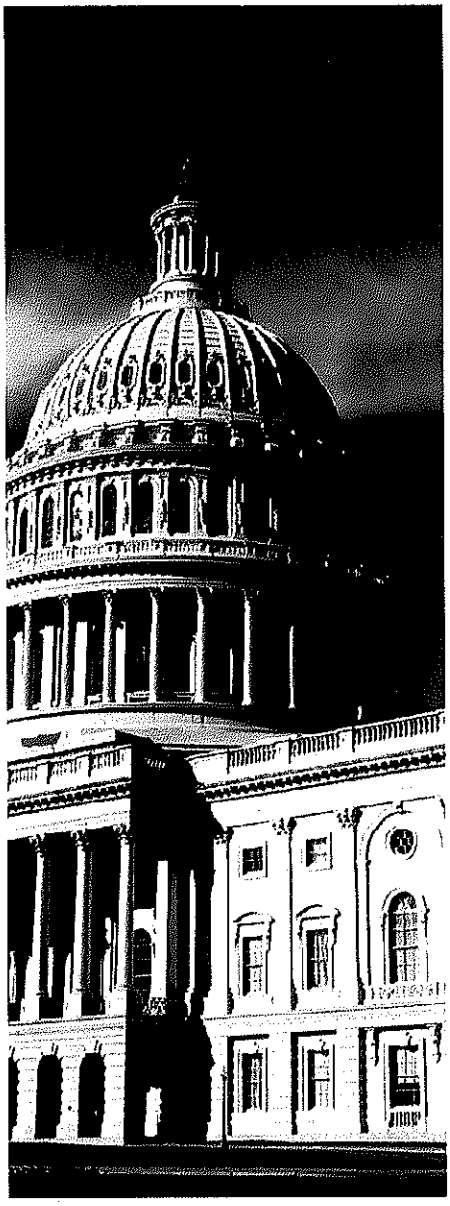
Report No. DODIG-2014-086

SECRET

INSPECTOR GENERAL

U.S. Department of Defense

June 25, 2014



(U) U.S. Central Command Vulnerability Management Program Needs Improvement

Classified By: (b)(6)
Derived From: Multiple Sources
Declassify On: 20390625

Copy 16 of 22

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

SECRET

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

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

Vision

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

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

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

(U) Results in Brief

(U) U.S. Central Command Vulnerability Management Program Needs Improvement

June 25, 2014

(U) Objective

(U) Our objective was to determine whether the U.S. Central Command's (USCENTCOM) vulnerability management program (VMP) effectively identified, remediated, and mitigated network vulnerabilities.

(U) Finding

~~(S)~~ Although USCENTCOM effectively identified network vulnerabilities, it was not consistently effective in remediating and mitigating those vulnerabilities. Specifically, USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g)

- ~~(S)~~ USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec. 1.4(g)
- ~~(S)~~ USCENTCOM - (b)(1), Sec 1.4(Sec 1.4(Sec 1.4(g)

(U) This occurred because USCENTCOM system managers did not monitor resolution actions taken to mitigate and remediate the network vulnerabilities as required by USCENTCOM policy.

(U) (Finding cont'd)

~~(S)~~ In addition, USCENTCOM technicians did not properly maintain a record of actions taken to mitigate and remediate USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) This occurred because, for USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g)

(U//~~FOUO~~) Furthermore, USCENTCOM technicians did not consistently include required information on (b) (7)(E) This occurred because system managers were not required to (b) (7)(E)

(U) As a result, USCENTCOM's VMP is unable to function optimally and there is an increased risk (b) (7)(E) In addition, insufficient details on resolution actions and incomplete (b) (7)(E)

(U) Recommendations

(U) We recommend that the Chief, U.S. Central Command, Systems Division monitor resolution actions to ensure vulnerabilities are resolved in a timely manner and conduct periodic reviews of resolution action documentation to ensure technicians properly document resolution actions. In addition, we recommend the Chief configure Remedy to properly capture and retain resolution activities and conduct periodic reviews to ensure technicians prepare change requests as required by internal policy.

(U) Results in Brief

(U) U.S. Central Command Vulnerability Management Program Needs Improvement

(U) Management Comments

(U) The Chief, U.S. Central Command, Cyber Security Division, provided comments that disagreed with elements of the finding, but did not address the specific report recommendations. Therefore, we request that the Chief, Systems Division, provide comments on the final report by July 25, 2014. Please see the recommendations table on the next page.

(U) Recommendations Table

Management	Recommendations Requiring Comment
(U) Chief, U.S. Central Command, Systems Division	1, 2, 3, and 4

* Please provide comments by July 25, 2014.

