISPS, stated, "There are rare circumstances that may warrant an exception to policy, but significant justification must be provided to my [ISPS, NDPC, OUSD(P)] office for consideration. More often than not we [ISPS, NDPC, OUSD(P)] do not approve exceptions." In April, USSOCOM submitted a request to the OUSD(P) for an exception to policy. According to an OUSD(P) senior staff official, OUSD(P) was the last to know when foreign officers were [assigned to] commands and were called on to determine how to make [the assignment] legal.

(U//~~FOUO~~) The foreign officers were placed under a visit request, to make them compliant with the DoDD 5230.20, while OUSD(P) decided how to resolve the situation. However, according to the OUSD(P) senior official, placing foreign officers at a DoD organization under a recurring visit request should not serve as an alternative to DoDD 5230.20 requirement to establish a concluded agreement before the assignment of a foreign officers. The OUSD(P) senior official stated that DTSA told all commands

⁹ (U) Coalition Village (Coalition Coordination Center) is collocated with USCENTCOM, MacDill Air Force Base, Tampa, FL. The Coalition Village was established after the September 11, 2001 attacks, and was comprised of representatives from 65 nations that worked with USCENTCOM Service members in the war on terrorism.

that concluded agreements must be in place before the assignment of a foreign officer; however, getting the commands to comply with the regulation was difficult. The OUSD(P) senior official also stated that the lack of an established agreement with the foreign country creates risk for the U.S. Government. In September 2012, USSOCOM assigned NATO FLOs to USSOCOM headquarters and its element in the National Capital Region, Washington, DC. USSOCOM did not conclude an international agreement with NATO, in spite of the OUSD(P) request.

(U//~~FOUO~~) **2013.** Foreign officers from Denmark, Germany, the United Kingdom, the Netherlands, Spain, and Sweden were assigned to the ISCC (formerly the GSN OPT), before concluded international agreements.

(U//~~FOUO~~) **2014.** In May, USSOCOM hosted an International SOF Conference in Tampa, Florida. The USSOCOM Commander invited 84 partner nations to work at USSOCOM headquarters. USSOCOM officials acknowledged that during the International SOF Conference, partner nations who toured the J3-I spaces, were provided a FLO versus NREO fact sheet that was actually "FOR OFFICIAL USE ONLY," as an expression of U.S. policy. An after-action report of the International SOF Conference stated that the FLO versus NREO fact sheet represented negotiations with the partner nations in advance of OUSD(P) authorization to do so. It gave the partner nations the impression that all nations that toured the J3-I space could request representation at USSOCOM. Also, foreign officers from New Zealand (one month before an international agreement) and Jordan (two months after an international agreement was concluded) joined the ISCC. Additionally, in May the ISCC was formally integrated into the USSOCOM staff and designated the USSOCOM J3-I. A foreign officer from Germany was later assigned to the USSOCOM J3-I prior a concluded international agreement. As of December 2014, 19 foreign officers (8 NREOs and 11 FLOs) representing 12 countries, were permanently assigned to USSOCOM.

**(U) Table 2. Foreign Officers Permanently Assigned to USSOCOM Headquarters
(as of December 2014)**

Partner Nations	With Concluded MOUs In Compliance With DoDD 5230.20		With Non-Concluded MOUs Not In Compliance With DoDD 5230.20	
	FLOs	NREOs	FLOs	NREOs
Australia	2	1		
Canada	1	1		
Denmark		1		
France				2
German			1	1
Jordan	1			
New Zealand	1			
Norway				1
Netherlands			2	
Spain		1		
Sweden			1	
United Kingdom	2			
Permanently assigned as of December 2014	7	4	4	4

(U//~~FOUO~~)

(U) Foreign Intelligence Officers at USSOCOM

(U) According to the Office of Partner Engagement, DIA had no record of agreements from 2011 to 2014 granting USSOCOM the authority to collect or exchange military intelligence information with foreign governments, as required by DoDD 5530.3. Additionally, DIA did not issue any DDLs to USSOCOM between 2011 and 2014 to negotiate or conclude military intelligence agreements with foreign governments.

(U//~~FOUO~~) In November 2011, USSOCOM assigned a Canadian officer as a NREO, three years before the international agreement was concluded in November 2014. The Canadian embassy processed a foreign visit request (CA11-A3103) for a Canadian

intelligence liaison officer to serve as the Deputy J2, USSOCOM. The Canadian NREO stated that he worked as a FLO and his duties included: answering Canadian SOF intelligence requirements; liaison officer coordination with other SOF units and DIA; providing assistance to the Joint Special Operations University; and providing U.S. and Canadian SOF with relevant intelligence information.

(U//~~FOUO~~) A German Bundesnachrichtendienst (BND), (the Federal Intelligence Service), FLO was assigned to USSOCOM, under a recurring visit request (ID # GM14-A660). USSOCOM did not have a concluded international agreement or intelligence agreement with the German government. The BND FLO was tasked to facilitate intelligence exchanges and intelligence sharing with the Joint Intelligence Center, USSOCOM, in support of USSOCOM J2 focus areas. The BND FLO was also tasked to provide intelligence reports and support to a TSOC's request for information and intelligence requirements, and provide support for BND's staff visits to USSOCOM. As of December 2014, the international agreement for a German NREO was still in negotiation.

(U//~~FOUO~~) USSOCOM did not have an existing international or intelligence agreement
SOCOM Section 1.7(e) for 1.4(a)

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] was approved in accordance with an OUSD(P) memorandum dated January 5, 2015, authorizing temporary duty personnel and operational planning visits beyond 30 days. According to another USSOCOM official, USSOCOM would work with DIA to leverage DIA's intelligence sharing and bi-lateral agreements, allowing these intelligence liaison officers to remain at USSOCOM and exchange intelligence information. As previously stated, DIA had not issued USSOCOM authority to intelligence information with foreign governments.

¹⁰ (U) Islamic State of Iraq and the Levant (ISIL) is a militant group and self-proclaimed caliphate and Islamic State which is led by Sunni Arabs from Iraq and Syria.

(U//~~FOUO~~) USSOCOM did not have an existing international or intelligence agreement with the Dutch government. According to a USSOCOM staffer, USSOCOM attempted to go around OUSD(P) and the DoD regulations by "piggybacking" off the Army's international intelligence agreement with the Netherlands. In December 2014, USSOCOM contacted the Foreign Liaison Program Office, Deputy Chief of Staff for Intelligence (G-2), Department of the Army about using the existing Army memorandum of agreement as a bridging solution while USSOCOM and the Netherlands worked an international agreement for a non-reciprocal exchange through the Dutch Parliamentary approval process. The USSOCOM staffer stated that USSOCOM was trying to get "as legal as possible, as quickly as possible." According to a U.S. Army official, OUSD(P) did not provide policy approval for the U.S. Army's management of the Dutch FLO position in USSOCOM. The Dutch FLO was assigned to USSOCOM in January 2013 and remained at USSOCOM as of December 2014.

(U) Temporary Assignment of Foreign Officers to USSOCOM

(U//~~FOUO~~) A USSOCOM official stated that USSOCOM's J3-I staff tried to reassign the United Arab Emirates liaison from SOCCENT to USSOCOM. According to a USSOCOM official, a representative from the United Arab Emirates Embassy requested USSOCOM's foreign disclosure officer (FDO) to approve an extended visit request for the assignment of a United Arab Emirates liaison officer to USSOCOM. A USSOCOM FDO representative stated that the United Arab Emirates' embassy representative was told that USSOCOM did not have a concluded agreement with the United Arab Emirates, the embassy representative insisted that he was instructed by J3-I personnel to submit the extended visit request and it would be approved.

(U//~~FOUO~~) SOCOM (b)(3) 10.U.S.C. 130b, (b)(5), (b)(6)

[REDACTED]
[REDACTED]:

(U//~~FOUO~~) SOCOM (b)(3) 10.U.S.C. 130b, (b)(5), (b)(6)

[REDACTED]
[REDACTED]

SOCOM (b)(3) 10.U.S.C. 130b, (b)(5), (b)(6)

(U//~~FOUO~~) SOCOM (b)(3) 10.U.S.C. 130b, (b)(5), (b)(6) :

(U//~~FOUO~~) SOCOM (b)(3) 10.U.S.C. 130b, (b)(5), (b)(6)

(U//~~FOUO~~) SOCOM (b)(5) USSOCOM staff continued to assign foreign officers to the USSOCOM as operational planners on recurring or extended visit requests. According to a USSOCOM senior official, a Belgian officer was at USSOCOM and officers from Estonia, Poland, and Finland were inbound [from USCENTCOM in 2015]. According to the USSOCOM official, USSOCOM would grant these FLOs access to USSOCOM, as temporary planners against the ISIL threat, under extended visit requests for 30 days or more. USSOCOM had not concluded international agreements with Belgium, Estonia, Poland, and Finland. The USSOCOM senior staff official stated that USSOCOM brought partner nations into USSOCOM before the completion of formal agreements in the same manner in which USCENTCOM brought partner nations into the command to support USSCENTCOM's ongoing operations.

(U) Employment of Foreign Officers at USSOCOM

(U) The USSOCOM Commander assigned two NREOs to the USSOCOM staff. An Australian officer was assigned to the USSOCOM Operations Office (J3) and a Canadian officer was assigned to the USSOCOM Intelligence Office (J2). These officers were assigned pursuant to international agreements for NREOs. There were approximately 19 foreign officers at USSOCOM, working on behalf of their government as FLOs, NREOs, or dual-used as a "hybrid" (exchange officer working as a liaison officer). According to

an OUSD(P) senior official, USSOCOM drafted a request for change in policy that allowed for a foreign liaison-exchange officer hybrid.

(U//~~FOUO~~) **USSOCOM Deputy Operations Officer (DJ3).** USSOCOM did not have an international agreement with the Australian government before the assignment of the first Australian NREO. The Australian NREO arrived on December 9, 2012, but the non-reciprocal exchange agreement was not concluded until July 23, 2013. The Australian officer served as the USSOCOM Deputy Operations Officer, J3, who managed and coordinated the collective efforts of a multi-disciplined staff of 300 active and reserve military and civilian personnel. The Deputy J3 shared the full scope of responsibility with the USSOCOM J3. In the absence of the USSOCOM J3, the Deputy J3 possessed the same authority as the USSOCOM J3 (subject to limitations in law or regulations for matters requiring action by a U.S. commissioned officer or employee of the U.S. Government).

(U//~~FOUO~~) **USSOCOM Deputy Intelligence Officer (DJ2).** The Canadian embassy processed a foreign visit request (CA11-A3103) for a Canadian intelligence liaison officer to serve as the Deputy J2, USSOCOM. In November 2011, USSOCOM assigned the Canadian officer as a NREO. No exception to policy or waiver was submitted for the assignment of the Canadian NREO. The international agreement for Canadian exchange officers was concluded in November 2014. As part of the international agreement for the Canadian NREO, the duty description (Annex B), Terms of Reference, and Legal Status Certification (Annex A, Section III) were not ratified. The Canadian officer stated that he worked as an FLO. The Canadian officer's duties included answering Canadian SOF intelligence requirements, coordinating with other SOF units and DIA, providing assistance to the Joint Special Operations University, and providing U.S. and Canadian SOF with relevant intelligence information.

(U//~~FOUO~~) According to a USSOCOM senior official, the then-USSOCOM Commander envisioned the foreign officers working on behalf of their nation first and then de-conflicting, coordinating, and partnering through USSOCOM's special operations liaison officers and staff to make it happen. In 2013, the USSOCOM Commander tasked

the senior staff officer to draft letters to the SECDEF, OUSD(P), Director National Intelligence, and DoS about a legislative proposal to change current policy on the use of FLOs and USSOCOM's ability to fund liaison officers' temporary duty and office

SOCOM (b)(5)

(U//~~FOUO~~) request that USD(P) approve a FLO agreement that had some non-reciprocal exchange authority embedded into it. The limitation there [was] that agreement would not give [US]SOCOM the authority to cover office expenses (which can get relatively expensive) but could cover temporary duty expenses in a limited capacity.

(U//~~FOUO~~) In 2014, several USSOCOM FLOs were scheduled to travel to Washington, D.C., to support private events for the Global SOF Foundation¹¹, a private company owned by the former Director of the ISCC, USSOCOM. The German Embassy submitted an official visit request for the German SOF Commander and his Senior Enlisted Advisor to attend the Global SOF Symposium¹² in St. Petersburg, Florida. The Chief of Staff, USSOCOM, later released a memorandum that stated the Global SOF Symposium hosted by the Global SOF Foundation, a non-federal entity, did not meet the criteria to be mission-critical to USSOCOM. The memorandum directed the Office of Communications, USSOCOM, to process invitations from the Global SOF Foundation and determine USSOCOM's level of support to the event. According to a USSOCOM senior staff official, USSOCOM's FLOs and exchange officers from Jordan, Denmark, Germany, New Zealand, and France participated in the Global SOF Symposium. Further, this same

¹¹ (U) LinkedIn Homepage: Global SOF Foundation (GSF) is a private company owned by COL (retired) Stuart Bradin, former Director of the ISCC, USSOCOM. The GSF leads an international effort to increase understanding of Special Operations; advance SOF capabilities; and responsibly promote the role of Special Operations by strategically linking public and private sector initiatives.

¹² (U) The Global SOF Symposium 2015, hosted by the Global SOF Foundation in St Petersburg, Florida, February 24-25, 2015, was a forum for U.S. and international SOF leaders to build relationships through networking opportunities, discuss international efforts to defeat global threat, and pinpoint ways for global SOF to interoperate.

individual stated FLOs represented USSOCOM at other events. One Canadian FLO was tasked to travel to Colombia to represent USSOCOM.

(U) Service Components and Subordinate Commands

(U) DoDD 5530.3, paragraphs 13.3(1)(2), granted the Secretaries of the Army, the Navy, and the Air Force (for predominantly uni-Service matters) and the CJCS (for other than uni-Service matters) the authority to negotiate and conclude international agreements. These agreements covered combined military planning, command relationships, military exercises and operations, force deployments, exchange programs, and the collection or exchange of military information and data other than military intelligence.

(U) As previously discussed, DoDD 5230.20 states the terms and conditions for all assignments of foreign nationals to the DoD Components must be established in a legally binding international agreement, or an annex to such agreement, which must be negotiated pursuant to DoDD 5530.3. In addition, DoDD 5230.20 also states that requests for coordination and approval of DPEP, CPP, FLO, and foreign personnel arrangements must include a position description and a DDL or equivalent written disclosure guidance.

(U//~~FOUO~~) Senior Service officials at the USASOC, Naval Special Warfare Command (NAVSPECWARCOM), and Air Force Special Operations Command (AFSOC) reported to us that their respective Services generated all international agreements. Marine Corps Special Operations Command, Special Operations Command-Europe (SOCEUR), Special Operations Command-Korea (SOCKOR), and Special Operations Command-South (SOCSOUTH) reported they did not have foreign officers or international agreements for the assignment of foreign officers to their commands.

(U//~~FOUO~~) According to USSOCOM officials, USSOCOM did not maintain oversight of international agreements or partner nation's representation at the subordinate commands and Service components. The selection of prospective countries and

requirements for foreign SOF were generated by component commanders or Service Secretaries.

(U) Air Force Special Operations Command

(U//~~FOUO~~) AFSOC used an existing international agreement between the Department of the Air Force and the United Kingdom for the assignment of defense personnel exchange officers. AFSOC provided the modified Annex B (position descriptions), security plans, and certification documents to this international agreement in compliance with the DoD regulations.

(U) Since 2011, there were two United Kingdom Defense exchange officers assigned to the AFSOC under the DPEP. According to AFSOC documentation, "the Military Personnel Exchange Program was created to allow our allies to gain familiarity with the U.S. Air Force's conduct of operations and to improve coalition interoperability. It establish[ed] an active relationship for sharing of military service experience, professional knowledge, and doctrine to the maximum extent permissible under the information disclosure policies of the U.S. and the foreign governments concerned."

(U//~~FOUO~~) The exchange officers were assigned to the 15th Special Operations Squadron (15 SOS) Hurlburt Field, Florida, as MC-130H Special Operations Aircraft commanders/pilots. The exchange officers planned and executed MC-130H tactical missions under combat conditions with limitations imposed by squadron mission objectives and tactical situations. They participated in various exercises and deployed to hostile areas and foreign countries with parent government acquiescence in military action. The exchange officers were employed in leadership or instructor positions and were required to rate U.S. personnel. As of December 2014, AFSOC reported there was one United Kingdom Defense exchange officer assigned to AFSOC.

(U) Naval Special Warfare Command

(U//~~FOUO~~) NAVSPECWARCOM used six existing international agreements for the assignment of exchange officers that were concluded between the Department of the

Navy and the United Kingdom, Australia, France, Germany, Italy, and Norway. NAVSPECWARCOM provided DDLs, dated March 19, 2008, and April 15, 2011, to the Annex Bs (duty descriptions) of the respective international agreements.

(U) United States Army Special Operations Command

(U//~~FOUO~~) USASOC used seven existing international agreements that were concluded between the Department of the Army and Germany, the Netherlands, Australia, Canada, Columbia, and the United Kingdom. Annexes A and B to the international agreement between the DoD and Australian government were not ratified at the time of assignment. USASOC took immediate action to ratify required annexes to existing international agreements in accordance with DoD regulation and authority after we brought it to their attention.

(U//~~FOUO~~) USASOC reported 20 foreign officers assigned to USASOC between 2011 and 2014 under the Defense Foreign Liaison Program and the Defense MPEP. These foreign liaison and exchange officers' positions were established through an MOU between the Department of the Army, as represented by the USSOCOM Commander and the ministries of partner nations. According to a USASOC senior official, the selection of prospective countries and requirements for foreign SOF were generated by the Commander, USASOC, or the Secretary of the Army. The senior USASOC official stated that USSOCOM did not have oversight of SOF partners within USASOC and that USSOCOM staff would be involved only with initiatives generated by USSOCOM.

(U//~~FOUO~~) As of December 2014, eleven foreign officers remained at USASOC. The nine exchange officers were from: the United Kingdom (1); Germany (1); Colombia (2); Canada (1); and Australia (4). The two FLOs were from Germany and the Netherlands.

- (U//~~FOUO~~) The Australian exchange officers served as training officers for a U.S. Airborne Ranger battalion. The Australian MPEPs were responsible for the efficient execution of training management, coordinating all land, ammunition, logistics, air and airspace resources for the battalion, and served as the primary

liaison officer to the installation staff to ensure the proper maintenance of ranges and close-quarter combat facilities.

- (U//~~FOUO~~) The Canadian MPEP served as team members of an assault team, responsible for planning and conducting close-quarter combat, direct action, special reconnaissance, and other sensitive compartmented activities. The Canadian MPEP maintained a worldwide deployment readiness posture.

