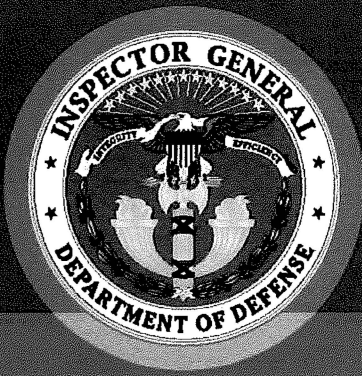


SECRET



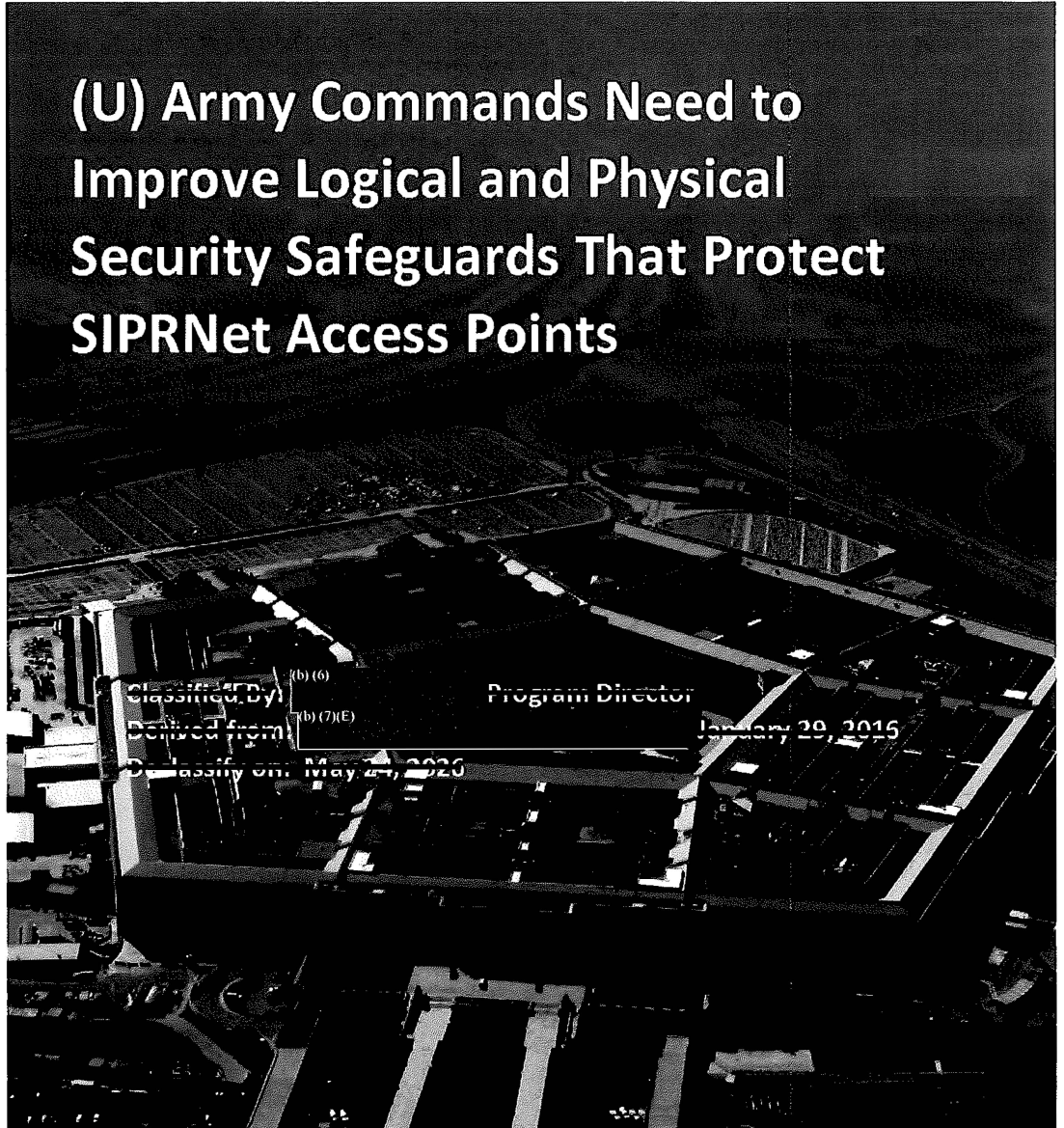
INSPECTOR GENERAL

U.S. Department of Defense

AUGUST 5, 2016



(U) Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points



Classified By: (b) (6)
Derived from: (b) (7)(E)