~~SECRET~~

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

June 25, 2014

MEMORANDUM FOR COMMANDER U.S. CENTRAL COMMAND

SUBJECT: (U) U.S. Central Command Vulnerability Management Program Needs Improvement (Report No. DODIG-2014-086)

~~(S)~~ We are providing this report for review and comment. Although USCENTCOM's vulnerability management program effectively identified network vulnerabilities, it was not consistently effective in remediating and mitigating those vulnerabilities.

(U) We considered management comments on a draft version of this report when preparing the final report. DoD Directive 7650.3 requires that all recommendations be resolved promptly. Comments from the Chief, U.S. Central Command, Cyber Security Division, did not address the specifics of the recommendations. Therefore, we request comments from the Chief, U.S. Central Command, Systems Division, on the recommendations by July 25, 2014.

(U) Please provide comments that conform to the requirements of DoD Directive 7650.3. Please send a PDF file containing your comments to (b)(6) [redacted]@dodig.smil.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

(U) We appreciate the courtesies extended to the staff. Please direct questions to (703) 699(b)(6) [redacted] (DSN 499(b)(6) [redacted].

(b)(6) [redacted]
Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

(U) Introduction

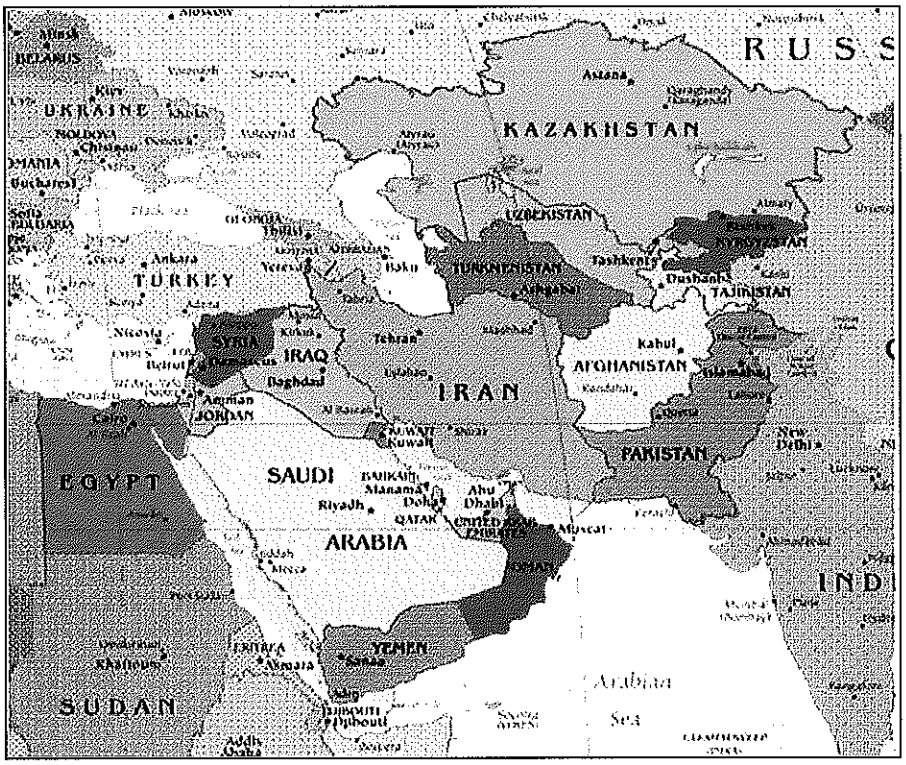
(U) Objective

(U) Our objective was to determine whether the U.S. Central Command's (USCENTCOM) vulnerability management program (VMP) effectively identified, remediated,[1] and mitigated[2] network vulnerabilities. We limited our review to USCENTCOM headquarters in Tampa, Florida. See Appendix for a discussion of our scope and methodology and prior coverage.

(U)Background

(U) USCENTCOM is one of nine combatant commands that promote cooperation among nations, respond to crises, and deter or defeat aggression. USCENTCOM's area of responsibility includes 20 countries.

(U) USCENTCOM's Area of Responsibility



(U) Source: U.S. Central Command, March 2009

[1] (U) Remediate: the act of correcting a vulnerability or eliminating a threat.

[2] (U) Mitigate: to implement compensating controls to remove a risk without correcting the vulnerability.

(U) With the increasing number of cyber threats, the successful execution of vulnerability management, from discovery to prompt remediation, is necessary to protect an entity's operations. For USCENTCOM, vulnerability management is crucial in safeguarding the warfighter and USCENTCOM efforts in countries such as Afghanistan, Iraq, and Yemen.