(U) Special Operations Command – Pacific

(U) Special Operations Command – Pacific (SOCPAC) used the March 4, 2009, international agreement between USSOCOM and the Australian Special Operations Command and the July 29, 2011, international agreement between USSOCOM and the Minister for National Defence of Canada for the assignment of two FLOs. All required annexes and DDLs were in compliance with DoD's regulation and authority.

(U) As of December 2014, the two FLOs were assigned to SOCPAC as part of the Defense FLO Program. The Australian and Canadian Liaison Officers supported the development of a global network of SOF and enhanced the interoperability between their respective countries' special operation commands and USSOCOM.

(U) The two FLOs to SOCPAC served in the following capacity:

- (U) One Australian officer from the Australian Special Operations Command was assigned to SOCPAC in 2014. According to Annex B, July 2014, to the MOU between USSOCOM and Australian government, the Australian FLO participated in SOCPAC working groups, conferences, and seminars; provided situational awareness to SOCPAC and the Australian Special Operations Command on theater SOF activities; identified combined U.S. and Australian engagement opportunities; contributed to SOCPAC planning efforts to promote Australian capabilities and integrate Australian Special Operations Command intent; and advised and assisted in U.S. and Australian information exchange.

- (U) One Canadian officer from the Canadian Special Operations Command Special Operations Planning and Liaison Element¹³ was assigned to SOCPAC in 2014. The Canadian FLO participated in SOCPAC working groups, conferences, and seminars; provided situational awareness to SOCPAC and Canadian Special Operations Command on theater SOF activities; identified combined U.S. and Canada engagement opportunities; contributed to SOCPAC planning efforts to promote Canadian capabilities, integrated their intent; and advised and assisted in U.S. and Canada information exchange.

(U) Special Operations Command – Africa

(U) Special Operations Command – Africa (SOCAF) used international agreements between USSOCOM and the governments of the United Kingdom and Canada for the assignment of FLOs. According to a Letter of Arrangement, signed on March 22, 2013, the SOCAF Commander established a SOF Liaison Program between Canadian Special Operations Forces Command and USSOCOM. The Letter of Arrangement specifically addressed the details for the employment of a liaison position at SOCAF and solidified a "Memorandum of Understanding Between the Department of Defense of the United States of America and the Department of National Defence of Canada Regarding Special Operations Liaison Officers," July 2011. As of December 2014, SOCAF did not have an Annex B, a certification, or DDLs to the MOUs between USSOCOM and the governments of the United Kingdom and Canada in accordance with DoDD 5530.3.

(U) At the time of assignment, USSOCOM FDO was unaware of SOCAF's Letter of Arrangement and the assignment of a Canadian liaison officer to SOCAF, or that SOCAF used the international agreement between the Commander, USSOCOM and the Government of Canada as the basis for the assignment.

(U//~~FOUO~~) SOCOM Section 1.7(e) for 1.4(d)

¹³ (U) Special Operations Planning and Liaison Element was a regionally based team of Canadian Special Operations Command liaison officers with duties concerning all SOF organizations within the U.S. Pacific Command Area of Responsibility.

officers from Canada and the United Kingdom were assigned to United States Africa Command (USAFRICOM) and served as liaison officers to SOCAF. As of December 2014, there were three FLOs assigned or attached to SOCAF in the following capacity:

- (U//~~FOUO~~) One Canadian LNO was assigned to SOCAF in August 2013, under the Defense FLO Program. The assignment of the Canadian LNO was pursuant to the required annexes and certifications to the "Memorandum of Understanding Between the Department of Defense of the United States of America and the Department of National Defence of Canada Regarding Special Operations Liaison Officers," July 2011.
- (U//~~FOUO~~) Two United Kingdom FLOs were assigned to USAFRICOM, J5, and on extended visit to SOCAF under the DPEP. These UK FLOs were also assigned to SOCEUR. Information received in response to our data call revealed that SOCAF unofficially hosted an additional United Kingdom FLO from the British Directorate Special Forces.

(S) SOCOM (b)(1) 1.4(d)

[REDACTED]

(U//~~FOUO~~) As of December 2014, the annexes and certifications for the Canadian liaison officer to SOCAF had not been ratified. According to SOCAF officials, the command was in the process of developing the Annex B to the USSOCOM and Canadian Special Forces Command's MOU. SOCAF leadership would determine and assign the appropriate contact officers and a SOCAF DDL would be drafted.

(S) SOCOM (b)(1) 1.4(d)

[REDACTED]

SOCOM (b)(1) 1.4(d)

(U) Joint Special Operations Command

(U//~~FOUO~~) The Joint Special Operations Command (JSOC) used three existing international agreements for FLOs that were concluded between USSOCOM and the governments of Australia, Canada, and the United Kingdom. JSOC provided the annexes to these existing international agreements which were in accordance with DoD regulation. However, some Annex Bs were vague in comparison to the actual duties which these foreign officers performed. According to a JSOC official, the Annex Bs for FLOs who conduct classified missions should be classified and contain the level of detail consistent with [their] required duty description.

(U) In response to our data call, JSOC conducted a review of foreign officer involvement and reported since 2011, the command has hosted 802 foreign officers' visits to elements of JSOC. According to JSOC officials, 14 FLOs were assigned to JSOC under MOUs concluded between USSOCOM and the following foreign countries:

- (U//~~FOUO~~) Five Australian Special Operations Command FLOs were assigned to JSOC to represent the Australian Special Operations Command across all staff functions within JSOC: Two Australian FLOs were assigned to JSOC's headquarters; one FLO was assigned to JSOC's Security Operations Training Facility, 3rd Operational Support Group; and two FLOs were assigned to JSOC's Combat Applications Group. The international agreement between USSOCOM and the Australian government was concluded in 2009. The first Australian FLO was assigned to JSOC in 2010.
- (U//~~FOUO~~) One Canadian SOF Command FLO was assigned to JSOC headquarters in 2014 to represent Canadian Special Forces Command across all

staff functions within JSOC. The international agreement between USSOCOM and the Canadian government was concluded in 2011.

- (U//~~FOUO~~) Eight United Kingdom of Great Britain FLOs were assigned to the JSOC to represent the United Kingdom's Director Special Forces Command across all staff functions: one FLO was assigned to the Security Operations Training Facility; three FLOs were assigned to JSOC headquarters; two FLOs were assigned to JSOC's Combat Applications Group; one FLO was assigned to JSOC's Security Operations Training Facility, 3rd Operational Support Group; and one FLO was assigned to the JSOC's Aviation Tactics Evaluation Group across all staffs of JSOC. The first British FLO was assigned to JSOC in 2011. The international agreement between USSOCOM and the United Kingdom was concluded in 2013. According to JSOC, as of December 2014, six defense FLOs remained at JSOC.

(U) Special Operation Command Forces – Central

(U//~~FOUO~~) SOCCENT did not have required international agreements for the foreign officers assigned or attached to SOCCENT or subordinate task force. According to a USSOCOM official, OUSD(P) advised USCENTCOM and SOCCENT that international agreements were required. However, he stated that the command's position was, "We don't have time for that. We are busy with the war." SOCCENT did not have required annexes, certifications, or assurances that governed the roles and responsibilities of the foreign officers who were assigned to SOCCENT or its subordinate task force. According to a USSOCOM official, USSOCOM did not maintain oversight of SOCCENT's international agreements or the assignment of foreign SOF officers.

(U) In response to our data call, SOCCENT reported 12 foreign officers were assigned or attached to SOCCENT and subordinate Combined Joint Special Operations Task Force-Iraq (CJSOTF-I) from 2011 to 2014. According to a SOCCENT representative, SOCCENT hosted four NREOs (two Jordanian and two United Arab Emirates) and eight foreign officers.

(U//~~FOUO~~) As of December 2014, there were no foreign officers assigned to SOCCENT headquarters. However, seven foreign officers remained attached to CJSOTF-I. SOCCENT reported two Australian officers, two Spanish officers, one Canadian officer, one Italian officer, and one Dutch officer deployed to Iraq with CJSOTF-I but were not assigned to USCENTCOM or SOCCENT. SOCCENT did not provide any additional information.

(U//~~FOUO~~) According to a USSOCOM official, the USSOCOM Commander did not approve the assignment of any FLOs to SOCCENT nor did USSOCOM have oversight of any foreign officers assigned to SOCCENT. SOCCENT did not provide DDLs, duty descriptions, or international agreements, in response to our data call. A USSOCOM official stated that during the [Iraq/Afghanistan] wars, SOCCENT and USSOCOM brought foreign officers into the command without international agreements and were allowed to operate that way for many years.

(U//~~FOUO~~) We issued a follow-up data call to SOCCENT requesting the following information for the foreign officers assigned or attached to SOCCENT and a complete list of names, roles, duty descriptions, and dates of assignments; the MOUs, annexes or technical agreements; any funding associated with the assignment and deployment of those foreign officers; and a determination of the continued requirement to have foreign officers at SOCCENT. According to a SOCCENT official, SOCCENT did not track the foreign officers' involvement and could not provide any additional information concerning the foreign officers.

(U) According to SOCCENT, the four NREOs only had access to the U.S. Non-secure Internet Protocol Router Network (NIPRNET) and never had access to classified spaces or the U.S. SECRET Internet Protocol Router Network (SIPRNET). SOCCENT did not provide sufficient information on the foreign officers at SOCCENT; therefore, the status of the foreign officers' involvement at SOCCENT between 2011 and 2014 could not be further evaluated.

(U) International Visits Program

(U//~~FOUO~~) Deputy Secretary of Defense Memorandum, "Accountability of Department of Defense Sponsored Foreign Personnel in the United States (U.S.)," May 18, 2004, states that DoD Components must account for DoD sponsored foreign personnel in the United States. Additionally, DoDD 5230.20, paragraph 4.8, states that DoD sponsored visits by foreign nationals to the DoD Components, except visits at activities or events that are open to the general public, must be documented using the Foreign Visits System (FVS) Confirmation Module where practicable.

(U) The International Visits Program was established by DoD to process visits by, and assignments of, foreign representatives to U.S. DoD Components. It was designed to ensure that classified information and controlled unclassified information that was to be disclosed to foreign nationals had been properly authorized for disclosure to their governments. It also ensured that the requesting foreign government or organization made administrative arrangements (e.g., date, time, and place) and provided a security assurance when classified information was involved in the visit or assignment.

(U//~~FOUO~~) USSOCOM maintained accountability of the foreign officers assigned to USSOCOM through the FVS. ~~SOCOM Section 1.7(e) for 1.4(g)~~. USSOCOM did not have oversight of foreign nationals assigned or on extended visits to its subordinate components. OUSD(P) and USSOCOM personnel stated that they were unaware of foreign officers being assigned or attached to USSOCOM component commands. A USSOCOM official stated the TSOCs and Service Components approved their own foreign visit requests.

(U//~~FOUO~~) We issued a second data-call to USSOCOM's subordinate commands and Service components. The results of the data-call identified that foreign SOF officers were assigned, attached, or on extended visits to those SOF components. Per DoDD 5530.3, the assignment of foreign officers to units outside the continental United States was not governed by the FVS.

(U//~~FOUO~~) A USSOCOM security official stated that the FVS was inadequate because the parent nation embassies submitted clearance information through the FVS and could clear a foreign officer to whatever level the embassy designated. An OUSD(P) senior official stated that although DTSA had oversight of visit policy, DTSA did not have operational control of the process because the commands approved foreign visits. The official stated his biggest concern was about "personal unofficial visits," although each installation would have a log of its visitors.

(U//~~FOUO~~) According to a FD official, OUSD(P) had not set policy for overseas foreign visit requests. At the time, overseas foreign visit requests were approved by subordinate commands and processed between base security and the respective partner nation. Based on the information provided, some subordinate commands could not fully account for all foreign SOF officers assigned or on extended visits to the TSOCS from 2011 to 2014. In December 2014, USSOCOM began an internal review to gain better visibility of the international agreements and foreign officer assignments within the USSOCOM enterprise.

(U) Funding the Integration of Foreign Officers

(U//~~FOUO~~) According to the terms of USSOCOM's concluded and pending international agreements, the travel and training expenses for the FLOs were to be paid by their home governments. USSOCOM was to request host nations' reimbursement for office facilities, equipment, supplies, and services required for the FLO to fulfill their MOU. USSOCOM officials and FLOs believed that all of the foreign officers' expenses, such as travel or training, were paid by the FLOs' home governments. However, according to other USSOCOM officials, USSOCOM had not begun to account for the daily office expenses of the foreign officers at the USSOCOM. A USSOCOM J3-I official said that there were 16 FLOs at USSOCOM whose expenses had not been billed since 2012. Exchange officers' expenses, on the other hand, were paid by the U.S. Government.

(U//~~FOUO~~) According to the Integration Center for Financial Management official, USSOCOM had not determined which office within USSOCOM had financial

responsibility for overseeing partner nation integration. The Financial Management Office, which provided coordination on the financial appendix included in each foreign officer's memorandum of agreement, was not initially aware of the reimbursement budget requirement. At the time of this evaluation, USSOCOM did not have the capability to document the cost of the FLOs. According to USSOCOM's concluded agreements, reimbursements would be made through Foreign Military Sales or Acquisition Cross-Services Agreements; however, USSOCOM did not have either option available to it in order to bill each respective country. USSOCOM was in the process of establishing a method to bill the partner nations for reimbursable costs. According to a subordinate command official, foreign officers within their respective command were not billed for normal daily costs of doing business, such as paper and electricity. See Appendix C for additional information concerning the funding associated with the integration of foreign officers.

(U) Conclusion

(U//~~FOUO~~) Between 2011 and 2014, USSOCOM was not in full compliance with applicable laws and directives concerning the assignment and use of foreign officers. A total of 27 foreign officers had been assigned or on extended visits to USSOCOM Headquarters with and without concluded international agreements. As of December 2014, 19 foreign officers remained. USSOCOM had concluded nine formal international agreements on behalf of the United States covering 11 total personnel. USSOCOM had five agreements for foreign liaison officers with Australia (2), Canada (1), Jordan (1), New Zealand (1), and United Kingdom (2) that covered a total of 7 personnel. USSOCOM had four agreements for nonreciprocal exchange officers with Australia (1), Canada (1), Denmark (1) and Spain (1) covering an additional 4 personnel. Therefore, as of December 2014, four foreign liaison officers (2-Netherlands, 1-German, and 1-Sweden) and four nonreciprocal exchange officers (1-German, 2- France, and 1-Norway) remained at USSOCOM Headquarters without concluded international agreements.

~~(S//NF)~~ SOCOM (b)(1) 1.4(d)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) In furtherance of the USSOCOM Commander's vision of the ISCC, from 2011-2014, USSOCOM issued personal invitations to the governments of France and Spain and later extended invitations to other countries to participate at the Special Operation Forces Conference. This offer constituted the initiation of negotiations for international agreements pursuant to DoDD 5530.3, Enclosure E.2.1.2.

(U) However, USSOCOM did not address the prerequisites of the delegated Circular 175 authority, which specifies the terms and conditions that must be addressed in the underlying international agreement that governs the assignment of foreign officers. Additionally, USSOCOM did not comply with the coordination requirements of DoDD 5530.3, Section 6. Therefore, the Secretary of State was not informed of USSOCOM's agreements and was unable to report the text of those international agreements to Congress as required by the Case Act.

(U) In addition, USSOCOM lacked the authority to initiate and conclude international agreements pertaining to the assignment of foreign officers under MPEP.¹⁴ OUSD (P) advised USSOCOM in May 2013 that the authority to negotiate and conclude international agreements must be requested from OUSD(P).¹⁵

¹⁴ (U) The USSOCOM FDO was aware of this limitation and advised the USSOCOM staff as early as late November 2011.

¹⁵ (U) While the general authority to conclude international agreements concerning exchange programs has been delegated to the Combatant Commands, there is no evidence that USSOCOM relied upon that delegation before OUSD(P) advised them that they did not have such authority.

(U) When the OUSD(P) learned of the existence and procedural defects of the USSOCOM action concerning the assignment of foreign officers, OUSD(P) faced several choices to remedy this matter, including negating the arrangements, potentially resulting in the return the foreign officers to their respective countries, or taking remedial actions in order to ratify the agreements, permitting the continued function of the ISCC by USSOCOM. OUSD(P) chose ratification, and took actions consistent with that course of action, including issuance of exceptions to policy concerning the proper conclusion of prerequisite international agreements, in accordance with DoDD 5530.3.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation A. 1.

(U) We recommend that the Under Secretary of Defense for Policy update DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005, to include the establishment of criteria for granting exceptions to policy and clarification of guidance on the use of extended visit requests.

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

(U) The Assistant Secretary of Defense (Acting) Special Operations/Low-Intensity Conflict, responding for OUSD(P), concurred with our findings and recommendations.

(U) Our Response

(U) OUSD(P)'s comment was responsive to our recommendation. We request that OUSD(P) update the DoD OIG concerning the status of DoDD 5230.20 revisions within 90 days of this report.

(U) Recommendation A.2.

(U) We recommend that the Commander, United States Special Operations Command:

(U) A.2.a. Ensure all international agreements for the foreign officers assigned or on extended visits to the United States Special Operations Command and subordinate commands are in compliance with Public Law 111-84, DoD Directive 5503.3, "International Agreements," July 18, 1987, Circular 175, "Authority to Negotiate and Conclude Non-Reciprocal International Defense Personnel Exchange Agreements," October 20, 2011, and Circular 175 "Authority to Negotiate and Conclude Foreign Liaison Assignments," October 17, 2011.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM commented that currently all foreign personnel assigned to USSOCOM and its subordinate commands had an approved MOA or had an OUSD(P) approved exception to policy pending the completion of their specific MOA.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation and we require no further comment.

(U) A.2.b. Ensure existing Annex Bs to the international agreements contain the level of detail and classification consistent with the foreign officer's actual mission requirement.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM responded that all "Annex Bs" (duty descriptions) for exchange officers were being modified to reflect the level of detail consistent with their duties.

(U) Our Response

(U) USSOCOM's comment was partially responsive to our recommendation. USSOCOM's response only addressed the modification of Annex B's for exchange officers. We recommend Annex B's (duty descriptions) for FLOs, as well as exchange officers, be consistent with their specific mission requirements. We request additional comments within 30 days of this report.

(U) A.2.c. Require component commanders to ensure that all required annexes, certifications, and designated disclosure letters are ratified in

accordance with Circular 175 authority and DoD Directive 5530.03, "International Agreements," July 18, 1987.

(U) United States Special Operations Command Response

(U) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM commented that the executive agreements for foreign officers assigned to Headquarters USSOCOM, component headquarters, and subordinate subunified command headquarters will be reviewed and maintained in accordance with the applicable directives and policy guidance.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We request that USSOCOM provide a written update to DoD IG concerning the status of USSOCOM's review of its international agreements and supplemental annexes within 90 days of this report. .

(U) A.2.d. Request an exception to policy for the non-reciprocal and exchange officers who are currently assigned to the United States Special Operations Command without concluded international agreements.