Program Director

January 29, 2015

Declassify on: May 24, 2020

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Copy 49 of 60

SECRET

~~SECRET~~

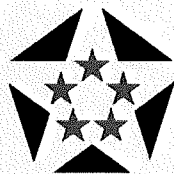
INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

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

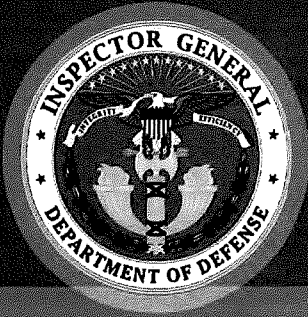
Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline 800-424-9988

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

~~SECRET~~



(U) Results in Brief

(U) Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points

(U) August 5, 2016

(U) Objective

(U) We determined whether the Army effectively protected SECRET Internet Protocol Router Network (SIPRNet) access points.¹ Specifically, we reviewed the security safeguards protecting the SIPRNet access points at (b) (7)(E)

[REDACTED]

(U) Findings

(S) Army commands (b) (1), EO 13526, sec. 1.4(g) . Specifically, among other findings, the Army (b) (1), EO 13526, sec. 1.4(g)

[REDACTED]

Additionally, the (b) (1), EO 13526, sec. 1.4(g)

(U) ¹ SIPRNet access points are all possible physical or logical connections where a user can access the network.

Visit us at www.dodig.mil

(U) Findings (cont'd)

(S) (b) (1), EO 13526, sec. 1.4(g)

[REDACTED]

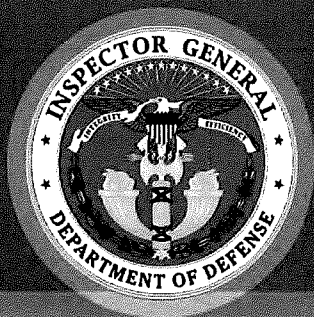
Furthermore, Army commands (b) (1), EO 13526, sec. 1.4(g) properly complete access request forms, or ensure security-related training was taken because the commands did not implement effective processes and procedures. (b) (1), EO 13526, sec. 1.4(g)

[REDACTED]

(FOUO) (b) (7)(E)

[REDACTED]

(U) ² Logical security refers to system-based mechanisms (such as firewalls, permission settings, and usernames and passwords) that designate who or what has access to a specific system or function.



(U) Results in Brief

(U) Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points

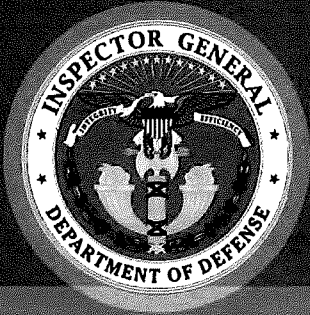
(U) Recommendations

(U) Among other recommendations, we recommend the:

- (FOUO) Army Chief Information Officer and Commander, Army Cyber Command and Second Army, review and correct the deficiencies included in this report at other Army commands;
- (FOUO) Army Chief Information Officer, in coordination with the Commander, Army Cyber Command and Second Army, establish and implement procedures to (b) (7)(E);
- (FOUO) Commander, 7th Signal Command (Theater), review whether subordinate commands implemented (b) (7)(E);
- (FOUO) (b) (7)(E);

(U) Recommendations (cont'd)

- (FOUO) (b) (7)(E) develop and implement processes to (b) (7)(E);
- (FOUO) (b) (7)(E) verify access request forms are properly completed;
- (FOUO) (b) (7)(E) ensure required security-related training is taken;
- (S) (b) (1), EO 13526, sec. 1.4(g);
- (FOUO) Division Chief, Army Spectrum Management Office, (b) (7)(E);



(U) Results in Brief

(U) Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points

(U) Recommendations (cont'd)

(FOUO) (b) (7)(E)
[Redacted]
[Redacted]

(U) Management Comments and Our Response

(U) Based on management comments, we added the Commander, Army Cyber Command and Second Army, to eight recommendations; the Commander, 7th Signal Command (Theater), to three recommendations; and the Division Chief, Army Spectrum Management Office, to two recommendations. We also removed the Commander, 7th Signal Command, from one recommendation and the Commander, U.S. Army Electronic Proving Ground from two recommendations.