(U) The USCENTCOM Command, Control, Communications, and Computers Division (CCJ6) is responsible for information assurance, network, and cyber-security functions. (b)(7)(E) [redacted]

- (U) (b)(7)(E) [redacted]
- (U) (b)(7)(E) [redacted]
- (U) (b)(7)(E) [redacted]

(U) (b)(7)(E) [redacted]

(U) Vulnerability Management Program Requirements

(U) The National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, requires that agencies use vulnerability scanning tools to scan their information systems for vulnerabilities at a frequency determined by the agency. The publication also requires that agencies analyze vulnerability scan reports and results, and remediate legitimate vulnerabilities.

(U) DoD Instruction (DoDI) 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, states that IA programs must provide the capability to systematically identify and assess vulnerabilities and to direct and track coordinated mitigations. In addition, DoDI 8500.2 states that the vulnerability management process should enable agencies to independently validate mitigation activities through inspections or automated vulnerability assessment tools. DoDI 8500.2 also requires the development of vulnerability management procedures and the performance of regular internal and external assessments.

(U) Combatant Command Network Responsibility

(U) According to Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," February 9, 2011, Combatant Commanders are responsible for ensuring compliance with U.S. Cyber Command (USCYBERCOM) warnings and tactical directives or orders to protect and defend DoD information networks. In addition, Combatant Commanders are responsible for taking actions to mitigate vulnerabilities. Combatant Commanders should also assess the risk and potential operational impact associated with hardware and software vulnerabilities.

(U) USCENTCOM Requirements for Vulnerability Remediation

(U) USCENTCOM requires system managers to remediate vulnerabilities within (b)(7)(E) of identification. The "Information Assurance Vulnerability Management and Non-Information Assurance Vulnerability Management Remediation Procedure," DCN 1258, Version 1.1, August 20, 2013, provides the overall procedures for USCENTCOM vulnerability remediation. Table 1 provides a breakdown of the daily activities that should be taken after USCENTCOM (b)(7)(E) [redacted]

Table 1. (U) (b)(7)(E) *Process for Resolving Vulnerabilities*

(b)(7)(E)

(U) Source: Information Assurance Vulnerability Management and Non-Information Assurance Vulnerability Management Remediation Procedure, DCN 1258 Version 1.1, August 20, 2013

(U) USCENTCOM also implemented C4 Systems Division, DCN 1070, Version 2.1, "Authorized Service Interruption and Maintenance Action Process Overview," August 9, 2013 (DCN 1070), (b)(7)(E) According to DCN 1070, this ensures that USCENTCOM efficiently and effectively controls, coordinates, and manages changes. USCENTCOM's policy also requires change managers to track all resolution actions throughout the lifecycle of the change.

(U) Applications Used to Manage USCENTCOM Vulnerabilities

(U) USCENTCOM used Retina, Microsoft System Center Configuration Manager (SCCM), and BMC Remedy Change Management System (Remedy) to identify vulnerabilities, patch system weaknesses, and manage network changes.

(U) Retina

(U) Retina is a vulnerability scanner used to identify vulnerabilities, such as missing patches and configuration weaknesses. The weaknesses identified by Retina allow organizations to implement controls to mitigate or remediate the vulnerabilities, to protect assets and information. It is a widely used scanning tool in DoD.

(U) Microsoft System Center Configuration Manager

(U) SCCM is a system management software that allows organizations to deploy secure and scalable patches automatically, manage compliance settings, and manage assets.

(U) BMC Remedy Change Management System

(U) Remedy provides a system for planning, scheduling, implementing, and tracking changes made to the network, which includes changes made to mitigate and remediate known vulnerabilities. It includes functions for:

- (U) requesting changes,
- (U) obtaining approval for changes,
- (U) analyzing risks associated with implementing changes,
- (U) coordinating tasks related to changes, and
- (U) recording changes made to the networks.

(U) Review of Internal Controls

(U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses related to USCENTCOM's ability to (b) (7)(E) [redacted] In addition, USCENTCOM system managers did not properly (b) (7)(E) [redacted] We will provide a copy of this report to the senior officials responsible for internal controls in USCENTCOM.

(U) Finding

(U) Inconsistent Vulnerability Management Program at USCENTCOM

~~(S)~~ Although USCENTCOM effectively identified network vulnerabilities, it was not consistently effective in remediating and mitigating those vulnerabilities. Specifically, USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) [redacted]

- ~~(S)~~ USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) [redacted]
- ~~(S)~~ USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) [redacted]

(U) This occurred because USCENTCOM system managers did not monitor resolution actions taken to mitigate and remediate the network vulnerabilities as required by USCENTCOM policy.