(U) United States Special Operations Command Response

(U) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation and stated that the recommended action was complete.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation and we require no further comment.

(U) A.2.e. Seek appropriate authority for the foreign intelligence officers assigned or attached to United States Special Operations Command and follow established procedures for the collection and exchange of intelligence in accordance with DoDD 5530.0.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, non-concurred with our recommendation. USSOCOM disputed the finding that the Command initiated agreements for the exchange of military intelligence with foreign governments before gaining the approval of DIA. USSOCOM asserted that the Command has been in compliance with all authorities and policies for intelligence-focused FLOs. USSOCOM further stated that at no time were intelligence-related FLOs assigned as Exchange Officers, and no representatives from foreign intelligence agencies have ever been assigned to USSOCOM. All foreign officers assigned to USSOCOM were representatives of their respective Ministries of Defense.

(U) Defense Intelligence Agency Response

(U) Although not required to respond, the Director of Security, DIA, responding for the Agency, commented that the exchange officers assigned to USSOCOM during this period of time were assigned under the Defense Personnel Exchange Program, of which the Defense Intelligence Personnel Exchange Program is a subset. DIA reviewed the limited information available and indicated the Canadian Deputy J2 position could be appropriately categorized as a Defense Intelligence Personnel Exchange, vice a DPEP, and would then be subject to DIA Instruction 5230.002. DIA's coordination of this response memo with USSOCOM J2 revealed an incorrectly identified Canadian NREO position with duties at the Deputy J2. The position was instead a Canadian FLO assigned to the Joint Intelligence Center, which would not be subject to DIAI 5230.002. According to DIA, USSOCOM had separately addressed this factual error in its response to the DoD IG Draft Report.

(U) Our Response

(U//~~FOUO~~) We stand by our recommendation. As written on pages 25 and 26 of this report, in November 2011 the Canadian embassy processed a foreign visit request (CA11-A3103) for a Canadian intelligence liaison officer to serve as the Deputy J2, USSOCOM. USSOCOM assigned the Canadian officer as a NREO. The international agreement for Canadian exchange officers was concluded in November 2014. The

DDIG-2016-090 / 48

Canadian officer stated that he worked as a FLO and his duties included answering Canadian SOF intelligence requirements, coordinating with other SOF units and DIA, and providing U.S. and Canadian SOF with relevant intelligence information. In July 2014, a German Bundesnachrichtendienst (BND) (the Federal Intelligence Service) FLO was assigned to USSOCOM, under a recurring visit request (ID # GM14-A660). According to the draft Annex B, USSOCOM tasked the BND FLO to facilitate intelligence exchanges and intelligence sharing with the Joint Intelligence Center, USSOCOM, in support of USSOCOM J2 focus areas. In addition the BND FLO would provide intelligence reports and support to a TSOC's request for information and intelligence requirements, and provide support for BND's staff visits to USSOCOM. As a result, our recommendation remains valid and consistent with DoDD 5530.3 and DoDD 5230.30. DoDD 5530.3 requires DIA to concur with all proposed agreements concerning intelligence and intelligence-related matters. DoDD 5230.20 requires DIA to issue guidance governing the negotiation and conclusion of agreements for the assignment of foreign intelligence officers under the Defense Intelligence Personnel Exchange Program. We request additional comments within 30 days of this report.

(U) A.2.f. Maintain oversight of all foreign Special Operations Forces assigned or on extended visit to United States Special Operations Command's subordinate commands and Service components.

(U) United States Special Operations Command Response .

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM commented that it was in the process of developing and promulgating command policy regarding oversight of foreign SOF assigned to or on extended visits across the headquarters and USSOCOM's subordinate commands based on this report's recommendations. Additionally, USSOCOM commented that the Command would monitor the international agreements entered into by its SOF Service component headquarters.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We request USSOCOM provide a written update to the DoD IG on the status of USSOCOM's policy regarding oversight of foreign SOF assigned to or on extended visits across the USSOCOM's enterprise within 90 days of this report.

(U) A.2.g. Ensure that United States Special Operations Command components maintain compliance with DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals" concerning the invitation, visit, and assignment of foreign officers.

(U) United States Special Operations Command Response

(U) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM commented that it continues to improve its foreign officer program based on recommendations in this DoD IG report.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We require no further comment.

(U) A.2.h. Eliminate the "dual" use of foreign officers (with or without concluded agreements) in accordance with current regulatory guidance.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM commented that it ensures foreign officers are only afforded exchange officer status after the conclusion of an MOA. USSOCOM also stated that it differentiates between foreign liaison and exchange officers.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We require no further comment.

(U) A.2.i. Establish a process for reimbursement of costs associated with hosting Foreign Liaison Officers.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM commented that countries were now billed for services annually via the appropriate Acquisition and Cross-Servicing Agreements.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation and we require no further comment.

(U) Finding B

(U) USSOCOM Did Not Fully Comply With SCIF Requirements

(S//NF) SOCOM Section 1.7(e) for 1.4(g)

- (U) Foreign officers assigned to USSOCOM had unfettered access to SOCOM Section 1.7(e) for 1.4(g)

- (U) SOCOM Section 1.7(e) for 1.4(g) and were authorized to escort other SOCOM Section 1.7(e) for 1.4(g) partners had access;

- (U) SOCOM Section 1.7(e) for 1.4(g)

(U//FOUO) SOCOM Section 1.7(e) for 1.4(g)

(U) Criteria

(U) IC Directive 705, "Sensitive Compartmented Information Facilities," May 26, 2010.

ICD 705 states that all IC SCIFs must comply with uniform IC physical and technical security requirements. ICD 705 is "designed to ensure the protection of SCI and foster efficient, consistent

DODIG-2016-098/52

and reciprocal use of SCIFs in the IC." ICD 705 applies to all IC accredited facilities where SCI is processed, stored, used or discussed. The Office of Security (SEC), DIA, was designated as the accrediting official for DoD SCIFs. All waivers to SCIF physical security requirements must be approved by the Head of an Intelligence Community Element, which, in USSOCOM's case, is the Director, DIA. Although the SEC was designated the sole accrediting authority for physical and technical (TEMPEST) security for permanent SCI facilities, automated information system accreditations must be obtained to process SCI.

(U) DoD Manual 5105.21-V2, "Sensitive Compartmented Information (SCI) Administrative Security Manual. DoD Manual 5105.21-V2, Enclosure 2, Physical Security, paragraph 6i(2), states "SCI-indoctrinated foreign nationals may be granted access to a SCIF either as a visitor or an embedded part of the organization per agreement between their government and the USG [U.S. Government]." The manual also states that foreign nationals will not be permitted to escort personnel. "Foreign nationals without appropriate SCI indoctrinations must not be admitted inside a SCIF unless special approval is obtained in advance by the Head of an Intelligence Community Element or designee." Paragraph 6 i(3) states, "Whenever SCI-indoctrinated foreign nationals are provided general access to a SCIF as part of their official daily duties, the organization will ensure that compensatory security measures aimed at protecting against the inadvertent or deliberate release of non-releasable information, both foreign government and USG, is taken and foreign disclosure guidelines must be followed." Paragraph 6i (3)(d) goes on to state, "Unique security procedures must be developed and clearly documented in the local standard operating procedure (SOP)."

(U) Physical Security, Access, and Counterintelligence

(U) Physical Security of the SCIF

(U) In April 2014, DIA reaccredited USSOCOM's SCIFs and authorized open storage of SCI material. DIA determined that ~~SOCOM Section 1.7(e) for 1.4(g)~~, met all the physical standards in accordance with ICD 705 and DoD Manual 5105.21.

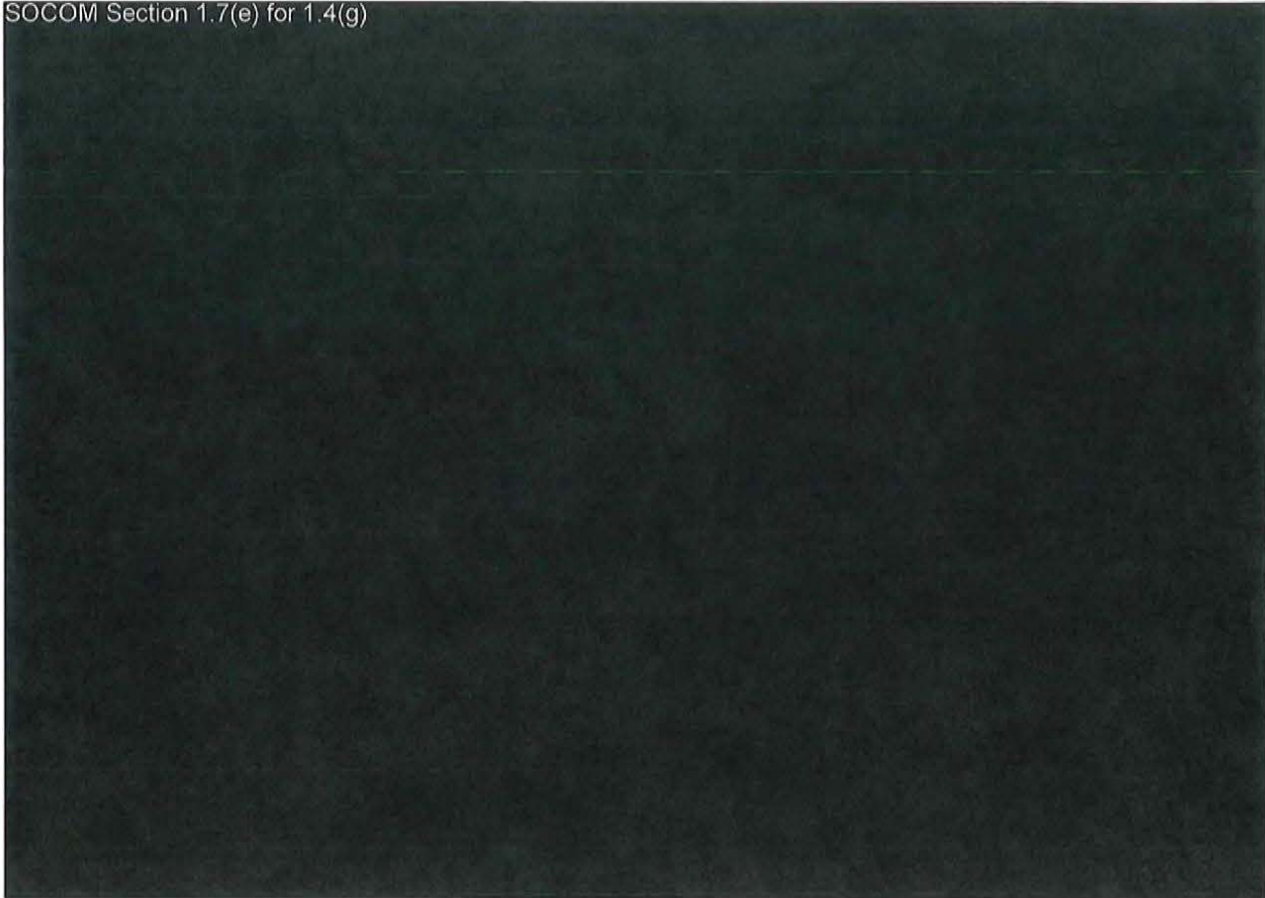
(~~G//NF~~) On April 21, 2014, DIA SEC conducted an in-progress review of USSOCOM's renovation of ~~SOCOM~~. USSOCOM's construction project modified the overall square footage of the existing SCIF, to carve out a collateral ISCC and newly renovated SCIF spaces adjacent to the ~~SOC~~. The USSOCOM Commander designed the ISCC/J3-I to function as the main collaboration hub for international SOF missions. The watch floor was to be dedicated to collateral operations. Controlled adjacent rooms were constructed, operated, and maintained for reciprocal use as a temporary secure working area. A USSOCOM senior official stated that the ISCC/J3-I location was selected based on the proximity to the ~~SOC~~ SCIF, which was the "heartbeat of USSOCOM." USSOCOM designed the ~~SOC~~ to operate 24 hours per day, seven days per week (continuous operations). Within the collateral space, one permanent SCIF (S0-14-003) was devoted to U.S. personnel only. Another SCIF (S0-14-004) was used by Commonwealth Five Eye partners.

(U) J3-International Spaces (Non-SCIF)

(U//~~FOUO~~) The J3-I was the primary location in which partner nation representatives worked (excluding those partner nation representatives who worked in the J2, Special Operations Research, Development, and Acquisition Center (SORDAC), and the ~~SOCOM Section 1.7(e) for 1.4(g)~~ had a total capacity of 105 individuals, which was configured for 63 U.S. with 37 partner nation officers. The primary workspace was based on an open floor plan to allow better integration and maximum collaboration between the U.S. and partner nation SOF. ~~SOCOM Section 1.7(e) for~~

~~(g)~~
~~(g)~~
~~(g)~~
~~(g)~~
~~(g)~~

SOCOM Section 1.7(e) for 1.4(g)



(U) Figure 1. USSOCOM J3-I Headquarters

(U) Mitigation Efforts

~~(S//NF)~~ SOCOM Section 1.7(e) for 1.4(g)



(~~C//NF~~) The Staff Assistance Visit report stated the building security posture was "top notch." DIA recommended final accreditation of the ~~SOCOM Section 1.7(e) for 1.4(g)~~

We asked DIA to clarify the language in the report which recommended granting foreign nationals operational control of the facility. The report stated:

(U) ~~SOCOM Section 1.7(e) for 1.4(g)~~

(~~C//NF~~) According to a DIA official, FVEY officers did not have operational control of a DIA facility. DIA intended to create a compartmented area under the ICD 705 guidelines. However, FVEY officers had unlimited access to DIA SCIF SO-14-004, which was created as a stand-alone FVEY SCI area. The DIA official stated that given the absence of U.S.-only information in SCIF SO-14-004 (FVEY SCIF), the risk of giving unfettered access to the only FVEY SCIF was deemed acceptable based on the mitigations identified in the SOCOM Special Security Officer's (SSO) email. The DIA security official stated the recommendation should have been to allow foreign nationals access control of the FVEY facility instead of operational control. He stated that DIA would take action to correct the terminology and ensure the SSO, USSOCOM, understands the difference.

(~~C//NF~~) We also asked DIA to clarify the language in the facility accreditation for SCIF SO-14-004, which stated that "accreditation is based on the safeguards and countermeasures identified in REF D [Email from SSO SOCOM..., Subj: FW: Status of SO-14-004, Dated: 01 May 2014]." According to a DIA security official, the information relevant to the accreditation should have been spelled out in DIA's accreditation message. DIA referenced the SSO's email and its proposed mitigations, but did not spell out the requirement in the actual accreditation message. DIA stated that it had changed that practice within the Security Branch.

(U//~~FOUO~~) In addition to a physical accreditation and TEMPEST accreditation, an automated information system security accreditation was required to process SCI electronically. USSOCOM did

not provide us with its automated information system accreditations or documentation that DIA granted foreign nationals general access to any other SCIFs located in ~~SOCOM~~.

~~(S//NF)~~ SOCOM Section 1.7(e) for 1.4(g)
[Redacted text block]

~~(S//NF)~~ SOCOM Section 1.7(e) for 1.4(g)
[Redacted text block]

¹⁶(U) TSCM involves techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to National Security Information, restricted data, and sensitive but unclassified information.

SOCOM Section 1.7(e) for 1.4(g)

(U) Foreign Officer Access to USSOCOM's SCIFs

(U//~~FOUO~~) Between 2012 and 2013, the USSOCOM Commander decided to give unescorted access to the partner nation officers in SOCOM Section 1.7(e) for 1.4(g)

. In response to our data call concerning foreign officer's access, a USSOCOM official explained that SOCOM Section 1.7(e) for 1.4(g)

(U) Reoccurring Access for Foreign Officers

(U) According to DoDM 5105.21-V2, foreign nationals without appropriate SCI indoctrinations must not be admitted inside a SCIF unless special approval is obtained in advance by the Director, DIA or designee. SOCOM Section 1.7(e) for 1.4(g)

The DIA official also stated that FLOs are not allowed unescorted access to the U.S. only parts of a SCIF. According to the DIA official, FLOs work on behalf of their country and are allowed limited access to specific information deemed releasable to their country.

(C//~~NF~~) As part of USSOCOM's integration effort, the USSOCOM Commander invited all FLOs, both SCI and non-SCI cleared, to attend the Commander's weekly meetings in the SOCOM Section . In 2013, the senior intelligence officer, USSOCOM's Director of Intelligence, authorized escorted access by non-SCI cleared foreign nationals during designated times. According to the authorization memorandum, USSOCOM risk mitigation strategies minimized the loss or compromise of U.S. SCI and non-releasable information.

(U) FVEY Partners Swipe Access

(U) According to DoDM 5105.21-V2, when SCI-indoctrinated foreign nationals are provided general access to a SCIF as part of their official daily duties, the organization will ensure that compensatory security measures aimed at protecting against the inadvertent or deliberate release of non-releasable information, both foreign government and U.S. Government, is taken and foreign disclosure guidelines must be followed. A risk assessment must weigh the benefit to the U.S. Government of foreign national personnel in the SCIF against the risk that security measures will not adequately protect against unauthorized disclosure. The results from that risk assessment will be provided to SEC, DIA for review. Regardless, the regulation stated, foreign nationals were not permitted to escort personnel.

(U//~~FOUO~~) USSOCOM security personnel believed that personnel from USSOCOM Special Security Office "did everything they could do" to secure the SCIF area. The USSOCOM Security Management official said that the ~~SOCOM Section 1.7(e) for 1.4(g)~~

[6 a.m. to 8 p.m.]. He also said that one security weakness was that the FVEY partners did not always announce their entrance into the SCIF; therefore, they could walk into "NOFORN" meetings. Another USSOCOM security official stated that the FVEY officers were on an "honor system" not to access the ~~SOC~~ during NOFORN presentations. A USSOCOM security official stated that the ~~SOCOM Section 1.7(e) for 1.4(g)~~

Joint Intelligence Center. According to the USSOCOM official, USSOCOM Deputy J3, an Australian Brigadier General, had unfettered access to ~~SOCOM Section 1.7(e) for 1.4(g)~~ USSOCOM FVEY officers, with unescorted SCIF access, were also allowed to escort foreign visitors into the areas in which they had access, which was against DoDM 5105.21-V2 policy. A USSOCOM FLO stated that the [FVEY partners] were told they were authorized to escort two years ago and that "It would be disappointing if a U.S. escort requirement was re-introduced for FVEY officers. The U.S. escort requirement would be a waste of U.S. staff effort and not recipro[cal] to your [U.S. special operations liaison officers] authorities in our nations."

(U//~~FOUO~~) According to a DIA official, foreign exchange officers are considered to be part of the work force and given limited access based on the agreement between the two countries. This access is spelled out in the DDL and is usually restricted to a specific mission. However, the officers

are generally given limited access within the work space of the assigned team. They are not authorized unlimited access to "U.S. only" areas.