(U) The Army Chief Information Officer;

(b) (7)(E)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

addressed all specifics of the

(U) Management Comments and Our Response (cont'd)

(U) recommendations and, therefore, no further comments are required. Comments from the Commander, 7th Signal Command (Theater), did not address the recommendation to ensure required training is taken before SIPRNet access and to maintain training records. (b) (7)(E)

[Redacted], responding for the Program Director, (b) (7)(E) did not address the recommendation to develop and implement processes to (b) (7)(E). We request that the Commander and the Program Director provide additional comments on the final report.

(U) The Commander, Network Enterprise and Technology Command;

(b) (7)(E)
[Redacted]
[Redacted]
[Redacted]
[Redacted]

[Redacted] did not provide comments on a draft of this report. We request that the Commander, Directors, and Staff Judge Advocate provide comments on the final report.

(U) The Commander, Army Cyber Command and Second Army; and the Deputy Commanding General, Installation Management Command, provided unsolicited comments that addressed the specifics of the recommendations. The Division Chief, Army Spectrum Management Office, also provided unsolicited comments, but the comments did not address the recommendation to (b) (7)(E)

[Redacted]. We request that the Division Chief, Army Spectrum Management Office, provide additional comments on this recommendations. Please see the Recommendations Table on the next page.

SECRET

(U) Recommendations Table

(U)	Management	Recommendations Requiring Comment	No Additional Comments Required
	Commander, Network Enterprise Technology Command	A.3.a, A.3.b	
	Commander, 7th Signal Command (Theater)	A.3.a, A.3.b	A.4
(b) (7)(E)		A.8.a	A.8.b, A.8.c
		B.3.a, B.3.b, B.4.a, B.4.b, B.4.c	
			A.5.a, A.5.b, B.1.a, B.1.b
		B.7	
	Army Chief Information Officer		A.1, A.2.a, A.2.b
(b) (7)(E)		A.6	
		B.6	
		A.3.a, A.3.b, A.7.a, A.7.b, A.7.c, A.7.d, B.3.a, B.3.b	
			B.2
		B.7	
			A.3.a, A.3.b, A.9.a, A.9.b, A.9.c, A.9.d, A.9.e, B.2
		A.3.a, A.3.b, A.10, B.4.a, B.4.b, B.4.c, B.5.a, B.5.b, B.6	
			A.5.a, A.5.b, A.11, B.1.a, B.1.b
		A.3.a, A.3.b, A.12.a, A.12.b, A.12.c, B.7	
	Commander, Army Cyber Command and Second Army		A.2.a, A.2.b, A.3.a, A.3.b, A.7.a, A.7.b, A.7.c, and A.7.d
	Division Chief, Army Spectrum Management Office	B.5.b	B.5.a

(U)

(U) Please provide Management Comments by September 6, 2016.



~~SECRET~~

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

August 5, 2016

MEMORANDUM FOR AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: (U) Army Commands Need to Improve Logical and Physical Security Safeguards
That Protect SIPRNet Access Points (Report No. DODIG-2016-119)

(S) We are providing this report for review and comment. The Army commands (b) (1), EO 13526, sec. 1.4(g) [redacted], complete required training and access request forms, (b) (1), EO 13526, sec. 1.4(g) [redacted]. In addition, the Army commands (b) (1), EO 13526, sec. 1.4(g) [redacted]. We conducted this audit in accordance with generally accepted government auditing standards.

(U) We considered management comments on a draft of this report when preparing the final report. Based on management comments, we added the Commander, Army Cyber Command and Second Army, to Recommendations A.2.a, A.2.b, A.3.a, A.3.b, A.7.a, A.7.b, A.7.c, and A.7.d; the Commander, 7th Signal Command (Theater) to Recommendations A.3.a, A.3.b, and A.4; and the Division Chief, Army Spectrum Management Office, to Recommendations B.5.a and B.5.b. We also removed the Commander, 7th Signal Command, from Recommendation A.2.a and the Commander, U.S. Army Electronic Proving Ground, from Recommendations B.5.a and B.5.b. DoD Directive 7650.03 requires that recommendations be resolved promptly.