~~(S)~~ In addition, USCENTCOM technicians did not properly maintain a record of actions taken to mitigate and remediate USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) [redacted] This occurred because, USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) [redacted]

(U//~~FOUO~~) Furthermore, USCENTCOM technicians did not consistently include required information on (b) (7)(E) [redacted] This occurred because (b) (7)(E) [redacted]

(U) As a result, USCENTCOM's VMP is unable to function optimally, and there is an increased risk (b) (7)(E) [redacted] In addition, insufficient details on resolution actions and incomplete (b) (7)(E) [redacted]

(U) USCENTCOM Effectively Identified Vulnerabilities

~~(S)~~ USCENTCOM effectively identified vulnerabilities on USCENTCOM - (b)(1): Sec. 1.4(a), Sec. [redacted]

- USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

~~(S)~~ After identifying the vulnerabilities, the security analysts USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(U) USCENTCOM Lacked Consistency in Remediating and Mitigating Vulnerabilities

~~(S)~~ Although USCENTCOM's VMP was effective in identifying vulnerabilities, it was not consistently effective in remediating and mitigating those vulnerabilities. USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

- ~~(S)~~ USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)
- ~~(S)~~ USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

[3] (U) An asset is a major application, general support system, high-impact program, physical plant, mission-critical system, person, piece of equipment, or a logically related group of systems.

(U) The National Institute of Standards and Technology Special Publication 800-53, requires that agencies analyze vulnerability scan results and remediate legitimate vulnerabilities.

(U) Vulnerabilities Not Resolved in a Timely Manner

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(U) Lack of Assurance Automated Patches Remediated Vulnerabilities

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(U) Mitigation and Remediation Actions Not Monitored

(U//FOUO) USCENTCOM system managers did not monitor resolution actions taken to mitigate and remediate the network vulnerabilities as required by USCENTCOM policy. (b)(7)(E)

4 (S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

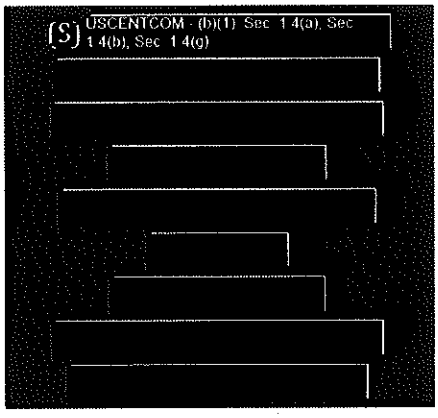
(U//FOUO) (b)(7)(E) [redacted]

(U) Mitigation and Remediation Actions Not Properly Documented

(U) USCENTCOM technicians did not properly document actions taken to mitigate and remediate network vulnerabilities. (b)(7)(E) [redacted] According to DoDI 8500.2, agencies should track mitigation actions. In addition, USCENTCOM DCN 1070 requires change managers to track all resolution actions throughout the lifecycle of the change. The USCENTCOM vulnerability manager stated details of resolution actions were supposed to be documented and maintained in Remedy. (b)(7)(E) [redacted]

~~(S)~~ USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) [redacted]

(S) USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g)



[redacted]

(S) USCENTCOM - (b)(1); Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g) [redacted]

(U) Technicians Did Not Always Follow USCENTCOM Policy for Preparing Change Requests

(U//FOUO) USCENTCOM technicians did not always include required information in change requests initiated to track remediation and mitigation actions for resolving vulnerabilities. Specifically, (b)(7)(E) [redacted]

- (U) (b)(7)(E) [redacted]
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)

(U) USCENTCOM implemented this policy in an effort to standardize the process for network changes. The intent was to allow managers, division leads, and technicians to properly execute the change process and would ensure efficient and effective control, coordination, and management of changes to the network.

(U) This occurred because system managers did not conduct reviews of the change requests to ensure they included the required information. System managers should conduct a review of change requests to ensure technicians prepared documents as required by internal policy.

(U) Increased Risk of Persistent Cyber Attacks

(U) As a result, USCENTCOM's VMP is unable to function optimally. In addition, there is an increased risk of (b)(7)(E) [redacted]

(U) USCENTCOM Acknowledged VMP Improvements are Needed

(U) The ISSM at USCENTCOM agreed that the processes between vulnerability identification and vulnerability resolution needed improvement. The first step was to (b)(7)(E) [redacted]

ISSM also agreed that USCENTCOM needed to improve the process for (b)(7)(E) [redacted]

(U) Management Comments on the Finding and Our Response

(U) Management Comments on Inconsistent Vulnerability Management Program at USCENTCOM

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g) [redacted]

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(U) Our Response

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

(U) Recommendations, Management Comments, and Our Response

(U) We recommend that the Chief, U.S. Central Command, Systems Division:

1. (U) Monitor resolution actions taken to mitigate and remediate the network vulnerabilities to ensure vulnerabilities are resolved in a timely manner.

2. (U) Conduct periodic reviews of resolution action documentation to ensure technicians properly document resolution actions.