(U) Special Operations Research Development and Acquisition Center

(U//~~FOUO~~) USSOCOM had civilian Science and Technology liaison representatives from the United Kingdom and Australia working at the SORDAC. These United Kingdom and Australian officers were at the SORDAC on extended visit requests and had a separate office with a safe and computer certified at the SECRET//RELEASABLE level. A USSOCOM official believed that foreign officers from the United Kingdom, Australia, Norway, and Canada assigned to USSOCOM respected the processes for science and technology requests for information; however, there was no formal process for other partner nations to request science and technology information. The USSOCOM official said that the ability to reach out to the British and Australian SOF science and technology communities was beneficial to working on joint projects.

(U//~~FOUO~~)SOCOM Section 1.7(e) for 1.4(g)
[Redacted]

[Redacted]. A J3-I official said that partner nation integration into the SORDAC was easy, as long as the agreements were in place. The civilian believed that USSOCOM learned just as much from the partner nation representatives as the partners did from USSOCOM.

(U) Conclusion

(S//~~NF~~)SOCOM Section 1.7(e) for 1.4(g)
[Redacted]

Finding B

SOCOM Section 1.7(e) for 1.4(g)
[Redacted]

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation B

(U) Revised Recommendation

(U) As a result of comments from USSOCOM, we revised draft report Recommendation B.1.a to omit the recommendation to withdraw Five Eye partners' escort authority.

(U) Recommendation B.1.a

(U) We recommend that the Commander, United States Special Operations Command:

(U) B.1.a. Discontinue the practice of Five Eye partners providing escort within SCIF spaces in order to comply with Intelligence Community Directive 705, Sensitive Compartmented Information Facilities," and DoD Manual 5105.21-V2, "Sensitive Compartmented Information (SCI) Administrative Security Manual," October 19, 2012.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, non-concurred with our recommendation. USSOCOM stated that it disputed the finding that FVEY partners were authorized to escort other foreign nationals into SCIFs in which FVEY partners had access. Additionally, USSOCOM provided the response that USSOCOM's Manual 380-6 stated that only U.S. cleared personnel are authorized escort of personnel in the SCIF. FVEY partners have never been afforded SCIF escort privileges.

(U) Our Response

(U) USSOCOM's comment was non-responsive to our recommendation. We agree FVEY officers did not have the written authority to escort personnel into SCIFs in accordance with U.S. policy and directive. However, as written on page 59 of this report, a USSOCOM FLO stated that in 2012, the FVEY partners were told that they were authorized to escort foreign visitors into areas in which they had access, to included SCIFs. Our evaluation concluded that USSOCOM FVEY officers, with

unescorted SCIF access, routinely escorted foreign visitors into the areas in which the FVEYs had access. Therefore, USSOCOM did not adhere to USSOCOM Manual 380-6 by allowing USSOCOM FVEY officers to perform escort duty. For clarity, we have restated our recommendation that the USSOCOM Commander discontinue the practice of allowing FVEY officers escort privileges. We request that USSOCOM provide written comments to revised Recommendation B.1.a within 30 days of this report.

(U) B.1.b. Restrict Five Eye partners' swipe access to the Global Mission Support Center when the meeting sign does not illuminate "RELEASABLE."

(U) United States Special Operations Command Response

(U) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation and we require no further comment.

(U) B.1.c. Establish formal procedures for processing requests for information concerning science and technology information by foreign liaison officers.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM provided the comment that in July 2014 USSOCOM published Regulation 10-4, "Partner Nation Requests for Information and Requests for Support." Since then, all partner-nation-related requests adhere to the guidance within USSOCOM Reg. 10-4 to ensure accountability and appropriate review, to include those pertaining to science and technology.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation and we require no further comment.

(U) Recommendation B.2.

(U) We recommend the Director, Defense Intelligence Agency:

(U) B.2.a. Establish appropriate policy and procedures for integrating partner nation representatives into Defense Intelligence Agency accredited Sensitive Compartmented Information Facilities

(U) Defense Intelligence Agency Response

(U) The Director of Security, DIA, responding for the Agency, concurred with our findings and recommendations. DIA commented that it was in the process of completing draft policy concerning the integration of partner nation representatives into DIA-accredited SCIFs. A completion date could not be determined due to further coordination with the Office of the Under Secretary of Defense (Intelligence).

(U) Our Response

(U) DIA's comment was responsive to our recommendation. We request that DIA provide a written update to the DoD IG concerning the status of the draft policy integrating partner nation representatives into DIA-accredited SCIFs within 90 days of this report.

(U) B.2.b. Review the accreditation for the Five Eye Sensitive Compartmented Information Facility (S0-14-004) and ensure the accreditation certificate is in accordance with Defense Intelligence Agency and Intelligence Community Directive 705 requirements.

(U) Defense Intelligence Agency Response

(U) The Director of Security, DIA, responding for the Agency, concurred with our findings and recommendations. DIA further stated that this action was reviewed and corrected.

(U) Our Response

(U) DIA's comment was responsive to our recommendation. We request DIA update the DoD OIG on what actions were taken to correct the accreditation certificate for the Five Eye Sensitive Compartmented Information Facility (S0 14-004) within 90 days of this report.

DDOIG-2016-090/64

(U) B.2.c. Review the United States Special Operations Command's automated information systems accreditation.

(U) Defense Intelligence Agency Response

(U) The Director of Security, DIA, responding for the Agency, suggested that the review of USSOCOM's automated information systems accreditation be addressed by USSOCOM J6, the accrediting official responsible for automated information systems in accordance with Department of Defense Manual 5105.21.V2.

(U) Our Response

(U) DIA's comment was not responsive to our recommendation. DIA did not concur or non-concur with our finding or recommendation. DIA's facility reaccreditation message "Facility Reaccreditation for ~~SOCOM Section 1.7(e) for~~ April 24, 2014, stated that "this reaccreditation was one of three [facility, TEMPST, and automation information system] accreditations required to process SCI electronically and must be maintained on file within the facility." The SEC, DIA, identified the Chief Information Officer, DIA as the designated automation authority within the DoD and the IC. DoDM 5105.21.V2 states that the designated approval authority will decide whether to grant accreditation approval to operate a system. We request that DIA review USSOCOM's automated information system accreditations and determine if these accreditations are in full compliance with DIA's facility reaccreditation message cited above, DoDM 5105.21.V2, ICD 705, and ICD 503. We request DIA provide comments to the DoD OIG concerning USSOCOM's automation information system accreditation requirements within 30 days of this report.

(U) Finding C.

(U) USSOCOM Improperly Disclosed Classified Information to Foreign Officers

(U) USSOCOM was not in full compliance with security regulations in its disclosure of classified information to foreign officers. This situation existed because USSOCOM or subordinate commands:

- (U//~~FOUO~~) Shared classified military information and controlled unclassified information with foreign officers before having all DDLs, security assurances, or proper release authority;
- (U//~~FOUO~~) Released bi-lateral information and foreign government information without the concurrence of the appropriate host nations; and
- (U//~~FOUO~~) Conducted meetings and shared information with partner nations that were not coordinated through USSOCOM's Foreign Disclosure Management System or FDO.

(U//~~FOUO~~) As a result, foreign officers received information that they were not authorized to receive.

(U) Criteria

(U) Under the terms of National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 1, 1988,¹⁷ (NDP-1) the SECDEF and the Deputy SECDEF are the only officials within DoD who may grant [unilateral] exceptions to NDP-1. However, in most cases, exceptions to policy are granted or denied by the

¹⁷ (U) The NDP-1 provided to designated disclosure authorities on a need-to-know basis from the Office of the Director for International Security Programs, OUSD(P).

National Disclosure Policy Committee.¹⁸ Under DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992, the Secretary of Defense has delegated disclosure authority to the Secretaries of the Military Departments and other DoD officials whose decisions must be compliant with NDP-1.

(U) DoD Directive 5230.11 also implements NDP-1 and provides policy, responsibilities, and procedures governing the disclosure of classified military information to foreign governments and international organizations. Paragraph 4.4 states that classified military information must not be disclosed to foreign nationals until the appropriate designated disclosure authority receives security assurance memorandums from the foreign government of the individuals who are cleared to receive the information. Paragraph 6.1.1 states that before any discussions with foreign representatives on the negotiation of an international agreement, the DoD components must determine the extent to which classified military information will be required for release and obtain disclosure authorization for the information. Enclosure 3, "NDP-1 Disclosure Criteria, Conditions, and Limitations," prohibits the disclosure of classified information originated by or for another Department or Agency, or officially obtained from a foreign government. An exception could be if the Department or Agency consents to the release or if the information has been conveyed by the foreign government with express written consent to its further disclosure.

(U) DoD Directive 5230.20, paragraph 4.5, states that access by foreign nationals to classified information must be in accordance with DoD Directive 5230.11 and DoD Directive 5200.1-R, "Information Security Program," January 1997 (subsequently superseded by DoDM 5200.01, "DoD Information Security Program: Overview, Classification and Declassification," 24 February 2012). They will have access only to information that does not exceed the level authorized under NDP-1 for release to their governments. Exceptions to NDP-1 will not be granted to accommodate the assignment of FLOs, DPEP, Co-operative Program Personnel, or foreign personnel arrangements.

¹⁸ (U) The National Disclosure Policy Committee is the central authority for formulating, promulgating, administering, and monitoring national disclosure policy.

(U//~~FOUO~~) USSOCOM Directive 550-2 states that USSOCOM and component FDOs are responsible for review of any classified military information and controlled unclassified information or bi-lateral classified aspects of topics nominated by the Component or TSOC for discussion. The directive also states that all products, information, data, and materials developed as a result of the ISCC/J3-I's request for information and request for support process, require coordination with USSOCOM's command FDO or J3-I's FDO for disclosure and release to foreign partners. For any topics nominated by the Interagency Partnership Program, the Interagency Partnership Program must ensure a foreign disclosure review from interagency original classification authority¹⁹ is accomplished.

(U) Foreign Disclosure Program

(U//~~FOUO~~) The USSOCOM foreign disclosure program was split between the Command foreign disclosure office and the Directorate for Intelligence (J2) foreign disclosure office. USSOCOM's foreign disclosure program had established foreign disclosure policy and procedures for the protection of classified information and enabling of information sharing. USSOCOM Command Foreign Disclosure Office was responsible for international programs, including export licenses and technical data transfers, and the protection of classified military information as defined by NDP-1. USSOCOM established a foreign disclosure management system in which all requests for release of classified military information and controlled unclassified information was processed through the FDO or designated representative. According to a FDO, most liaison officers and command personnel followed USSOCOM's Foreign Disclosure Management System policy - with the exception of the ~~SOCOM Section~~ who was the subject of several foreign disclosure incidents.

(U//~~FOUO~~) An OUSD(P) official stated that disclosure to foreign officers was based on the security assurance and position description for the foreign officer. According to a USSOCOM foreign disclosure official, the security assurances should be maintained on

¹⁹ (U) Original Classification Authority. The authority given by SECDEF to classify military information that originates in and is controlled by a specific command. Original Classification Authority cannot be further delegated.

foreign officers assigned to USSOCOM and components. According to a USSOCOM FDO, classified military information shared with current partner nations was based on an approval from the geographical combatant commands. The geographical combatant commands determined the "need-to-know" to share the type of information that was being provided at the commander's update brief. According to a USSOCOM FDO official, the foreign disclosure office advised the USSOCOM staff to protect bi-lateral agreements at all cost.

(U) Disclosure of Classified Information to Foreign Officers

(U//~~FOUO~~) According to our data call response concerning foreign officer access to classified military information or controlled unclassified information, a USSOCOM official replied, "The exchange officers only receive information on a limited basis and only when there is a clearly defined benefit to the United States." A USSOCOM security official clarified the accuracy of USSOCOM's response. He stated that the answer, "is correct if the standard for 'defined benefit' is it helps relationships with the FLOs."

(U//~~FOUO~~) ~~SOCOM Section 1.7(e) for 1.4(a)~~ to establish trust with the foreign partners. He accepted the risk of inadvertent disclosure and, according to USSOCOM personnel, pressured those in the command to share more with the foreign partners. USSOCOM personnel were concerned that when leadership put pressure on subordinates, people would make mistakes or act unethically trying to meet the Commander's intent.

(U//~~FOUO~~) According to a USSOCOM official, USSOCOM's leadership was advised that non-SCI partner nation officers ~~SOCOM Section 1.7(e) for 1.4(d)~~ The senior official stated that USSOCOM started circumventing the process for bringing foreign officers into the SCIF and alleged that during a SOCCENT planning session, the J3-1 broadcast a ~~SECRET//REL~~ briefing out of the ~~SOCOM Section 1.7(e) for 1.4(g)~~ participants were cleared for the information. ~~SOCOM Section 1.7(e) for 1.4(g)~~ had the capability to stream video to offices outside the SCIF. A USSOCOM cyber security official stated he was unaware of a tool that did discretionary routing [sending data from the big screens] out of the ~~SOC~~.

(U//~~FOUO~~) USSOCOM did not own most of the classified data it worked with and was required to request permission from the appropriate owner before releasing information to a foreign partner. A senior staff official stated USSOCOM briefed bi-lateral information to the GCCs without the concurrence of the foreign government or originating authority.

(U//~~FOUO~~) A USSOCOM investigation was done on a J3-I representative who changed briefing information, after the presentation had been approved for release by the FDO, in order to brief unauthorized information. The investigation concluded that DoS information was briefed to the ~~SOC~~ concerning Peru purchasing night-vision goggles without obtaining permission from DoS.

(U//~~FOUO~~) In addition to planning meetings and operational briefings, partner nation representatives were invited to the Commander's Update Briefing in which each SOF subordinate commands briefed the USSOCOM Commander on the current status of SOF personnel, SOF operations, security corporation activities, and other key-leader events. Some foreign officers within USSOCOM and SOF Components complained that they were not receiving enough information to effectively do their jobs. The Australian exchange officer serving as the USSOCOM Deputy J3 voiced concerns over being excluded from weekly updates distributed to key leaders within USSOCOM Headquarters.

(U//~~FOUO~~) On June 10, 2013, the Commander informed a group of senior personnel that the new Australian SOCOM Deputy J3 would have access to everything except a few special access programs. On July 2, 2013, a DIA employee assigned to USSOCOM reported to DIA his concern that NOFORN data was being improperly released by USSOCOM HQ to the FLOs and the Australian general officer newly assigned as Deputy J3. The DIA SEC team investigated this report to determine whether there was a valid basis to the employee's concern and to review the processes in place regarding release and disclosure of classified national security information to embedded foreign exchange officers and found no improper disclosure or release of classified national security information to the Australian Deputy J3. The DIA SEC team determined that the DIA

Finding C

employee and other personnel within the USSOCOM staff weren't sufficiently educated in what USSOCOM was doing to enable foreign officer access.

(S//NF) SOCOM (b)(1) 1.4(d)

[Redacted text block]

(S) SOCOM (b)(1) 1.4(d)

[Redacted text block]

Finding C

SOCOM (b)(1) 1.4(d) [Redacted]

~~(S//NF)~~ SOCOM (b)(1) 1.4(d) [Redacted]

(U//FOUO) A USSOCOM security official stated that USSOCOM was drafting packages to request DIA's authority to negotiate intelligence sharing agreements with the military intelligence services of six partner nations. According to the USSOCOM security official, DIA and USD(I) had not granted USSOCOM the authority to exchange intelligence information with existing partner nations at USSOCOM, but did allow USSOCOM to release documents that were REL [releasable] to the respective countries.

(U) Special Operations Command – Africa

~~(S)~~ SOCOM (b)(1) 1.4(d) [Redacted]

SOCOM (b)(1) 1.4(d)

(U) Special Operations Command – Central

(U//~~FOUO~~) In 2013, a SOCCENT Foreign Disclosure Program Assessment stated that USCENTCOM issued DDLs to the USCENTCOM's FDOs. SOCCENT's FDOs were not issued DDLs and not authorized to approve the release or disclosure of classified SOF information to foreign SOF officers at SOCCENT. The assessment stated that SOCCENT FDOs were not integrated into partner nation's engagements, and that they should have been proactive to ensure that USCENTCOM had the legal and policy requirements for the establishment of FLO MOUs, in accordance with DoDD 5230.20. The assessment cited that SOCCENT FDOs did not know:

- (U//~~FOUO~~) if there were concluded MOUs for the FLOs or NREO at SOCCENT;
- (U//~~FOUO~~) of the existence or scope of applicable DDLs;
- (U//~~FOUO~~) how classified military information was disclosed to foreign officers assigned to SOCCENT; and
- (U//~~FOUO~~) the contact officer(s) for the foreign officers assigned to SOCCENT.

(U) Foreign Disclosure Office Staffing Shortages

(U//~~FOUO~~) USSOCOM foreign disclosure officials stated that USSOCOM components lacked full-time FDO manning, which seriously limited foreign disclosure capability at the commands. According to a USSOCOM foreign disclosure official, SOCEUR, JSOC, USASOC, AFSOC, and NAVSPECWARCOM had full-time FDOs. SOCAF had an approved FDO position that was vacant. All other TSOCs and Service components relied upon FD guidance as an additional duty within their staffs.

(U//~~FOUO~~) According to a USSOCOM official, personnel who were tasked to provide FD support to a TSOC cannot focus on the strategic projects that support the entire SOF enterprise. As result, multiple projects were left undone. The USSOCOM official stated

DDIG-2016-028/73

that projects included the daily management of products in USSOCOM's foreign disclosure management system, building and supporting USSOCOMs' FDO Network (to include training), maintaining the FVS, and providing support to USSOCOM's technology transfer. According to another USSOCOM official, the lack of FD support within the TSOCs and Service components was the reason provided to the Australian Deputy J3 as to why there was minimal effort to make information releasable. FDOs were challenged with handling the amount of information that required foreign disclosure review. According to the 2013 SOCCENT FDO assessment, FDOs were serious about their responsibilities, but had little time away from their day-to-day jobs to devote to FD tasks and duties. Similar to the SOCCENT FDOs, other FDOs did not have flexibility to support exercises or real-world operations. The report found that FDOs were in a constant reactive mode, which prevented them from being involved in many activities.

(U//~~FOUO~~) The 2013 USSOCENT FDO assessment recommended the SOCCENT FD office add at least one full-time FDO, which would provide the time and expertise to build an effective foreign disclosure program. According to a JSOC official, USCENTCOM conducted a staff study and determined that JSOC's FD office needed at least four FDOs. However, given that no growth in the headquarters staff would be permitted, any increase in FDOs would have to be realigned from another part of JSOC. There was insufficient support for such realignment and JSOC's FD office remained undermanned, perpetuating the risk to its foreign disclosure program. A 2010 manpower survey recommended USSOCOM's FD office staff be increased to ten personnel. The command did not support an increase from five personnel. Subsequently, USSOCOM hired a GS-15 to oversee the command's FD program.