(U) The Army Chief Information Officer; (b) (7)(E) [redacted]
[redacted]
[redacted] addressed all specifics of the recommendations.

(U) Comments from the Commander, 7th Signal Command (Theater), did not address Recommendations A.3.a and A.3.b and comments from the (b) (7)(E) [redacted]
[redacted] did not address Recommendation A.8.a. Therefore, we request the Commander and Program Director provide additional comments on these recommendations by September 6, 2016.

(U) The Commander, Network Enterprise Technology Command; (b) (7)(E) [redacted]
[redacted]
[redacted]

~~SECRET~~

~~SECRET~~

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

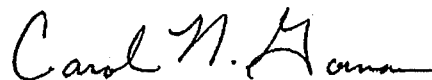
did not provide comments on a draft of this report. Therefore, we request that the Commander, (b) (7)(E) provide comments on the final report by September 6, 2016.

(U) The Commander, Army Cyber Command and Second Army; the Deputy Commanding General, Installation Management Command; and the Division Chief, Army Spectrum Management Office, provided unsolicited comments on a draft of this report. Comments from the Commander, Army Cyber Command and Second Army, addressed the command's responsibility to ensure corrective actions were taken across the Army. However, comments from the Division Chief, Army Spectrum Management Office, did not address Recommendation B.5.b. Therefore, we request additional comments on this recommendation by September 6, 2016.

(U) Please provide comments that state whether you agree or disagree with the findings and recommendations. If you agree with our recommendations, describe what actions you have taken or plan to take to accomplish the recommendations and include the completion dates of your actions. If you disagree with the recommendations or any part of them, please give specific reasons why you disagree and propose alternative action if that is appropriate.

(U) Please provide comments that conform to the requirements of DoD Instruction 7650.03. Classified comments must be sent electronically over the Secret Internet Protocol Router Network. Please send a PDF file containing your comments to (b) (6) and (b) (6). Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. Comments provided on the final report must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).



Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

~~SECRET~~

(U) Contents

(U) Introduction.....	1
(U) Objective.....	1
(U) Background.....	1
(U) Review of Internal Controls.....	3
(U) Finding A.....	4
(FOUO) (b) (7)(E).....	4
(FOUO) (b) (7)(E).....	5
(FOUO) (b) (7)(E).....	6
(FOUO) (b) (7)(E).....	7
(FOUO) (b) (7)(E).....	8
(FOUO) (b) (7)(E).....	9
(U) System Access Forms Were Not Completed or Incorrectly Completed.....	11
(U) Required Security Training Was Not Conducted or Completed.....	13
(FOUO) (b) (7)(E).....	16
(U) Recommendations, Management Comments, and Our Response.....	17
(U) Finding B.....	34
(FOUO) (b) (7)(E).....	34
(FOUO) (b) (7)(E).....	35
(FOUO) (b) (7)(E).....	36
(FOUO) (b) (7)(E).....	38
(U) Recommendations, Management Comments, and Our Response.....	39
(U) Appendix A	47
(U) Scope and Methodology.....	47
(U) Use of Computer-Processed Data.....	50
(U) Use of Technical Assistance.....	51
(U) Prior Coverage.....	51
(U) Appendix B	52
(U) Appendix C	53
(U) Appendix D	57
(U) Appendix E.....	60

(U) Management Comments	62
(U) 7th Signal Command (Theater) Comments	62
(U) (b) (7)(E)	72
(U) (b) (7)(E) Comments.....	73
(U) Army Chief Information Officer Comments.....	77
(U) (b) (7)(E)	78
(U) (b) (7)(E) Comments	80
(U) US Army Installation Management Command Comments	81
(U) Army Cyber Command and Second Army Comments	84
(U) Army Spectrum Management Office Comments	87
(U) Glossary	88
(U) Acronyms and Abbreviations.....	90
(U) Annex	91

(U) Introduction

(U) Objective

(U) Our audit objective was to determine whether the Army effectively protected SECRET Internet Protocol Router Network (SIPRNet) access points.³ Specifically, we reviewed the security safeguards⁴ protecting SIPRNet access points at selected locations. This is the third in a series of audits to review the safeguards implemented by the Military Departments for protecting the SIPRNet.