3. (U) (b)(7)(E) [redacted]

4. (U) Conduct periodic reviews to ensure technicians properly document resolution actions and prepare change requests as required by internal policy.

(U) Management Comments Required

(U) The Chief, U.S. Central Command, Cyber Security Division, did not address the specific report recommendations. We request that the Chief, U.S. Central Command, System Division, provide comments on the final report by July 25, 2014.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this performance audit from June 2013 through April 2014, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We interviewed IA personnel at USCENTCOM headquarters responsible for vulnerability identification, remediation and mitigation, and change management. We also interviewed the USCYBERCOM Information Assurance Vulnerability Management Program Chief, to identify USCYBERCOM's role in the combatant commands VMP. In addition, we reviewed Federal and DoD and USCENTCOM guidance governing VMP. Specifically, we reviewed:

- (U) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003;
- (U) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011;
- (U) USCENTCOM C4IES, Compliance Management (CMT), "Information Assurance Vulnerability Alert Process," DCN 1375, Version 3.0, May 23, 2013;
- (U) USCENTCOM C4 Systems Division, DCN 1070, Version 2.1, "Authorized Service Interruption and Maintenance Action Process Overview," August 9, 2013; and
- (U) USCENTCOM C4 Systems Division, DCN 1258, Version 1.1, "IAVM and Non-IAVM Remediation Procedure," August 20, 2013.

(U) We observed the process for configuring Retina to perform vulnerability scans. We interviewed IA personnel responsible for the remediation and mitigation of vulnerabilities and change management. In addition, we reviewed USCENTCOM's internal process for remediating vulnerabilities and performing changes to its networks. We also examined the documentation USCENTCOM provided to determine whether it followed the process described by USCENTCOM.

(U) (b)(7)(E)

(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)

Table A. (U) Testing Universe and Sample Size per Asset Group

(U) Network	(U) Asset Group	(U) Universe	(U) Sample
(S) USCENTC	(S) USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g)		
	(S)		
	(S)		
	(S)		
	(S)		
	(S)		
(S) USCENT	(S)		
	(S)		
	(S)		
	(S)		
	(S)		
	(S)		
	(S)		

[5] (U) Critical Asset Groups - IT servers and hardware that USCENTCOM identified as critical to operations.

(U) Network	(U) Asset Group	(U) Universe	(U) Sample
(S) USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g)			
(S) USCENT COM (b) (cont'd)	(S) US CE		
	(S)		
	(S)		
	(S)		
	(S)		
	(S)		
	(S) USC ENT		
	(S)		
	(S) US CE		
(U) Total			

(S) Subsequently, we requested a December 18, 2013, USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) to determine USCENTCOM - (b)(1) Sec 1.4(a) Sec 1.4(b), Sec 1.4(g)

(S) From the samples described in Table A, we asked USCENTCOM to provide documentation that supported the resolution actions performed to remediate or mitigate the vulnerabilities. USCENTCOM provided USCENTCOM - (b)(1) Sec 1.4(a), Sec 1.4(b), Sec 1.4(g) We reviewed and analyzed the documentation to determine whether USCENTCOM established a VMP that effectively identified, remediated, and mitigated USCENTCOM - (b)(1) Sec 1.4(a) Sec 1.4(b), Sec 1.4(g).

(U) Use of Computer-Processed Data

(U) We used computer-processed data for our audit from (b) (7)(E) (b) (7)(E) verified that USCENTCOM used the most recent (b) (7)(E) As a result, we concluded that the data (b) (7)(E) were sufficiently reliable for the purpose of our review.

(U) (b)(7)(E) [redacted]

(U) Specifically, we identified significant errors and incomplete elements of key data, such as the omission of start dates and end dates, test plans, and implementation actions. Therefore, we concluded that the data included on (b)(7)(E) [redacted] were not reliable for purposes of our review.