(U) Lack of Foreign Disclosure Education

(U) The 2013 SOCCENT FDO assessment also stated that there was no program to teach FD awareness to all SOCCENT personnel. It recommended that "a command-wide foreign disclosure education program is needed to make SOCCENT personnel aware of the redlines in dealing with the assigned FLOs, foreign visitors, foreign conferences, and requests for information from foreign nationals, etc." According to FD officials, due to the increase in security violations, the current Deputy, J3-1, tasked the directorate to get

retrained on FD procedures. The USSOCOM Command FDO established a three-day FDO course on FD requirements. However, there was no set requirement for FD training throughout the USSOCOM enterprise.

(U) Conclusion

~~(S//NF)~~ SOCOM (b)(1) 1.4(d) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation C

(U) We recommend that the Commander, United States Special Operations Command:

(U//~~FOUO~~) C.1. Cease the systematic disclosure of NOFORN information to the Australian Deputy J3, conduct a thorough investigation of the instances of NOFORN information disclosed to date, take action as appropriate against any individuals found culpable, and revise United States Special Operations Command procedures to prevent future NOFORN disclosures.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, non-concurred with our recommendation. USSOCOM commented that it disputed the finding that NOFORN information was ever systematically disclosed to the Deputy J3, an Australian 1-Star Flag Officer. USSOCOM referred to the results of a 2013 DIA investigation that "found no improper disclosure or release of classified information to the Australian Deputy J3. The DIA team determined that the DIA employee (who made the accusation) and other people on the USSOCOM staff weren't sufficiently aware of what USSOCOM was doing to enable foreign officer access." USSOCOM believes the DIA finding to be accurate, stating that at no time was any NOFORN information deliberately or systematically disclosed to any foreign liaison or exchange personnel at USSOCOM. USSOCOM's procedures to prevent disclosure of NOFORN information are in accordance with DOD and DIA guidance and policy.

(U) Our Response

(U) We stand by our recommendation. We agree that in 2013 DIA found no improper disclosure or release of classified information to the Australian Deputy J3 and that USSOCOM had procedures in place to mitigate the improper disclosure of NOFORN

information. However, we found that USSOCOM representatives did not adhere to established policy and procedures concerning the disclosure of NOFORN information. Our evaluation concluded that subsequent to the DIA review, there were allegations that NOFORN and non-releasable data was improperly released by USSOCOM to the Australian Deputy J3. A USSOCOM senior staff officer acknowledged that he changed the electronic classification marking on a classified network from SECRET//NOFORN to SECRET//REL AUS in order to bypass security firewalls and facilitate classified information getting to the Australian Deputy J3. In addition, the USSOCOM senior staff officer stated that reclassifying information to bypass firewalls had been a common practice within USSOCOM J3 for years and was supported by the command. We request USSOCOM provide an update to the DoD OIG within 30 days of this report, concerning the status of allegations that NOFORN data was disclosed to the Australian Deputy J3, USSOCOM.

(U) C.2. Identify the number of foreign disclosure officers required by the Headquarters and subordinate commands under the United States Special Operations Command purview to maintain the international exchange programs.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM responded that corrective actions were on-going. USSOCOM provided the following comments:

- In September 2015, the Special Operations Capability Requirement Board officially approved the establishment of the J3-I Branch within the J3 Operations Directorate and approved the assignment of FLO personnel directly within the J3-I.
- USSOCOM proposed broad changes to the TSOC manning and capabilities via a DOTMLPF-P Change Recommendation. The DOTMLPF-P Change Recommendation identified the need for additional FDO billets at the TSOCs,

where none had previously existed, as well as the requirement for the development of additional, tailored "tetragraphs" to facilitate information sharing.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We request that USSOCOM update the DoD OIG concerning the status of its FDO billets within 90 days of this report.

(U) C.3. Determine whether the foreign disclosure offices at the Headquarters and subordinate commands under the United States Special Operations Command purview are adequately staffed.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM responded that corrective action was ongoing. In addition to the corrective actions for Recommendation C.2, USSOCOM consolidated staff responsibility for foreign disclosure, technology transfer analysis, intelligence engagement, and foreign visit management under the USSOCOM J2 Intelligence Directorate.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We request USSOCOM update the DoD OIG concerning staffing of its foreign disclosure offices within 90 days of this report.

(U) C.4. Assess the training requirements for foreign disclosure officers and ensure all special operation forces' foreign disclosure officers receive the necessary training.

(U) United States Special Operations Command Response

(U) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM responded that analysis is ongoing.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We request that USSOCOM update the DoD OIG on the outcome of its analysis and selected course of action within 90 days of this report.

(U) C.5. Assess the requirements for security education and training for personnel who are involved with international exchange programs and foreign government information, or work in coalition or bi-lateral environments, or in offices, activities, or organizations hosting foreign exchange officers.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM responded that corrective action was on-going. USSOCOM commented that it was reviewing its portfolio of international training to better inform the headquarters workforce of their role, function, and responsibilities in dealing with and managing foreign liaison and exchange personnel at the headquarters and its subordinate commands.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We request that USSOCOM provide a written update to the DoD OIG concerning their corrective actions within 60 days of this report.

(U) Finding D

(U) USSOCOM Did Not Fully Comply With Automated Information System Requirements

(U//~~FOUO~~) USSOCOM was not in full compliance with applicable directives concerning the installation and use of secure communication systems within a U.S. SCIF. This situation existed because:

- (U//~~FOUO~~) Between 2012 and 2014, USSOCOM officials facilitated the installation of the French and German's national secure communication systems before having concluded international agreements that codified the security procedures, minor facility modification, and fiscal responsibility associated with the installation of these national systems. Although in 2014 OUSD(P) granted a temporary exception to policy for the use of these national systems (exception to policy also included the Spanish system), USSOCOM still has not obtained concluded international agreements.
- (U//~~FOUO~~) USSOCOM lacked the approved automation information system accreditations required to process SCI within USSOCOM facilities and therefore was not in compliance with full SCIF accreditation requirements.

(U//~~FOUO~~) As a result, USSOCOM may have processed SCI material in areas that were not accredited for SCI automation.

(U) Criteria

(U) DoDM 5105.21 V2, "Sensitive Compartmented Information (SCI)
Administrative Security Manual: Administration of Physical Security, Visitor

Control, and Technical Security. DoDM 5105.21 V2 states that information assurance managers must obtain Automated Information System accreditations in accordance with ICD 705 and ICD 503. The designated approval authority must decide whether to grant accreditation approval to operate a system based on all available documentation and mitigating factors. Paragraph 6(i) prescribes essential safeguards relating to the integration or visit of foreign nationals to include foreign exchange officers, FLOs, or embedded foreign officers within DIA accredited SCIFs. Any deviations must be addressed with the responsible FD office, the supporting counterintelligence element, and be approved by the respective head of an intelligence community element or their designee. If information systems are involved, the designated approval authority for the particular network must give its approval.

(U) Information Security Responsibilities

(U//~~FOUO~~) Cyber Security Division, Information Technology (J6), USSOCOM, was responsible for the command's computer networks, the acquisition of tools for the network, the certification and accreditation of the networks, and the approval process. The Cybersecurity Officer said that the USSOCOM networks were not originally designed with the idea of foreign nationals being in the building, so actions were necessary to secure the network. The Cybersecurity Office and J6 worked in concert with the ISCC planning team to develop options to secure USSOCOM's network. In order to de-SCIF a portion of ~~SOCOM Section 1.7(e) for 1.4(e)~~

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

(U//~~FOUO~~) The Cybersecurity Officer said that USSOCOM requested Navy Air System Command perform a study of improvement to USSOCOM's network and that \$4 million had been identified in the FY15 budget to secure the infrastructure. The Cybersecurity Officer said that SIPRNET currently had some vulnerability, but the Joint Worldwide Intelligence Communications System (JWICS) was secure.

(U) Foreign Officer Access to Automation Systems

(U//~~FOUO~~) Foreign officers within USSOCOM enterprise had access to either U.S. NIPRNET, U.S. SIPRNET, TOP SECRET communications – STONEGHOST²⁰ account, SECRET coalition communications – Battlefield Information Collection and Exploitation System (BICES), or individual country national automation systems. According to a USSOCOM J6 official, network cabling within the ~~SOCOM Section 1.7(e) for 1.4(g)~~. The networks were not designed to be used in a building where foreign officers worked, so USSOCOM re-routed or used a protected distribution system to protect cabling from the classified systems. According to a USSOCOM J6 official, cybersecurity was an area in which USSOCOM had taken steps to reduce risk. However, as a cybersecurity official acknowledged, there remained vulnerabilities, particularly to the SIPRNET domain.

(U) Improper Installation of Foreign National Secure Communication Systems

(U) In accordance with DoD's delegated Circular 175 authority, DoD is required to include an addendum to an international agreement that includes the proposed secure communications system language before the installation of foreign government's secure communication system within a DoD organization. The addendum requires the organization that houses the foreign system to provide a workspace, codified security procedure, fiscal arrangements, installation, setup, use of the workspace, modification of facilities, and maintenance.

(U//~~FOUO~~) Between 2012 and 2014, USSOCOM allowed French and German officers to install and use their national secure systems within USSOCOM J3-I workspace before having a concluded international agreement that codified security procedures, fiscal arrangements, installation, setup, use of the workspace, modification of facilities, and maintenance. In April 2014, USSOCOM requested a temporary exception to policy to allow the French and German exchange officers to continue using their national secure

²⁰ (U) STONEGHOST is a REL FVEY JWICS that is monitored by DIA.

communication systems in USSOCOM's J3-I work spaces. These exchange officers used their national secure communications systems to communicate with their parent government in support of USSOCOM and their foreign government. USSOCOM further requested approval for the Spanish exchange officer to install a secure communication system. In April 2014, the OUSD(P) granted USSOCOM a temporary exception to the policy in order to allow the French, German, and Spanish exchange officers to use their national secure communication systems in USSOCOM work spaces.

(U) Inability to Verify Accreditation of USSOCOM SCIF for Automated Information Systems

(U) DoDM 5105.21-V2 states information assurance managers must obtain automated information system accreditations in accordance with ICD 705 or ICD 503. The designated approval authority must decide whether to grant accreditation approval to operate a system based on all available documentation and mitigating factors.

(U//~~FOUO~~) We were unable to determine if DIA had accredited the USSOCOM SCIF for automated information systems. We made multiple data calls to USSOCOM and DIA requesting a copy of the automated information accreditations. USSOCOM officials had not provided a copy of the DIA automated information systems accreditation as of the issuance of the draft report.

(U) Risk to Information Security

(U//~~FOUO~~) According to a USSOCOM official, the command accepted the risk of having foreign officers at USSOCOM with swipe and unescorted access. Foreign officers had ~~SOCOM Section 1.7(e) for 1.4(g)~~ Although USSOCOM used cameras to monitor ~~SOCOM Section 1.7(e) for 1.4(g)~~ gaining access to SIPRNET cables in the ceiling, installing listening devices, and having access to classified printers. According to a USSOCOM Cyber Security official, USSOCOM ~~SOCOM Section 1.7(e) for 1.4(g)~~. According to the USSOCOM official, in ~~SOCOM Section 1.7(e) for 1.4(g)~~, \$4 million in fiscal year 2015 was identified to further secure USSOCOM's infrastructure.

(S) SOCOM Section 1.7(e) for 1.4(g)
[Redacted text block]

(U) Possible Data Spillage

(U//FOUO) A USSOCOM official stated that there were numerous opportunities for SOCOM Section 1.7(e) for 1.4(g). As a result, the official believed that SOCOM may have had an inadvertent disclosure once a week. According to a USSOCOM security official, most violations involved SOCOM Section 1.7(e) for 1.4(g) stated that half of the security violations did not result in an actual security incident (that is what was thought to be a classified spillage was actually data that was inappropriately classified). However, does operate with two systems SOCOM Section and sometimes documents ended up on multiple systems with multiple classifications.

(U) Lack of Training

(U//FOUO) SOCOM Section 1.7(e) for 1.4(g)
[Redacted text block]
One USSOCOM official stated that USSOCOM personnel did not have training on writing for release. This caused the

improper classification of documents. Another USSOCOM official stated that USSOCOM component personnel were not writing for release and had the tendency to work backwards in their classification approach. He stated that component personnel started at a higher classification and then go down to [releasable] FVEY.

(U) Conclusion

(U//~~FOUO~~) From 2011 to 2014, USSOCOM officials allowed French and German foreign nationals to install and use their national secure communications systems within the SCIF before the conclusion of international agreements. In 2014, USSOCOM requested and received a waiver from USD(P) allowing the French, German, and Spanish officers to operate their secure communication systems until their international agreements were concluded and ratified the pertinent security procedures, fiscal arrangements, modifications, and installation foreign government's secure communication systems. As of December 2014, these international agreements had not been concluded. The unlimited exception to policy seems to diminish the relevance of the applicable policy that requires concluded agreements and annexes with appropriate language concerning foreign representatives' before the use of their national secure systems. Unlimited exceptions to policy provide no incentive to become compliant with DoDD 5530.3 and Circular 175 procedure.

(U//~~FOUO~~) Since the integration of foreign officers into USSOCOM, the command took reconfigured its information technology infrastructure, upgraded automation systems, and was in the process of completing upgrades to their secure domain to reduce risk to its automated information systems. However, vulnerabilities remained, particularly to the SIPRNET domain, because foreign officers had unfettered access to ~~SOCOM~~ Main.

(U//~~FOUO~~) USSOCOM requires a DIA automated information systems accreditation, but has not provided the DoD Office of Inspector General with copies of their accreditation. SCIF areas that operate systems without an approved automated information accreditation are not fully SCIF accredited and in violation of DoDM 5105.21-V2 and ICD 705.

Finding D

(U//~~FOUO~~) Finally, the lack of training may have contributed to accidental spillages and inadvertent disclosures, increasing vulnerabilities to USSOCOM's information technology.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation D

(U) We recommend that the Commander, United States Special Operations Command:

(U) D.1. Conclude international agreements, with appropriate language, for the French, German, and Spanish non-reciprocal exchange officers, allowing the continued use of their ~~SOCOM Section 1.7(e) for 1.4(g)~~

(U) United States Special Operations Command Response

~~(U//FOUO)~~ The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM responded that the analysis was ongoing. The Spanish MOA was complete. The French and German MOAs remained in negotiation as of the writing of this report, and their presence in the headquarters is governed by an OUSD(P) approved Exception to Policy. All French and German personnel under that Exception to Policy are treated as Liaison Officers until the agreements are concluded. Additionally, partner national classified information systems do not ride on or physically touch any of the USSOCOM networks. Connection was made through a commercial information line to the local service provider. The countries that utilized this capability were billed for that service via the ACSA process described in Annex A, par. 8 above. Additionally, the paragraph citing this problem under Finding D implies that the French and German systems were installed inside a U.S. SCIF, but that was not correct. The French and German systems were installed in the collateral J3-1 spaces only after DIA had accredited those spaces.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. Although not part of this recommendation, we agree that the French and German systems were installed in

the J3-I spaces. We request that USSOCOM provide written update to the DoD OIG concerning the outcome of its analysis and selected course of action within 90 days of this report.

(U) D.2. Obtain automated information systems accreditations for the secure facilities that process sensitive compartmented information electronically.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, non-concurred with our recommendation. USSOCOM responded that USSOCOM provided the appropriate Authority to Operate (ATO) documentation in accordance with ICD 503 governing the new Risk Management Framework for its ~~SOCOM~~ systems. USSOCOM maintained that the provided ATOs acceptably represent automated information system accreditation documents.

(U) Our Response

(U) USSOCOM's comment was partially responsive to our recommendation. On September 17, 2015, USSOCOM provided a site ATO (authorization to operate) and stated that USSOCOM ISSM could provide USSOCOM's SCIF accreditation letters. USSOCOM provided no other automated information systems accreditations for USSOCOM's SCIF. We request that USSOCOM update the DoD OIG concerning automation system accreditations or ATOs for all appropriate systems within USSOCOM SCIFs within 30 days of this report.

(U) D.3. Establish a comprehensive training program to educate all United States Special Operations Command personnel in "writing for release" to reduce the risk and incidents of misclassifying information and potentially excluding its availability to partner nations.

(U) United States Special Operations Command Response

(U//~~FOUO~~) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM responded that corrective action was ongoing. USSOCOM commented that in November 2015, Commander, USSOCOM, published the guidance: "We need to view 'writing for release' as a key enabler of our trans-regional efforts. If we view partner collaboration, integration, and de-confliction as critical factors in our ability to counter a growing threat, then we need to quickly adopt habits that allow us to give, and gain, information worthy of our relationships. This will have to play out in our briefings - our audiences, briefers, and assessments will need to become increasingly partner-oriented. Our partners - who we fully involved in deep dives of our previous battle rhythm - need the same access to the new battle rhythm. This is charter not only for HQ USSOCOM staff, but for our components, the TSOCs, our Interagency/Intelligence Community Liaison Officers, and our J3-I partners as well. The whole enterprise needs to embrace this." Accordingly, action continues in many forms to accomplish the Commander's intent.

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. We request that USSOCOM update the DoD OIG within 90 days of this report, concerning the specific actions being taken to educate USSOCOM enterprise on "writing for release."

(U) D.4. Incorporate recommendations from the United States Special Operations Command Cybersecurity Readiness inspection into guidance to reduce the risk of vulnerable systems.

(U) United States Special Operations Command Response

(U) The Deputy Commander, USSOCOM, responding for the Command, concurred with our recommendation. USSOCOM stated that it incorporated the recommendations of the inspection into J3-International policy, training, and guidance.

Finding D

(U) Our Response

(U) USSOCOM's comment was responsive to our recommendation. No further comment is required.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation. We evaluated USSOCOM's compliance with applicable statutes, DoD or IC directives, and security procedures.

(U) We focused on five areas of concern: 1) the assignment and employment of foreign officers; 2) foreign disclosure and access to sensitive, controlled, or classified information; 3) placement of foreign officers in proximity to security facilities and information systems; 4) security and counterintelligence risks associated with the integration of foreign officers into USSOCOM; 5) and funding of SCIF renovations and information systems. We did not evaluate each of the 5 areas of concern in all 13 SOF organizations. We did not comment on areas in which we did not find compliance issues.

(U) Our evaluation included 13 SOF organizations and data covering the four year period from 2011 to 2014. We issued 22 data calls and conducted 61 interviews with subject-matter experts. We obtained and reviewed documentation from the OUSD(P), DoD General Counsel; USSOCOM; AFOSI; DIA; TSOCs; and Service components. We conducted follow-up requests as needed.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this evaluation

(U) Prior Coverage

(U) No prior coverage has been conducted on foreign officers at USSOCOM during the last 5 years.