(U) Background

~~(FOUO)~~ The Army used a hybrid (centralized and decentralized) method to manage SIPRNet circuits⁵ and security. The Army Network Enterprise Technology Command is the Army's information technology service provider. The 7th Signal Command (Theater) (7th SC[T]), a command subordinate to the Army Network Enterprise Technology Command, manages the continental United States portion of the Army's enterprise network, Land Warrior Network. 7th SC(T) also manages the regional and local Network Enterprise Centers (NECs), ^{(b) (7)(E)} [REDACTED]. The regional and local NECs work together to varying degrees to manage physical and logical safeguards⁶ to protect the network. In addition to the NECs, ^{(b) (7)(E)} [REDACTED]

~~(FOUO)~~ In addition to Land Warrior Network, other Army commands manage SIPRNet connections independently of 7th SC(T). For example, ^{(b) (7)(E)} [REDACTED]

^{(b) (7)(E)} [REDACTED] The Figure shows the different SIPRNet management structures.

(U) ³ SIPRNet access points are all possible physical or logical connections where a user can access the network.

(U) ⁴ For this report, security safeguards are information assurance controls.

(U) ⁵ Circuits are devices that transmit data between two or more points.

(U) ⁶ Physical safeguards (such as locks, guards, and security containers) deter or delay adversaries' unauthorized access to the network. Logical safeguards are system-based mechanisms (such as firewalls, permission settings, and usernames and passwords) that designate who or what has access to a specific system or function.

(U) Figure: Simplified View of Army SIPRNet Management Structure



(U) Source: DoD Office of Inspector General.

(U) We visited seven installations and reviewed physical and logical safeguards for SIPRNet access points at the following locations:

- (U) (b) (7)(E)
- (U) (b) (7)(E)
- (U) (b) (7)(E)
- (U) (b) (7)(E);⁷
- (U) (b) (7)(E)
- (U) (b) (7)(E)

(U) ⁷ We visited the (b) (7)(E)

(U) The networks we reviewed were accredited under DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Program (DIACAP)," November 28, 2007. DIACAP was replaced by DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014. However, the authorizations to operate for the networks included in the audit scope were issued under DIACAP. See Appendix B for a discussion on the transition to RMF.

(U) Review of Internal Controls

~~(FOUO)~~ DoD Instruction 5010.40⁸ 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.

(b) (7)(E)

(b) (7)(E)

access forms were accurately completed; and required security training was completed.

~~(FOUO)~~ (b) (7)(E)

We will provide a copy of the report to the senior official responsible for internal controls at the Office of the Army Chief Information Officer, (b) (7)(E)

(U) ⁸ DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

(U) ⁹ (b) (7)(E)

(U) ¹⁰ (b) (7)(E)

(U) Finding A

(FOUO)

(b) (7)(E)

(FOUO) The Army

(b) (7)(E)

Specifically:

- (S) (b) (1), EO 13526, sec. 1.4(g) [Redacted]
- (FOUO) (b) (7)(E) [Redacted]
- (S) (b) (1), EO 13526, sec. 1.4(g) [Redacted]
- (FOUO) (b) (7)(E) [Redacted]
(b) (7)(E) [Redacted]
- (FOUO) (b) (7)(E) [Redacted]

- (FOUO) (b) (7)(E) [REDACTED]
[REDACTED] did not review and verify that SIPRNet user access request forms were properly completed. This occurred because the commands did not establish and implement processes to verify the forms were properly completed.
- (FOUO) (b) (7)(E) [REDACTED]
[REDACTED] did not ensure all personnel completed required security training before being granted access to the SIPRNet. This occurred because the commands did not establish policies and procedures to verify that users completed all required training before being granted SIPRNet access.

(FOUO) (b) (7)(E) [REDACTED] :

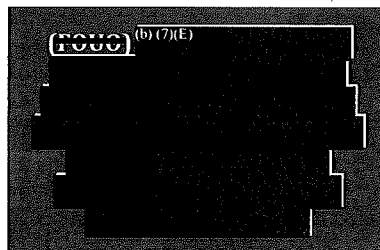
- (FOUO) (b) (7)(E) [REDACTED]
- (FOUO) (b) (7)(E) [REDACTED]
- (FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]

(FOUO) (b) (7)(E) [REDACTED]
[REDACTED]

(FOUO) The Army (b) (7)(E) [REDACTED]. Specifically, the Army Network Enterprise Technology Command list of (b) (7)(E) SIPRNet circuits owned by Army installations did not include (b) (7)(E) circuits that were found on a Defense Information Systems Agency-managed list of Army SIPRNet circuits. In addition, the Army's list of (b) (7)(E) circuits included (b) (7)(E) circuits that were not on Defense Information Systems Agency's list. We determined that discrepancies existed between the two lists, but did not verify the accuracy and completeness of either list.