(U) Use of Technical Assistance

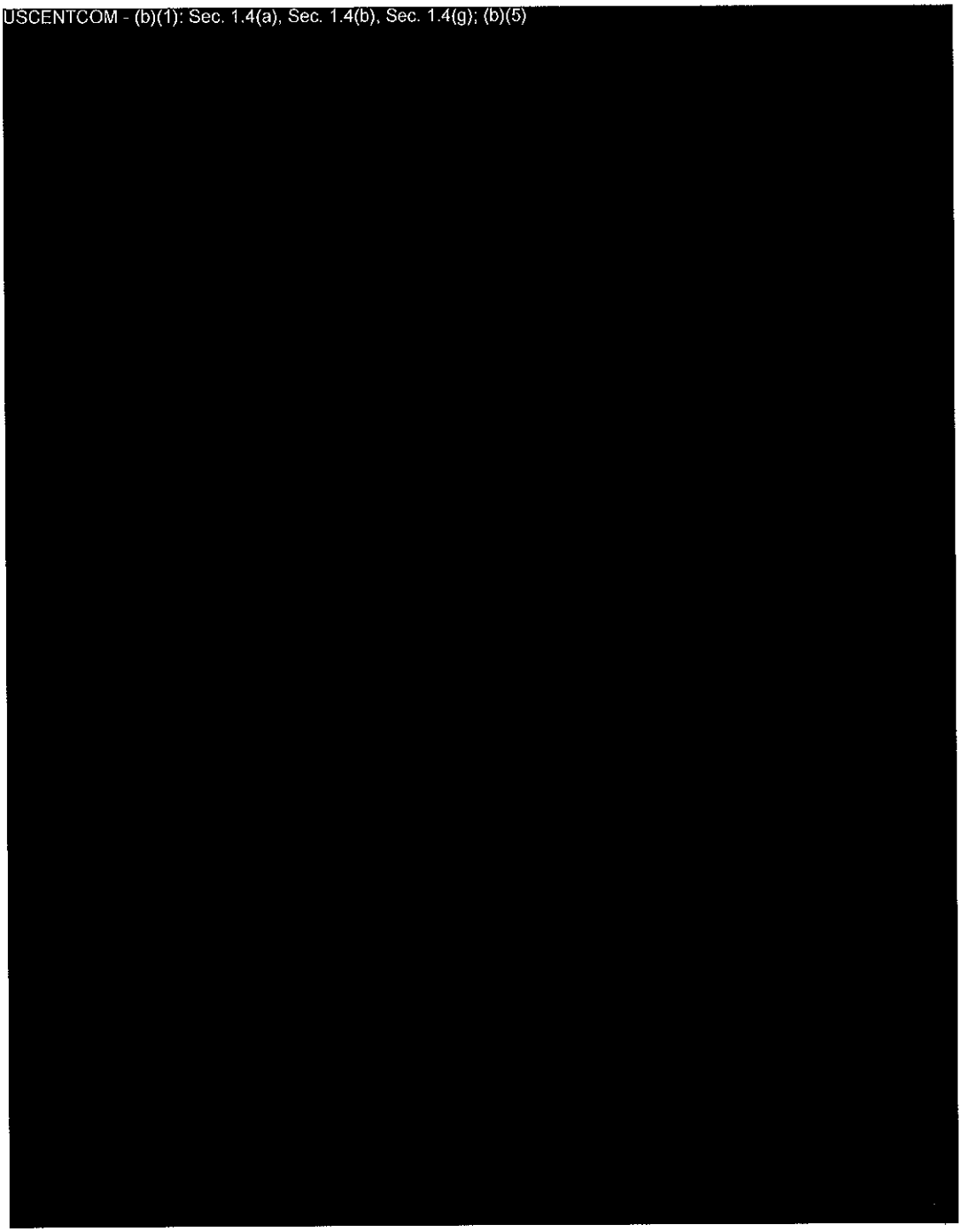
(U) QMD and the Information Systems Directorate assisted the audit team during the audit. QMD assisted with the statistical sampling methodology for selecting vulnerabilities to test the effectiveness of USCENTCOM's VMP. The Information Systems Directorate provided technical assistance to assist the audit team in gaining an understanding of the key areas and processes of a VMP and the data required to assess the effectiveness USCENTCOM's VMP.

(U) Prior Coverage

(U) No prior coverage has been conducted on assessing vulnerability management programs at USCENTCOM during the last 5 years.