(U) Appendix B

(U//FOUO) Foreign Officers Assigned to USSOCOM Headquarters, Subordinate Commands, and Service Components (2011-2014)

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
USSOCOM							
Australia	Deputy J3	Non-reciprocal DPEP (NRDPEP)	16-May-13	23-Jul-13	9-Dec-12	31-Dec-14	
Australia	SOCOM/J3-I	Visit	23-Jul-14	6-Mar-09	7-Jan-12	31-Dec-14	6-Jun-14 CDR ext. MOU thru 5 Mar 19
Australia	SORDAC	Science & Technology FLO	23-Jul-14	6-Mar-09	11-Dec-12	31-Jan-15	Waiver 3-Jul-14 thru NA
Canada	SOCOM/J3-I	FLO	17-Dec-09	29-Jul-11	23-Jul-11	31-Jul-15	
Canada	Deputy J2	NRDPEP	8-Sep-14	7-Nov-14	30-Nov-11	30-Sep-15	
Denmark	SOCOM/J3-I	NRDPEP	26-Jun-13	15-May-14	23-Jun-14	4-Jul-15	MOU not ratified by NREO
Denmark	SOCOM/J3-I	NRDPEP	26-Jun-13	15-May-14	14-Jun-13	1-Jul-14	MOU not ratified by NREO
Germany	SOCOM/J3-I	NRDPEP	26-Jun-13	NA	29-Feb-13	1-Mar-16	Waiver 3-Jul-14 thru NA
Germany	SOCOM/J3-I	FLO	NA	NA	7-Jul-14	6-Jul-15	
France	ISCC/J3-I	Temp NRDPEP	11-May-12	NA	14-May-12	NA	Temp Waiver 11-May-12 thru NA

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
France	SOCOM/J3-I	Visit	NA	NA	28-Jul-14	27-Jan-15	
France	SOCOM/J3-I	Visit	10-Sep-12 NRDPEP	NA	18-Jun-12	1-Sep-15	Temp Waiver May - Sep 12 and 3-Jul-14 thru NA
France	National Capital Region	NA	NA	NA	11-Oct-12	10-Oct-14	
United Kingdom	SOCOM/J3-I	FLO	23-Jun-11	28-Aug-13	5-Aug-13	5-Aug-15	MOU not ratified by FLOs
United Kingdom	SORDAC	Science & Technology/ FLO	23-Jun-11	28-Aug-13	5-Aug-13	31-May-15	MOU not ratified by FLOs
Jordan	SOCOM/J3-I	FLO	12-Dec-13	10-Jul-14	16-Sep-14	30-Sep-15	MOU not ratified by FLO
NATO	National Capital Region	FLO	NA	NA	NA	NA	DTSA requested MOU
NATO	SOCOM	FLO	NA	NA	28-Sep-12	15-Sep-14	DTSA requested MOU
Netherlands	SOCOM/J3-I	Visit	NA	NA	14-Jan-13	2-Feb-15	Waiver 3-Jul-14 thru NA
Netherlands	SOCOM/J3-I	Planner	26-Jun-13 Changed to FLO	NA	14-Sep-13	24-Oct-14	Waiver 3-Jul-14 thru NA
Netherlands	SOCOM/J3-I	Planner	26-Jun-13 Changed to FLO	NA	19-Sep-14	31-Dec-14	Waiver 3-Jul-14 thru NA
New Zealand	SOCOM/J3-I	FLO	13-Jan-14	11-Feb-14	13-Jan-14	31-Jan-16	
Norway	SOCOM/J3-I	Visit	26-Jun-13 NRDPEP	NA	1-Aug-14	1-Aug-15	Waiver 3-Jul-14 thru NA
Norway	SOCOM/J3-I	Visit	26-Jun-13 NRDPEP	NA	2-Aug-12	15-Aug-14	Signed Annex A but no MOU
Spain	SOCOM/J3-I	NRDPEP	23-Sep-13	19-Mar-14	11-Aug-14	25-Aug-17	MOU need SCS language for host nation system

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
Spain	SOCOM/J3-I	NRDPEP	23-Sep-13	19-Mar-14	1-Oct-13	22-Aug-14	MOU need SCS language for host nation system
Sweden	SOCOM/J3-I	Visit	13 Aug 14 FLO	NA	5-Aug-13	1-Aug-16	Waiver 3-Jul-14 thru NA
Finland		NRDPEP	18 Jul 14				
Italian		NRDPEP	17-Jul-14				
Japanese		NRDPEP	22-Aug-14				
Korea		NRDPEP	18-Jul-14				
Lithuania		NRDPEP	17-Jul-14				
Singapore		NRDPEP	18-Jul-14				
United Arab Emirates		FLO	11-Jun-4				
Poland		NRDPEP	18-Jul-14				
Peru		NRDPEP	17-Jul-14				
Israel							
SOCAF							
United Kingdom	British FLO to SOCAF and deputy FLO to USAFRICOM	FLO	NA	None	1-Aug-13	1-Feb-15	
United Kingdom	FLO to SOCAFRICA/ USAFRICOM Draft Position Description being coordinated.	FLO	NA	None	Unknown	1-Nov-14	No Annex B, DDL 8-Sep-14

DODIG-2016-098 / 94

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
Canada	Canadian FLO responsible for the development of SOF military plans and management of existing military plans within the Africa AOR.	FLO	NA	None	31-Jul-13	Present	Delegation of Disclosure Authority was not determined No DDL, Annex B, or contact officer
SOCCENT							
Jordan	NA	NRDPEP		None	1-Aug-12	1-Aug-13	
Jordan	NA	UNK		None	Unknown	1-Aug-13	
United Arab Emirates	NA	NRDPEP		None	1-Aug-13	1-Nov-13	
United Arab Emirates	NA	NRDPEP		None	Unknown	Unknown	
CJSOTF-I							
Australia	NA	NA		None	10-Oct-14	14-Dec-14	
Australia	NA	NA		None	20-Dec-14	Present	
Australia	NA	NA		None	20-Dec-14	Present	
Canada	NA	NA		None	17-Oct-14	Present	
Spain	NA	NA		None	20-Nov-14	Present	

DODIG-2016-098 / 95

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
Spain	NA	NA		None	20-Nov-14	Present	
Italy	NA	NA		None	9-Dec-14	Present	
Netherlands	NA	NA		None	15-Nov-14	Present	
SOCNORTH							
Canada	Vice Commander. Advise the commander on all aspects of SOF activity, employment, and capability.	NRDPEP		7-Nov-14	11-Jul-14	31-Aug-17	Annex A 20-Nov-14
Canada	J35 Action Officer. Serve as a SOCNORTH interface with international partners. Deploy as a member of a SOCNORTH Special Operations Joint Task Force or Special Operations Forward Liaison Element.	NRDPEP		7-Nov-14	31-Jul-14	31-Jul-17	
SOCAPAC							
Australia	Australian FLO to SOCPAC. Member of the Australian Special Operations Command (SOCOMD).	FLO			1-Jul-14	1-Jan-16	Annex B2 29-Jul-11

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
Canada		FLO			1-Jul-14	1-Jul-17	
JSOC							
Australia	Australian SOCOMD FLO. Represent Australian SOCOMD across all staff functions within JSOC	FLO		6-Mar-09	6-Dec-10	5-Dec-12	
Australia	Australian SOCOMD FLO. Represent Australian SOCOMD across all staff functions within JSOC	FLO		6-Mar-09	10-Oct-11	20-Jan-13	
Australia	Australian SOCOMD FLO with duty at Security Operations Training Facility	FLO		6-Mar-09	9-Dec-13	9-Dec-14	USSOCOM MOU ext. thru 5-Mar-19
Australia	Australian SOCOMD FLO to JSOC	FLO		6-Mar-09	1-Dec -12	18-Jan-15	USSOCOM MOU ext. thru 5-Mar-19
Australia	Australian SOCOMD FLO to JSOC	FLO		6-Mar-09	16-Dec-14	10-Feb-15	USSOCOM MOU ext. thru 5-Mar-19
Canada	Canadian Special Forces Command (CANSOFCOM) FLO to JSOC	FLO		29-Jul-11	1-Jul-14	31-Jul-16	
United Kingdom	Defence Special Forces (DSF) UK FLO to JSOC Combat	FLO		28-Aug-13	25-Jul-12	13-Jul-13	

Appendix B

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
	Applications Group						
United Kingdom	DSF UK FLO to JSOC Combat Applications Group	FLO		28-Aug-13	11-Sep-11	30-Nov-13	
United Kingdom	DSF UK FLO to JSOC	FLO		28-Aug-13	10-Jan-13	20-Jan-14	
United Kingdom	DSF UK FLO to JSOC Security Operations Training Center	FLO		28-Aug-13	01-Apr-13	1-Apr-14	
United Kingdom	HQ DSF Air Ops UK FLO to JSOC with duty at the Aviation Tactics Evaluation Group (AVTEG)	FLO		28-Aug-13	16-Sep-13	19-Jun-14	
United Kingdom	Act as the DSF UK FLO to JSOC Aviation Tactics Evaluation Group	FLO		28-Aug-13	17-Jun-13	31-Jul-15	
United Kingdom	DSF UK FLO to JSOC	FLO		28-Aug-13	1-Jul-13	31-Dec-15	
United Kingdom	HQ DSF Air Ops UK FLO to JSOC with duty at the Aviation Tactics Evaluation Group (AVTEG)	FLO		28-Aug-13	8-Feb-14	1-Mar-16	

DDIG-2016-098 / 98

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
AFSOC							
United Kingdom	International Exchange Partner. SOF Pilot. Attached to the 15th Special Operations Squadron	DPEP		MOU not evaluated	1-Jul-10	31-Jul-14	
United Kingdom	International Exchange Partner. Special Operations Pilot. Attached to the 15th Special Operations Squadron	DPEP		MOU not evaluated	15-Jan-14	31-Jan-17	
NAVSPEC-WARCOM							
United Kingdom	Assault Team Operator. Position UNK. On extended visit for the incoming PEP to conduct training before his 2 year deployment to USA with troops at Portsmouth, VA	DPEP		MOU not evaluated	2-May-14	31-Jul-16	
United Kingdom	Assault Team Operator I, assigned to attend JADED THUNDER debrief and also to interact with NSWDC's UK DPEP.	DPEP		MOU not evaluated	24-Jun-13	20-Aug-15	
Australia	Assault Team Operator assigned as the Troop Executive Officer, SASR (ARMY)	DPEP		MOU not evaluated	14-Nov-14	16-Jan-17	

Appendix B

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
France	ST-4 Assistant Troop Co/French exchange officer to the NSWG-2 at JEB Little Creek/Ft Story, IN.	DPEP		MOU not evaluated	2-Sep-13	30-Sep-15	
Germany	Combat Swimmer Instructor assigned as a Maritime Assistant	DPEP		MOU not evaluated	1-Jul-13	1-Aug-15	
Italy	Platoon leader AOIC - Advanced Training assigned to, Norfolk, VA	DPEP		MOU not evaluated	8-Dec-14	2-Jan-15	
Italy	Combat Swimmer Instructor	DPEP		MOU not evaluated	6-Nov-13	30-May-15	
Norway	ST-10 Assistant Troop CO assigned as an OD MCPO	DPEP		MOU not evaluated	22-Jul-13	1-Aug-15	
USASOC							
Germany	Assigned to USASOC HQs as a German Liaison Officer	FLO		MOU not evaluated	1-Apr-11	30-Sep-14	
Germany	Assigned to USASOC HQs as a German Liaison Officer	FLO		MOU not evaluated	1-Sep-14	30-Sep-17	
Netherlands	NA	FLO		MOU not evaluated	16-Jul-11	1-Aug-14	
Netherlands	NA	FLO		MOU not evaluated	1-Jul-14	1-Aug-17	
Australia	Assigned to the 2/75 RR as an Exchange Officer (Army)	MPEP		MOU not evaluated	1-Dec-12	31-Jan-14	
Australia	Assigned to the SOTF as the SASR Troop XO,	MPEP		MOU not evaluated	1-Dec-12	18-Jan-15	

DOBIC-2016-098 / 100

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
	ASSOCOMD (Army)						
Australia	Assigned to the 2/75 RR as an Exchange Officer, 2d Commando Regt	MPEP		MOU not evaluated	20-Jan-14	31-Dec-14	
Australia	Assigned to the 1 SFGA as a Special Forces Operator, 2 CDO Regt	MPEP		MOU not evaluated	12-Jun-13	17-Jun-15	
Australia	Assigned to the SOTF as a SI Climbing/Survival SASR	MPEP		MOU not evaluated	10-Dec-14	31-Dec-16	
Australia	Assigned to 1 SFGA as a SF SNCO, AUS SOCOMD	MPEP		MOU not evaluated	1-Dec-14	1-Feb-17	
Canada	Assigned to SOTF	MPEP		MOU not evaluated	NA	NA	
Canada	Assigned to SOTF as a CAP, CANSOF	MPEP		MOU not evaluated	1-Jul-14	31-Aug-15	
Colombia	Assigned to the Special Warfare Center and School (SWCS) as a Captain, Colombian Army	MPEP		MOU not evaluated	1-Apr-12	1-Apr-14	
Colombia	Assigned to the SWCS as a Sergeant,	MPEP		MOU not evaluated	15-Jun-12	15-Jun-14	
Colombia	Assigned to the SWCS as an Exchange Officer, Colombian Army	MPEP		MOU not evaluated	7-Jun-14	1-Jun-16	
Colombia	Assigned to the SWCS as a Sergeant	MPEP		MOU not evaluated	26-Aug-14	26-Aug-16	

Country	Position / Location	Billet Type	USD(P) Authority To Negotiate	MOU Concluded	Arrival Date	Departure Date	Misc
Germany	Assigned to the 6th MISB as an Exchange Officer	MPEP		MOU not evaluated	14-May-09	14-May-12	
Germany	Assigned to the 6th MISB as an Exchange Officer and Psychological Operations	MPEP		MOU not evaluated	1-Jul-12	30-Jun-15	
United Kingdom	Assigned to the 75 Ranger Regiment as an Exchange Officer	MPEP		MOU not evaluated	22-Jul-13	15-Jul-15	
United Kingdom	Assigned to the 75 Ranger Regiment as an Exchange Officer	MPEP		MOU not evaluated	1-Aug-11	12-Jul-13	
SOCEUR	N/A						
SOCKOR	N/A						
SOC SOUTH	N/A						
MARSOC	N/A						

(U) Appendix C

(U) Response to House Armed Services Committee and Other Relevant Information

1. (U) What was the USSOCOM Commander's authority and intent in the ISCC?

(U//~~FOUO~~) **Answer.** We did not find a specific directive that authorized the USSOCOM Commander to establish the ISCC. A USSOCOM senior official stated that USSOCOM derived its authority to build partnership capacity through the words echoed in national policy, the National Defense Strategy, and presidential speeches such as President Obama's "West Point"²¹ speech that mentioned "partnerships" more than 30 times. According to the USSOCOM senior official, building partnerships should include the USSOCOM headquarters because that was where planning took place.

(U) Commander's Intent for the ISCC

(U//~~FOUO~~) On September 4, 2011, USSOCOM Commander announced his vision to expand USSOCOM's support to the GSN by including partner nation's SOF representatives in USSOCOM. The USSOCOM Commander said,

(U//~~FOUO~~) to achieve my vision of including Partner Nation SOF Representatives into the SOCOM Headquarters, we will provide the greatest possible access to our facilities as well as appropriate access to our communications and information sharing systems. We will accommodate each nation's security requirements and ensure sensitive intelligence is protected in accordance with the laws and foreign disclosure policy of participating nations.

²¹ (U) President Barack Obama's speech to the United States Army Military Academy, West Point was delivered as part of the commencement ceremony for the class of 2014 on 28 May, 2014.

(U) ISCC Purpose

(U//~~FOUO~~) According to the Special Operations Forces 2020 (SOF 2020) paper, "A History of the Global SOF Network Operational Plan Team," March 2014, "the primary purpose of the ISCC was to enhance decision support for the Commander, U.S. Special Operations Command (USSOCOM) and our international partners in order to support, strengthen, and expand the Global SOF Network and to support the growth and interoperability of global SOF partners." See Introduction, "History of USSOCOM's International Special Operation Force Coordination Center (J3-I)" for additional details.

2. (U) Did USSOCOM have the appropriate authority and approval to implement a foreign liaison officer program and defense exchange program at USSOCOM?

(U) **Answer.** The USSOCOM Commander had the authority to implement a foreign liaison program and DPEP, under DoDD 5530.3, "International Agreements," June 11, 1987; CJCSI 2300.010 and DoS Circular 175, "Authority to Negotiate and Conclude Non-Reciprocal International Defense Personnel Exchange Agreements," October 20, 2011 and "Authority to Negotiate and Conclude Foreign Liaison Assignments", October 17, 2011. In 2011, USSOCOM lacked the necessary approvals; whereas, USSOCOM was prohibited from initiating, negotiating, or concluding an international agreement, without prior written approval by the OUSD(P) or designated official.

(U) The OUSD(P) DTSA eventually granted the USSOCOM Commander the authority to negotiate international agreements with 21 foreign governments.

(U) In accordance with 10 U.S.C. § 113, the SECDEF is the principal assistant to the President in all matters relating to DoD. The SECDEF has direction and control over the DoD, with the authority, unless specifically prohibited by law, to perform any of their functions or duties, or exercise any of their powers through, or with the aid of such persons in or organizations of the Department of Defense as they may designate. In paragraph 13, DoD Directive 5530.3, the SECDEF has the delegated authority to negotiate and conclude certain international agreements to the CJCS for other than uni-Service matters. In paragraph 2, CJCSI 2300.01D, the CJCS further delegated this authority to the combatant commanders. However, paragraph 8.4., DoD Directive 5530.3, states that all proposed international agreements having policy significance must be approved by the

NOIIG 2016-098 / 104

OUSDP) before any negotiation thereof, and again before they are concluded. The DoS issued Circular 175 authority to negotiate and conclude international agreements²² based on pre-approved DoS template agreements with NATO allies and other specified countries or their ministries.

(U) See Introduction "Criteria" and Finding A for additional details.

3. (U) What was USSOCOM's authority and use of foreign officers within USSOCOM's staff?

(U//~~FOUO~~) **Answer.** The National Defense Authorization Act, 2010, (Public Law 111-84), Section 1207 governed the assignment of defense exchange officers. DoD Directive 5230.20 governs the DoD International Visits Program, the FLO Program, DPEP, the Cooperative Program Personnel Program, and foreign personnel arrangements according to Section 2608(a) of title 10, United States Code. International agreements were USSOCOM's Commander's legal authorization to integrate foreign officers into USSOCOM. Beginning in 2012, the USSOCOM Commander did not have complete legal authority to integrate foreign officers into USSOCOM.

(U) There were two NREOs who were officially part of USSOCOM staff. The USSOCOM Commander assigned an Australian officer as the USSOCOM's Deputy Operations Officer (J3) and a Canadian officer as USSOCOM Deputy Intelligence Officer (J2). These officers were assigned pursuant to international agreements for NREOs. The other foreign officers at USSOCOM were working under the auspices of a FLO, NREO, or hybrid of an exchange officer working as a liaison officer. See Finding A and Finding C for additional details.

4. (U) Was USSOCOM in compliance with SCIF regulations?

(U//~~NF~~) **Answer.** USSOCOM was partially compliant with ICD 705 and DoDM 5105.21 physical security requirements. However, USSOCOM was not in compliance with the visitor access requirements, as outlined in DoDM 5105.21-V2.

²² (U) These international agreements were referred to as memorandum of understanding, memorandum of agreement, or technical agreements.

(~~C//NF~~) USSOCOM was in compliance with SCIF physical security requirements. The DIA reaccredited USSOCOM's SCIFs with authorized open storage of SCI material. DIA determined that ~~SOCOM Section 1.7(e) for 1.4(g)~~, met all the physical standards in accordance with ICD 705 and DoDM 5105.21-V2.

(U) DODM 5105.21-V2, Enclosure 2 Physical Security, paragraph 6 i(2), stated, "SCI-indoctrinated foreign nationals may be granted access to a SCIF either as a visitor or an embedded part of the organization per agreement between their government and the USG." The manual states that foreign nationals must not be permitted to escort personnel. Foreign nationals without appropriate SCI indoctrinations must not be admitted inside a SCIF unless special approval is obtained in advance by the head of an intelligence community element or designee. Paragraph 6 i(3) states, "Whenever SCI-indoctrinated foreign nationals are provided general access to a SCIF as part of their official daily duties, the organization will ensure that compensatory security measures aimed at protecting against the inadvertent or deliberate release of non-releasable information, both foreign government and USG, is taken and foreign disclosure guidelines must be followed." Paragraph 6 i(3)(d) goes on to state; "Unique security procedures must be developed and clearly documented in the local standard operating procedure (SOP)." See Finding B for additional details.

5. (U) What funding sources did USSOCOM use for the construction and renovation to USSOCOM HQ's SCIF?

(U//~~FOUO~~) **Answer.** USSOCOM's SCIF modifications were not budgeted as part of its Program Objective Memorandum. The Office of Integration Center for Financial Management was tasked with resourcing the expanded support to the GSN and the reconstruction associated with the integration of partner nation representatives into USSOCOM. According to a USSOCOM financial management official, USSOCOM did not view the renovations to its SCIF as construction, but viewed it as a modification to an existing facility. Additionally, USSOCOM did not view partner nation's integration efforts as a "new start." Therefore, USSOCOM did not seek congressional authorization.

(U//~~FOUO~~) According to a February 7, 2014, briefing to the USSOCOM Deputy Commander, the ISCC workspace was expected to open on April 11, 2014. The updated cost estimate for the project was more than \$7.2 million. An acquisition officer associated with the reconstruction project

stated that the construction and renovation was funded with O&M funds. There was no need for military construction funding because USSOCOM was not building a new building and they were not changing the purpose of the ~~SOCOM~~. According to the acquisition official, O&M funding limits for the building renovation were based on a percentage of the original building cost and the purpose of the building.

(U//~~FOUO~~) As of mid-2014, the J3-I project costed USSOCOM approximately \$7.125 million. These costs included approximately \$2.4 million in renovation costs and approximately \$4.7 million in collateral requirements, such as furniture, information technology hardware and installation, and security requirements. USSOCOM used \$2.48 million in Procurement funds and \$4.64 million in O&M funds. ~~SOCOM Section 1.7(e) for 1.4(g)~~

Office paid for the majority of the costs (on a reimbursable basis), USSOCOM initially spent less than \$125,000. O&M funds made up approximately 75% of the USSOCOM budget. However, there was no program line in USSOCOM's budget for the J3-I.

(U) Funding of BICES

(U//~~FOUO~~) USSOCOM was originally required to fund expansion and manning of the BICES system after the USD(I) BICES Office funded installation of the initial capability. The USD(I) BICES Office became USSOCOM's Servicing Agency and provided acquisition assistance which included the ordering of equipment, software and licensing on a reimbursement basis. USSOCOM used Procurement funds to purchase new terminals and O&M funds to pay for the contractors and for terminal upgrades. When the USD(I) BICES Office had additional money available, it was used to help combatant commands expand their BICES capabilities. USSOCOM and subordinate commands often reimbursed USD(I) BICES Office at the end of the fiscal year to help support the program.

(U) FY 2012. USSOCOM sent a \$498,000 Military Interdepartmental Purchase Request to add an SOF Exploitation portal.

(U) FY 2013. USSOCOM procured equipment to expand the ~~SOCOM Section 1.7(e) for~~ headquarters to 168 workstations and 9 video teleconference suites.²³

(U) FY 2014. SORDAC sent a \$2.483 million Military Interdepartmental Purchase Request for a SOCEUR effort. USASOC sent a \$223,000 Military Interdepartmental Purchase Request for dedicated USASOC O&M support. USSOCOM HQ sent a Military Interdepartmental Purchase Request for approximately \$124,000 to expand ~~SOCOM Section 1.7(e) for 1.4(g)~~ Center. SOCEUR sent an \$110,000 Military Interdepartmental Purchase Request to procure dedicated storage equipment, and a \$62,000 Military Interdepartmental Purchase request for deployable ~~SOCOM Section~~.

(U) Funding of Foreign National Secure Communication System Installation

(U//FOUO) In 2013, before the installation of the German secure communication system, a USSOCOM networks official expressed concerns with the legality of USSOCOM funding the installation of foreign government national secure systems. USSOCOM FDO personnel advised that the law required a concluded memorandum of agreement, which USSOCOM did not have with Germany. Other than simple administrative support, such as office space and equipment, a concluded international agreement would not allow host party (USSOCOM) funds to be spent to install communication systems for the parent government. A USSOCOM Staff Judge Advocate added that providing a separate communication suite for national business would be the responsibility of the foreign government.

²³ (U) Office of Undersecretary of Defense (intelligence) BICES could not provide the total amount spent on expanding US BICES for USSOCOM in 2013.

(S//NF) SOCOM (b) 1.4(a)
[Redacted text block]

(S//NF//FISA) SOCOM (b) 1.4(a)
[Redacted text block]

(S//NF) SOCOM (b) 1.4(a)
[Redacted text block]

³ (U) USSOCOM is the only unified or specified command with its own Research, Development & Acquisition function focused on SOF specific equipment. This SOF specific equipment is usually cutting edge and therefore highly sought after by both allies and adversaries.

These risks can be mitigated by changing current practices, consistent enforcement policies, training staff and establishing an effective and objective oversight mechanism.

(U//~~FOUO~~) A USSOCOM physical security officer said that USSOCOM headquarters was most vulnerable to the risk of technical penetration of the SCIF when foreign officers are walking through the spaces, but multiple personnel said that the threat has been mitigated through security in depth.²⁴

(~~S//NF~~) SOCOM (b) 1.4(a)

[REDACTED]

[REDACTED]

[REDACTED]

(U//~~FOUO~~) USSOCOM subordinate commands or Services did not provide counterintelligence assessments or report any counterintelligence investigations conducted by their command. Two security violations concerning a foreign partner were reported.

(U) Foreign Officer Misconduct

(U//~~FOUO~~) According to a USSOCOM FD official, USSOCOM did not have an established foreign officer misconduct program. The USSOCOM FD official, USSOCOM was exploring the process to establish such a program. USSOCOM was reviewing the Army's foreign officer's disciplinary program which the Army's G2 briefed during the USD(P) Executive Conference in 2013 as a model. In the meantime, USSOCOM did not have disciplinary action procedures to discourage violations of policy and procedures by foreign officers assigned to USSOCOM.

²⁴ (U) Security in-Depth. A determination by the Senior Agency Official that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include visitor access controls, use of an Intrusion Detection System, closed circuit video monitoring or other safeguards that mitigate the vulnerability of unalarmed areas during non-working hours.

~~(S//NF)~~ SOCOM (b) 1.4(a) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

~~(S//NF)~~ SOCOM (b) 1.4(a) [Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) Appendix E

(U) Benefits of Foreign Officer Assignment to the USSOCOM Enterprise

(U//~~FOUO~~) According to USSOCOM foreign officers, being liaison officers at USSOCOM was a great enabler to their government because of the access to available resources and the sharing of information which allowed the partner nation's SOF commanders to make better decisions. A USSOCOM FLO, who was assigned to USSOCOM for several years, believed that FLOs tried to find niches where their government could reciprocate the vast amount of information the U.S. provided. Foreign officers stated that they also benefited from working at USSOCOM J3-I by their: participation in regional working groups, their support to joint planning, and their doctrine lessons learned. Foreign officers indicated that their countries were satisfied with the placement at USSOCOM and benefited from them seeing the Commander's strategic picture. One FLO stated that their countries benefited more by having representation at USSOCOM than at the TSOCs.

(U//~~FOUO~~) According to the former Chief of Staff, USSOCOM, the assignment of the French was critical to USSOCOM's mission to establish partnerships not only with other nations, but also with our NATO partners. The USSOCOM Commander believed this assignment would contribute considerably to USSOCOM's world-wide efforts.

(U//~~FOUO~~) In December 2013, the Netherlands conducted an emergency extraction of personnel from South Sudan. While able to evacuate eight personnel, they were unable to secure their Embassy upon departure. In order to address this issue, the Dutch liaison officer was able to request assistance from USSOCOM. The Commander USSOCOM tasked his staff to support the request. The liaison officer was able to easily track, through email, the progression of the request. In the end, the predicted violence did not occur, neutralizing the need to secure the embassy. But, because of the efforts of the Dutch liaison officer, all was in place to fulfill the request, should events have required the course of action.

SOCOM (b) 1.4(a) [Redacted]
[Redacted]

SOCOM Section 1.7(e) for [Redacted] SOCOM (b) 1.4(a) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

SOCOM Section 1.7(e) for [Redacted] SOCOM (b) 1.4(a) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U//~~FOUO~~) Despite the violations to National and DoD authorities, USSOCOM personnel assessed that the assignment of foreign officers to the USSOCOM enterprise was helpful. Personnel said that the U.S. and its partner nations benefited from the joint and consistent efforts achieved through the integration of foreign partners within the USSOCOM enterprise. USSOCOM personnel believed that building pre-crisis partnerships helped U.S. SOF achieve increased interoperability.


(U//~~FOUO~~) There are inherent risks associated with the integration of foreign officers into the USSOCOM enterprise. These risks could be further mitigated if:

- (U//~~FOUO~~) USD(P) updated DoDD 5230.03 and DIA established policy that covers the integration of foreign officers into DIA SCIFs;
- (U//~~FOUO~~) USD(P) increased oversight and regulatory enforcement of international agreements and assignment of foreign officers to DoD organization;
- (U//~~FOUO~~) USSOCOM followed regulatory guidance concerning the assignment, access, and dual accreditation of foreign officers;
- (U//~~FOUO~~) USSOCOM requested an exception to national policy for nonreciprocal officers to remain at USSOCOM; and
- (U//~~FOUO~~) USSOCOM maintained oversight and accountability for all foreign SOF officers within the USSOCOM enterprise.

(U) Appendix F

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

~~SECRET//NOFORN~~



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5070 DEFENSE PENNSYLVANIA
 WASHINGTON, DC 20304-2000


POLICY 17 000

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL for INTELLIGENCE

SUBJECT: Audit of a Classified Program (Project No. D2014-DINT01-0206.000)

(U) Thank you for completing this review and providing the report. We concur with the findings and recommendations in this report. We ask that you provide this report to the Director of the Defense Technology Security Administration (DTSA) in order to review their equities related to DoDD 5230.20.

(U) My POC for this matter is (b) (6)





Theresa M. Whelan
 Assistant Secretary of Defense (Acting)
 Special Operations/Low-Intensity Conflict

~~SECRET//NOFORN~~

DODIG-2016-098 / 117

(U) Defense Intelligence Agency Comments

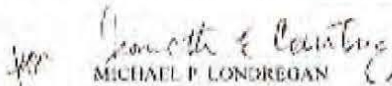
 UNCLASSIFIED DEFENSE INTELLIGENCE AGENCY <small>WASH DC 20315-6000</small> 	
U-15-095,048/SEC	
To:	DoD Inspector General Office
SUBJECT:	(U) Department of Defense Inspector General Evaluation of Foreign Officer Involvement at the United States Special Operations Command
References:	a. (U) DoD IG Draft Report, Evaluation of Foreign Officer Involvement at the United States Special Operations Command dated 25 March 2016 (S/NF) b. (U) Intelligence Community Directive 705 "Sensitive Compartmented Information Facilities," May 26, 2010 c. (U) Department of Defense Manual 5105.21, V2 "SCI Administrative Security Manual," October 19, 2012 d. (U) Department of Defense Directive 5230.20 "Visits and Assignments of Foreign Nationals," June 22, 2005 e. (U) Defense Intelligence Agency Instruction 5230.002 "Visits and Assignments of Foreign Government Representatives," July 3, 2014
1.	(U) The Defense Intelligence Agency (DIA), as the Accrediting Official, acknowledges and agrees with the findings and recommendations for items B.2 a., "Establish appropriate policy and procedures for integrating partner nation representatives into Defense Intelligence Agency accredited Sensitive Compartmented Information Facilities" and B.2 b., "Review the accreditation for the Five Eye Sensitive Compartmented Information Facility (50-14-004) and ensure the accreditation certificate is in accordance with Defense Intelligence Agency and Intelligence Community Directive 705 requirements." Item B.2 b. has already been reviewed and corrected, and we are currently working toward the completion of item B.2 a. No completion date is available at this time; it will require further coordination and review by DIA elements and the Office of the Under Secretary of Security for Intelligence.
2.	(U) The DIA, Office of Partner Engagement is responsible for administering the Defense Personnel Exchange Program (DPEP) in accordance with Department of Defense Directive 5230.20 and Defense Intelligence Agency Instruction (DIAI) 5230.002 "Visit and Assignments of Foreign Government Representatives." All the exchange officers assigned to USSOCOM during this period of time were assigned under the Defense Personnel Exchange Program, of which the Defense Intelligence Personnel Exchange Program is a subset. A review of the limited information available indicates the Canadian Deputy J2 (DJ2) position could be appropriately categorized as a DIPEP, vice a DPEP, and would then be subject to DIAI 5230.002. However, coordination of this response memo with USSOCOM J2 revealed
UNCLASSIFIED	

UNCLASSIFIED

an incorrectly identified Canadian non-reciprocal exchange officer (NREO) position with duties at the D12. The position is instead a Canadian Foreign Liaison Officer assigned to the Joint Intelligence Center, which would not be subject to DMI 5230.002. USSOCOM has separately addressed this factual error in its response to the DoD IG Draft Report.

3. (U) Recommend item B.2.c., "Review the United States Special Operations Command's automated information systems accreditation" be addressed by SCUM J6, the accrediting official responsible for automated information systems in accordance with Department of Defense Manual 5105.31, V2.

(U) The DIA point of contact is Gerald Anderson, SCIF Management Branch. (b) (6)


MICHAEL P. LONDREGAN
Director of Security

UNCLASSIFIED

(U) United States Special Operations Command Comments

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNITED STATES SPECIAL OPERATIONS COMMAND
OFFICE OF THE CHIEF OF STAFF
7701 TAMPA POINT BLVD
MACDILL AIR FORCE BASE, FLORIDA 32621-6201

MAY 09 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROGRAM ASSIGNMENTS, DEPARTMENT OF DEFENSE, 4800 MARK CENTER DRIVE, ALEXANDRIA, VA 22350 1500

SUBJECT: (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1-0206.00)

1. (U) REFERENCES:

- a. (U) Department of Defense (DOD) Inspector General Memorandum, Subject: Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command (USSOCOM), MacDill Air Force Base, FL, dated 5 September 2014
- b. (U) DOD Inspector General Memorandum, Subject: Same as above, dated 25 March 2016

2. (U//~~FOUO~~) In Reference b, the DOD Inspector General directed U.S. Special Operations Command (USSOCOM) to provide comments on the findings and recommendations contained in DOD Inspector General Project No. D2014-DINT1-0206.00.

3. (U//~~FOUO~~) Overall, USSOCOM concurs with the report's findings and recommendations, except as noted below. USSOCOM has always strived to achieve full compliance with DOD regulations and policies that govern extended visits by foreign visitors to the headquarters and USSOCOM subordinate commands, and views this assessment as a useful benchmark to make further improvements to the USSOCOM Foreign Officer Program. Based on the recommendations and findings in the report, USSOCOM will:

- a. (U//~~FOUO~~) Ensure international agreements are in full compliance with applicable laws and directives.
- b. (U//~~FOUO~~) Examine the training, preparation, and number of assigned Foreign Disclosure Officers (FDO), and make adjustments based on recommendations made in this report.
- c. (U//~~FOUO~~) Improve and formalize internal controls for the management of foreign visits and assignment of foreign personnel to the headquarters and subordinate commands.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//OFFICIAL USE ONLY~~

SOCS

SUBJECT (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1-0205 00)

4 (U) USSOCOM continues to work with the Under Secretary of Defense for Policy, the Defense Technology Security Administration, the Office of the General Counsel, and within its own staff to ensure full compliance with applicable laws and policies regarding the placement of foreign officers in the USSOCOM enterprise.

5 (U//~~FOUO~~) The report illustrates the complexity of the policy guidance by which the Department governs information sharing and the management of extended visits by foreign officers. This complexity hinders the ability of commanders to execute national and military strategic guidance, which place increasing emphasis on the need to build and work with partner nations. Operating within this complex policy context, three points deserve emphasis:

a. (U//~~FOUO~~) Commander, USSOCOM has the authority to develop an international officer program at Headquarters USSOCOM.

b. (U//~~FOUO~~) USSOCOM utilized Operations and Maintenance funds for the construction of its international coordination center in a manner consistent with its appropriation and authority.

c. (U//~~FOUO~~) At no time did USSOCOM willingly or knowingly disclose or compromise information to any uncleared foreign visitor, liaison officer, or exchange officer beyond the level of disclosure stipulated by National Disclosure Policy - 1.

6 (U) USSOCOM will continue to ensure compliance with the laws, policies, and guidance governing the assignment of foreign officers at U.S. commands. The investment USSOCOM has made in its international officer program has had strategic impacts by increasing our Special Operations Forces (SOF) partners' ability to contribute to security challenges of mutual interest, and we remain committed to continuing this investment in accordance with applicable laws and policies.