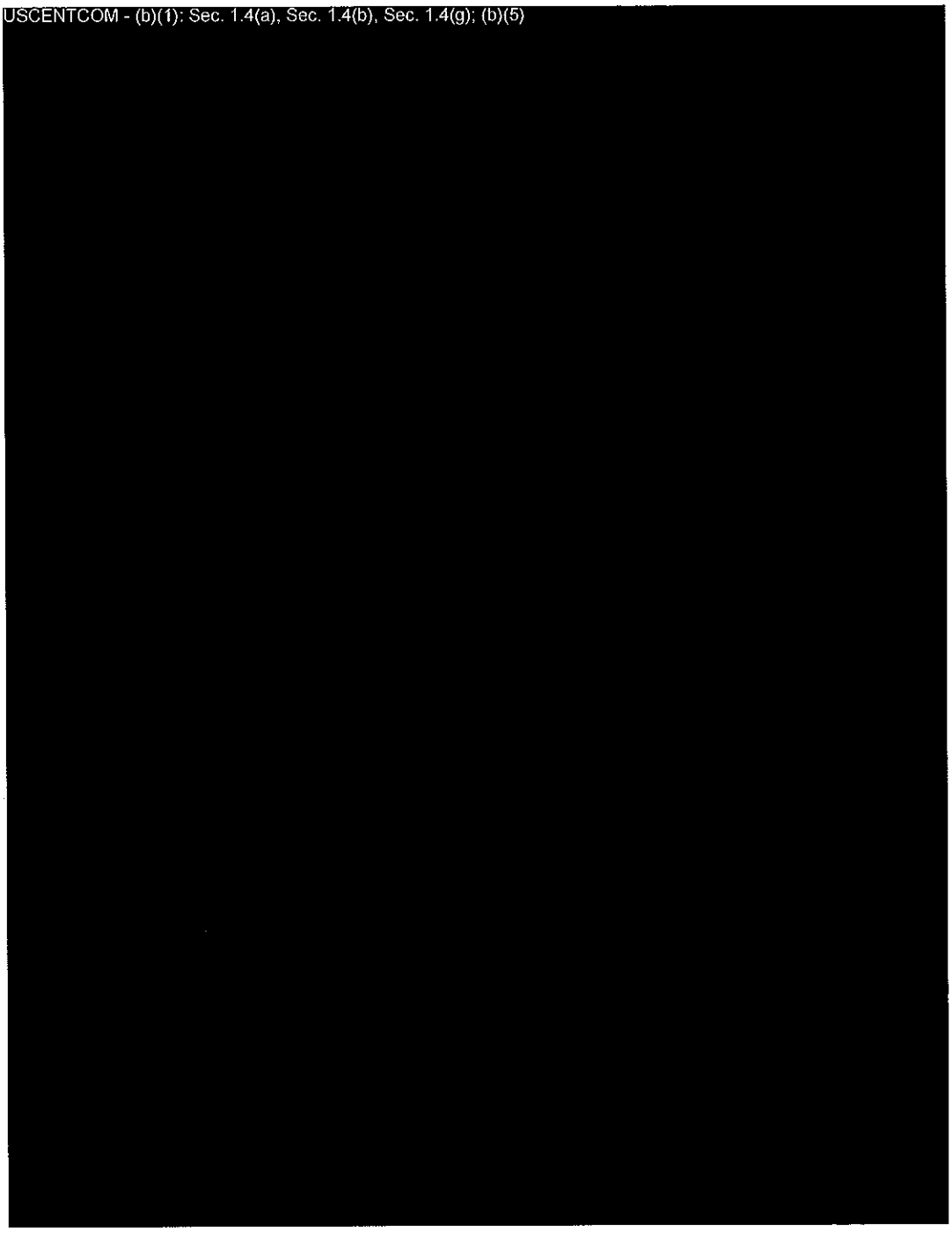
(U) Management Comments

(U) U.S. Central Command

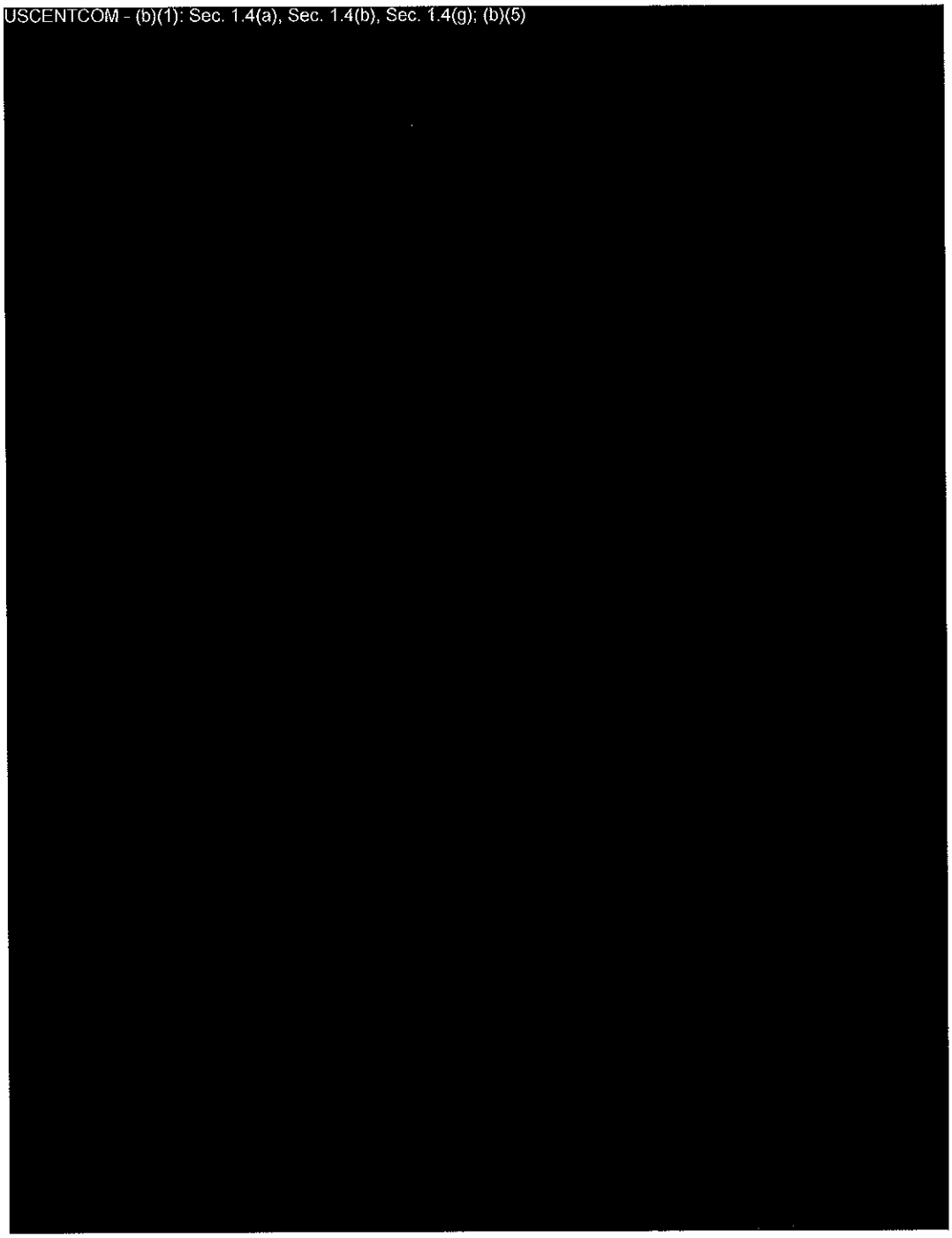


(U) U.S. Central Command (cont'd)

USCENTCOM - (b)(1): Sec. 1.4(a), Sec. 1.4(b), Sec. 1.4(g); (b)(5)



(U) U.S. Central Command (cont'd)



(U) Source of Classified Information

Source 1: (U)Retina Scan Results from August 3, 2013
Declassify on: 20230823
Date of Source: August 3, 2013

Source 2: (U)Retina Scan Results from August 19, 2013
Declassify on: 20230919
Date of Source: August 19, 2013

Source 3: (U)Retina Scan Results from December 31, 2013
Declassify on: 20231231
Date of Source: December 31, 2013

Source 4: (U)Microsoft Windows User Rights Finding Spreadsheet Associated with Problem Investigation 3829
Declassify on: 20230909
Date of Source: September 09, 2013

Source 5: (U)Microsoft Windows User Rights Finding Spreadsheet Associated with Problem Investigation 3833
Declassify on: 20230909
Date of Source: September 10, 2013

Source 6: (U)Unquoted Service Patch Internet Protocol Addresses associated with Problem Investigation 3760
Declassify on: 20230823
Date of Source: August 26, 2013

Source 7: (U)Audit of USCENTCOM VMP Follow-Up Questions – USCENTCOM's Response
Declassify on: 20231114
Date of Source: November 14, 2013

Source 8: (U)Problem Investigation (PBI) Remedy Ticket 2095
Classified By: (b)(6) [redacted]
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 9: (U)Problem Investigation (PBI) Remedy Ticket 3829
Classified By: (b)(6) [redacted]
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 10: (U)Problem Investigation (PBI) Remedy Ticket 3833
Classified By: (b)(6) [redacted]