7 (U) ~~SOCOM (b)(3) (10 U.S.C. 130b), (b)(6)~~
~~SOCOM (b)(3) (10 U.S.C. 130b), (b)(6)~~

4 Encls
1 Annex A
2 Annex B
3 Annex C
4 Annex D

J. MARCUS HICKS
Major General, U.S. Air Force
Chief of Staff

~~SECRET//NOFORN~~
SOCS
SUBJECT (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014 DINT1-0205 00)

Annex A. (U//~~FOUO~~) Finding A - Foreign Officers Assigned to U.S. Special Operations Command

1. (U//~~FOUO~~) A2a - Ensure all international agreements for the foreign officers assigned to or on extended visits to U.S. Special Operations Command (USSOCOM) and its subordinate commands are in compliance with applicable laws and DOD policies

(U//~~FOUO~~) Comment: Concur. At present, all foreign personnel assigned to HQ USSOCOM and its subordinate commands have either an approved Memorandum of Agreement (MOA), or have an Office of the Secretary of Defense for Policy (OSD(P)) approved exception to policy, pending completion of final negotiation of their specific MOA.

2. (U//~~FOUO~~) A2b - Ensure existing "Annex Bs" contain the level of detail needed to describe the actual mission of the exchange officer and classification consistent with the foreign officer's actual mission requirement

(U//~~FOUO~~) Comment: Concur. All "Annex Bs" (duty descriptions) for exchange officers are being modified to reflect the level of detail consistent with their duties.

3. (U//~~FOUO~~) A2c - Require component commanders to ensure all required annexes, certifications, and designated disclosure letters are in accordance with Circular 175 authority and DOD Directive 5530.03, "International Agreements," dated 18 July 1987

(U//~~FOUO~~) Comment: Concur. The executive agreements for foreign officers assigned to Headquarters USSOCOM, component headquarters, and subordinate subunified command headquarters will be reviewed and maintained in accordance with the applicable directives and policy guidance

4. (U//~~FOUO~~) A2d - Request exceptions to policy for the non-reciprocal and exchange officers who are currently assigned to HQ USSOCOM without concluded international agreements

(U) Comment: Concur. Complete

5. (U//~~FOUO~~) A2e - Seek appropriate authority for the foreign intelligence officers assigned or attached to USSOCOM and its subordinate headquarters

(U//~~FOUO~~) Comment: Non-concur. USSOCOM disputes the finding that it initiated agreements for the exchange of military intelligence with foreign governments before gaining the approval of Defense Intelligence Agency (DIA). USSOCOM has been in compliance with all authorities and policies for intelligence-focused Foreign Liaison Officers (FLOs). For clarification, at no time were intelligence-related FLOs assigned as

~~SECRET//NOFORN~~ //Y

SOCS

SUBJECT: (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1-0206 00)

Exchange Officers, and no representatives from foreign intelligence agencies have ever been assigned to USSOCOM. All foreign officers assigned to USSOCOM are representatives of their respective Ministries of Defense.

6. (U//~~FOUO~~) A2f – Maintain oversight of all foreign SOF assigned to or on extended visit to USSOCOM and its subordinate commands and Service components.

(U//~~FOUO~~) Comment: USSOCOM is in the process of developing and promulgating command policy and guidance regarding oversight of foreign SOF assigned to or on extended visits across the headquarters and USSOCOM's subordinate commands, based on the recommendations of this report. In addition, USSOCOM will monitor the international agreements entered into by its SOF Service component headquarters, even when those agreements are under the provisions of Service-generated policy guidance, and authority.

7. (U//~~FOUO~~) A2g – Eliminate the 'dual use' of foreign officers in accordance with current regulatory guidance.

(U//~~FOUO~~) Comment: Concur. USSOCOM ensures foreign officers are only afforded exchange officer status after the conclusion of an MOA. USSOCOM differentiates between foreign liaison and exchange officers.

8. (U//~~FOUO~~) A2h – Establish a process for reimbursement of costs associated with hosting foreign liaison officers.

(U//~~FOUO~~) Comment: Concur. Complete. USSOCOM computes costs of assigned foreign liaison officers based on the model established by the Joint Staff. Countries are now billed for services annually via the appropriate Acquisition and Cross-Servicing Agreements (ACSA).

~~SECRET//NOFORN~~ //Y

~~SECRET//NOFORN~~ Y
SOCS

SUBJECT: (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1-0206 00)

Annex B (U//FOUO) Finding B – U.S. Special Operations Command did not fully comply with Sensitive Compartmented Information Facilities requirements

1. (U//FOUO) B1a – ~~SECRET//NOFORN~~ SOCOM Section 1.7(e) for 1.4(d) comply with Intelligence Community Directive (ICD) 705, "Sensitive Compartmented Information Facilities (SCIF)," and DOD Manual 5105.21 V2, "Sensitive Compartmented Information (SCI) Administrative Security Manual, October 18, 2012.

(U//FOUO) Comment: Non-concur. USSOCOM disputes the finding that ~~SECRET//NOFORN~~ SOCOM partners were authorized to escort other foreign nationals into SCIFs in which ~~SECRET//NOFORN~~ SOCOM partners had access. USSOCOM Manual 380.6 states, only U.S. cleared personnel are authorized escort of personnel in the SCIF. ~~SECRET//NOFORN~~ SOCOM Section 1.7(e) for SCIF escort privileges.

2. (U//FOUO) B1b – ~~SECRET//NOFORN~~ SOCOM Section 1.7(e) for 1.4(d) Support Center when the meeting sign does not illuminate "RELEASABLE."

(U) Comment: Concur, Complete

3. (U//FOUO) B1c – Establish formal procedures for processing requests for information concerning science and technology information by foreign liaison officers.

(U//FOUO) Comment: Concur, Complete. In July 2014, USSOCOM Regulation 10-4, *Partner Nation Requests for Information/Requests for Support* was published. All partner nation-related requests adhere to the guidance within Reg. 10-4 to ensure accountability and appropriate review, to include those pertaining to science and technology.

~~SECRET//NOFORN~~ Y

~~XXXXXXXXXXXXXXXXXXXX~~
SOCS

SUBJECT: (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1 0206 00)

include those relevant to information sharing, multinational collaboration systems, and foreign disclosure

3. (U//~~FOUO~~) C3 – Determine whether the foreign disclosure office at the Headquarters and subordinate commands under USSOCOM are adequately staffed

(U//~~FOUO~~) Comment. Concur, corrective action is ongoing. In 2015, recognizing the need for unity of effort in foreign disclosure, USSOCOM consolidated staff responsibility for foreign disclosure, technology transfer analysis, intelligence engagement, and foreign visit management under the J2 Intelligence Directorate. See also para. 2, above.

4. (U//~~FOUO~~) C4 – Assess the training requirements for FDO and ensure all special operations forces FDOs receive the necessary training

(U//~~FOUO~~) Comment. Concur, analysis is ongoing.

5. (U//~~FOUO~~) C5 – Assess the requirements for security education and training for personnel who are involved with international exchange programs and foreign government information, or work in coalition or bi-lateral environments, or in offices, activities or organizations hosting foreign exchange officers.

(U//~~FOUO~~) Comment. Concur, corrective action ongoing. The rationale for consolidating international functions into a center, now called the J3-International, was intended to address this requirement. Working with international partners requires additional training and experience in foreign disclosure, international agreements, security assistance, information management, data management, technology protection, physical security, and how to "write for release." USSOCOM is reviewing its portfolio of international training to better inform the headquarters workforce of their role, function, and responsibilities in dealing with and managing foreign liaison and exchange personnel at the headquarters and its subordinate commands.

~~SECRET//NOFORN~~

SOCs

SUBJECT (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1-0206.00)

Annex D: (U//~~FOUO~~) Finding D – U.S. Special Operations Command did not fully comply with automated information systems requirements

1. (U//~~FOUO~~) D1 - Conclude international agreements, with appropriate language, for the French, German, and Spanish non-reciprocal exchange officers, allowing the continued use of their national secure communication systems.

(U//~~FOUO~~) Comment: Concur. Corrective action ongoing. The Spanish Memorandum of Agreement (MOA) is complete. The French and German MOA remain in negotiation as of the writing of this report, and their presence in the headquarters is government by an OSD(P) approved Exception to Policy. All French and German personnel under that Exception to Policy are treated as Liaison Officers until the agreements are concluded. Additionally, partner national classified information systems do not ride on or physically touch any of the USSOCOM networks. Connection is made through a commercial information line to the local service provider. The countries that utilize this capability are billed for that service via the ACSA process described in Annex A, par. 8 above. Additionally, the paragraph citing this problem under Finding D implies that the French and German systems were installed inside a U.S. SCIF, but that is not correct. The French and German systems were installed in the collateral J3-International spaces only after DIA had accredited those spaces.

2. (U//~~FOUO~~) D2 - Obtain automated information systems accreditations for secure facilities that process SCI electronically.

(U//~~FOUO~~) Comment: Non-concur. No partner nation information systems are, or have ever been, installed inside a SCIF at Headquarters, USSOCOM. The entire purpose of building the J3-International as a collateral office space was to ensure USSOCOM continues to meet the requirements of Intelligence Community Directive (ICD) 703 for all SCIFs. For SOCRATES systems, USSOCOM provided the appropriate Authority to Operate (ATO) documentation in accordance with ICD 503 that governs the new Risk Management Framework.² USSOCOM maintains that the provided ATOs acceptably represent automated information system accreditation documents.

² (U) Previously known as Certification & Accreditation for information systems under Defense Community Intelligence Directive 503.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

SOCS

SUBJECT (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1-0206 00)

3. ~~(S//FOUO)~~ D3 – Establish a comprehensive training program to educate all USSOCOM personnel in 'writing for release' to reduce the risk and incidents of misclassifying information and potentially excluding its availability to partner nations.

(U//~~FOUO~~) Comment. Concur, corrective action ongoing. In November 2015, Commander USSOCOM published the following guidance, "We need to view 'writing for release' as a key enabler of our trans-regional efforts. If we view partner collaboration, integration, and de-confliction as critical factors in our ability to counter a growing threat, then we need to quickly adopt habits that allow us to give, and gain, information worthy of our relationships. This will have to play out in our briefings – our audiences, briefers, and assessments will need to become increasingly partner-oriented. Our partners – who we fully involved in deep dives of our previous battle rhythm – need the same access to the new battle rhythm. This is charter not only for HQ USSOCOM staff, but for our components, the TSOCs, our Interagency/Intelligence Community Liaison Officers, and our J3-I partners as well. The whole enterprise needs to embrace this." Action continues in many forms to accomplish the Commander's intent.

4. (U) D4 – Incorporate recommendations from the USSOCOM Cybersecurity Readiness Inspection into guidance to reduce the risk of vulnerable systems.

(U) Comment. Concur. USSOCOM has incorporated the recommendations of the inspection into J3-International policy, training, and guidance.

~~SECRET//NOFORN~~



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
UNITED STATES SPECIAL OPERATIONS COMMAND
OFFICE OF THE CHIEF OF STAFF
7701 TAMPA POINT BLVD
MACDILL AIR FORCE BASE, FLORIDA 32821-5323

JUN 06 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROGRAM ASSIGNMENTS, DEPARTMENT OF DEFENSE, 4800 MARK CENTER DRIVE, ALEXANDRIA, VA 22350-1500

SUBJECT: (U) Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command, MacDill Air Force Base, FL (Project No. D2014-DINT1-0206.00)

1. (U) REFERENCES:

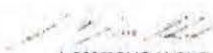
a. (U) Department of Defense (DOD) Inspector General Memorandum, Subject: Evaluation of Foreign Officer Involvement at the U.S. Special Operations Command (USSOCOM), MacDill Air Force Base, FL, dated 5 September 2014.

b. (U) DOD Inspector General Memorandum, Subject: Same as above, dated 25 March 2016.

c. (U) USSOCOM Response to Ref b, dated 9 May 2016.

2. (U//~~FOUO~~) In Reference c, USSOCOM's response inadvertently did not clearly address one of the DOD Inspector General Report's key recommendations, specifically, that USSOCOM "Ensure SOCOM components follow 5320.20 procedures." The discussion of that finding was included in Ref c, par. A2f. In order to ensure clarity, USSOCOM concurs with the recommendation to ensure that its components follow the requirements for extended visits by foreign officers, as described in DOD Regulation 5320.20. USSOCOM continues to improve its foreign officer program based on recommendations in Ref. b.

3. (U) SOCOM (b)(3) 10 U.S.C. 130b, (b)(6)
SOCOM (b)(3) 10 U.S.C. 130b, (b)(6)


J. MARCUS HICKS
Major General, U.S. Air Force
Chief of Staff

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

DODIG-2016-098 / 129

(U) Acronyms and Abbreviations

AFSOC	Air Force Special Operations Command
AFOSI	Air Force Office of Special Investigations
BICES	Battlefield Information Collection and Exploitation System
BND	Bundesnachrichtendienst
CJCS	Chairman of the Joint Chiefs of Staff
CJSOTF-I	Combined Joint Special Operations Task Force – International Security Assistance Force
DDL	Designated Disclosure Letter
DoS	Department of State
DPEP	Defense Personnel Exchange Program
DTSA	Defense Technology Security Agency
DIA	Defense Intelligence Agency
FD	Foreign Disclosure
FDO	Foreign Disclosure Officer
FLO	Foreign Liaison Officer
FVS	Foreign Visits System
FVEY	Five Eye
GCC	Geographic Combatant Command
SOC	[REDACTED]
GSN	Global SOF Network
GSN OPT	Global SOF Network Operation Planning Team
IC	Intelligence Community
ICD	Intelligence Community Directive
ISCC	International SOF Coordination Center
ISIL	Islamic State of Iraq and the Levant

Acronyms and Abbreviations

ISPS	International Security Programs Secretariat
J3-I	J3 International
JSOC	Joint Special Operations Command
JWICS	Joint Worldwide Intelligence Communications System
MARSOC	Marine Corps Special Operations Command
MPEP	Military Personnel Exchange Program
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NAVSPECWARCOM	Naval Special Warfare Command
NDP-1	National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations
NDAA	National Disclosure Authorization Act
NDPC	National Disclosure Policy Committee
NIPRNET	Non-secure Internet Protocol Router Network
NREO	Non-reciprocal Exchange Officer
OUSD(P)	Office of the Undersecretary of Defense for Policy
O&M	Operations and Maintenance
OPT	Operational Planning Team
PMO	Program Management Office
REL	Releasable
RSCC	Regional Special Operations Coordination Center
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SEC	Office of Security
SECDEF	Secretary of Defense
SIPRNET	Secret Internet Protocol Router Network
SOCAF	Special Operations Command – Africa
SOCENT	Special Operations Command – Central
SOCEUR	Special Operations Command – Europe

Acronyms and Abbreviations

SOCKOR	Special Operations Command – Korea
SOCNORTH	Special Operations Command – North
SOC PAC	Special Operations Command – Pacific
SOC SOUTH	Special Operations Command – South
SOF	Special Operations Forces
SORDAC	Special Operations Research, Development, and Acquisition Center
SSO	Special Security Officer
TSCM	Technical Surveillance Countermeasures
TSOC	Theater Special Operations Command
USAFRICOM	United States Africa Command
USAFSOC	United States Air Force Special Operations Command
USASOC	United States Army Special Operations Command
USCENTCOM	United States Central Command
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USSOCOM	United States Special Operations 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

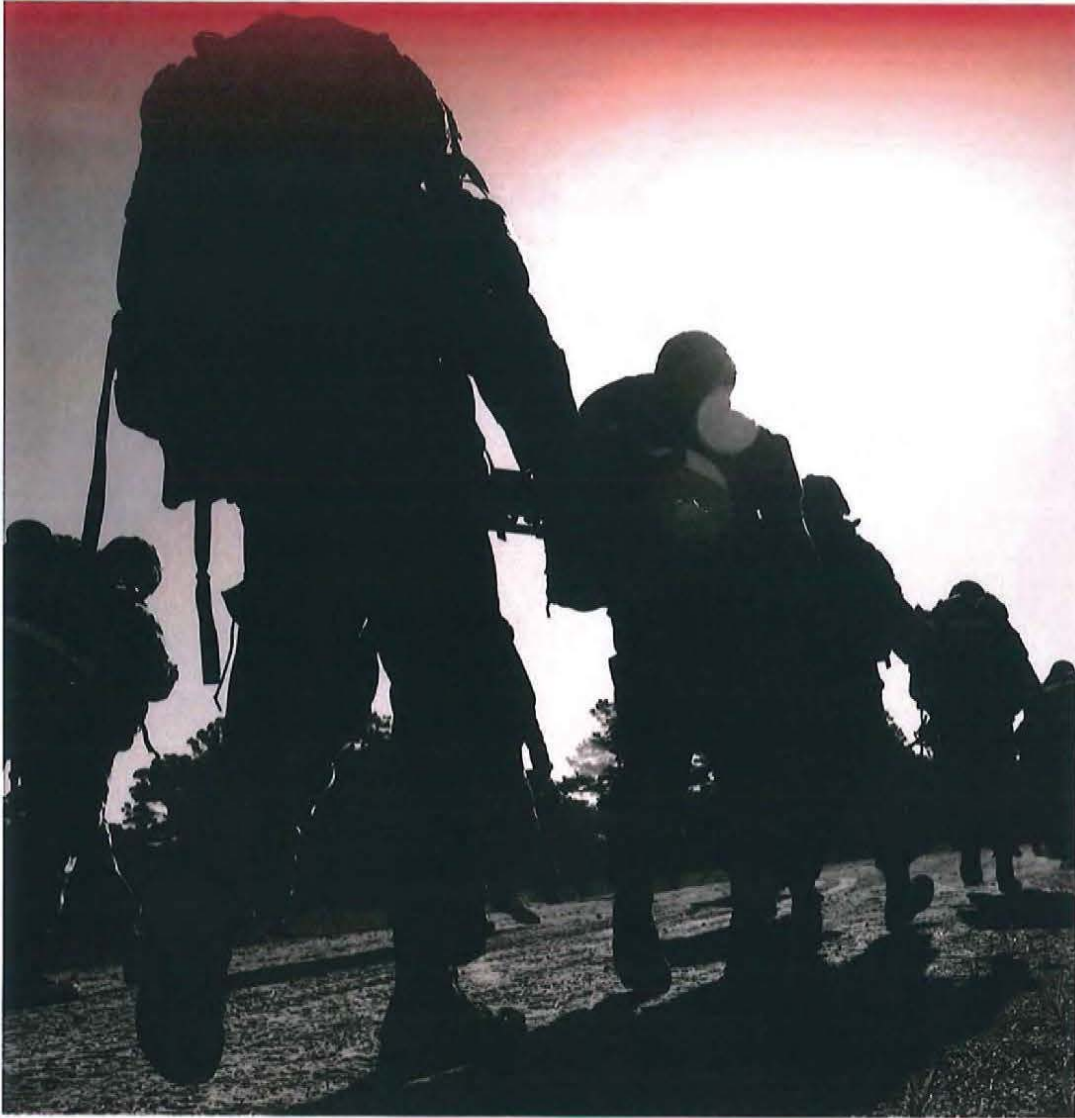
Twitter

twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline

SECRET//NOFORN//SOCOM Section 1.7(e) for 1.4(a)



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

SECRET//NOFORN//SOCOM Section 1.7(e) for 1.4(a)