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 11: (U)Problem Investigation (PBI) Remedy Ticket 3835
Classified By: (b)(6) [redacted]
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 12: (U)Problem Investigation (PBI) Remedy Ticket 3834
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 13: (U)Problem Investigation (PBI) Remedy Ticket 3837
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 14: (U)Problem Investigation (PBI) Remedy Ticket 3760
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 15: (U)Problem Investigation (PBI) Work Info History Printouts 2095
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 16: (U)Problem Investigation (PBI) Work Info History Printouts 3829
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 17: (U)Problem Investigation (PBI) Work Info History Printouts 3833
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 18: (U)Problem Investigation (PBI) Work Info History Printouts 3834
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

Source 19: (U)Problem Investigation (PBI) Work Info History Printouts 3760
Classified By: (b)(6)
Derived From: USCENTCOM Security Classification Guide, CCR 380-14, date published 15 March 14
Declassify on: 20231113

(U) Acronyms and Abbreviations

CAT	Category
CCJ6	Command, and Control, Communications and Computers Division
DoDI	Department of Defense Instruction
IA	Information Assurance
IT	Information Technology
ISSM	Information System Security Manager
NIPRNET	Non-Classified Internet Protocol Router Network
SCCM	System Center Configuration Manager
SIPRNET	Secret Internet Protocol Router Network
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
VMP	Vulnerability Management Program

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