(FOUO) In addition, we discovered circuit information that was different from the information reported by Army Network Enterprise Technology Command and 7th SC(T). Specifically, (b) (7)(E)

[REDACTED]



(FOUO) The Army did not have an effective process to (b) (7)(E)

[REDACTED]

[REDACTED] The Army Chief Information Officer, in coordination with the Army Cyber Command and Second Army, should establish and implement procedures to (b) (7)(E)

[REDACTED]

(FOUO) (b) (7)(E)

(FOUO) (b) (7)(E)

(U) ¹¹ (b) (7)(E)

(U) ¹² Defense Information Systems Agency, "Access Control in Support of Information Systems," Security Technical Implementation Guide version 2, release 3, October 29, 2010.

[illegible]

(FOUO) Although we identified that (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED].¹⁵ Therefore, we recommend that the
Commander, 7th SC(T), review whether subordinate commands (b) (7)(E) [REDACTED]

(FOUO) (b) (7)(E)

(S) (b) (1), EO 13526, sec. 1.4(g) [REDACTED]

(U) 14 (b) (7)(E)

(U) 16 (b) (7)(E)

(S) (b) (1), EO 13526, sec. 1.4(g) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Table 1 shows the length of time the (b) (1), EO 13526, sec. 1.4(g) [REDACTED]
[REDACTED]

(U) Table 1. Number and Duration of (b) (7)(E) [REDACTED]
(S) (b) (1), EO 13526, sec. 1.4(g) [REDACTED] (b) (1), EO 13526, sec. 1.4(g) [REDACTED]
(b) (1), EO 13526, sec. 1.4(g) [REDACTED]
(S)

(S) (b) (1), EO 13526, sec. 1.4(g) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(FOUO) (b) (7)(E) [REDACTED]

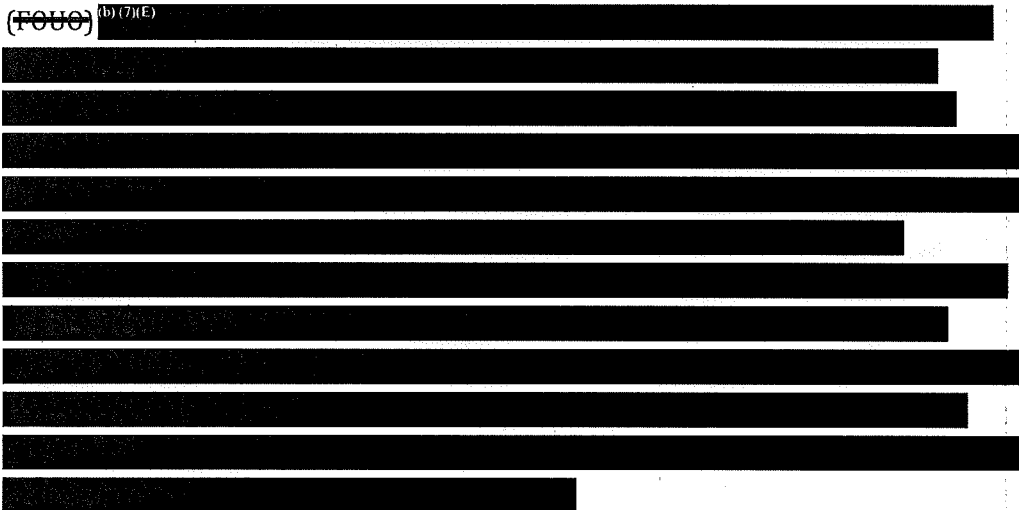
(FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) ¹⁷ For this report, (b) (7)(E) [REDACTED]
(U) ¹⁸ Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011.
(U) ¹⁹ Army Regulation 25-2, "Information Assurance," March 23, 2009.

(FOUO) (b) (7)(E)

A large block of text is redacted with black bars. It consists of approximately 10 lines of text, with varying lengths of redaction.

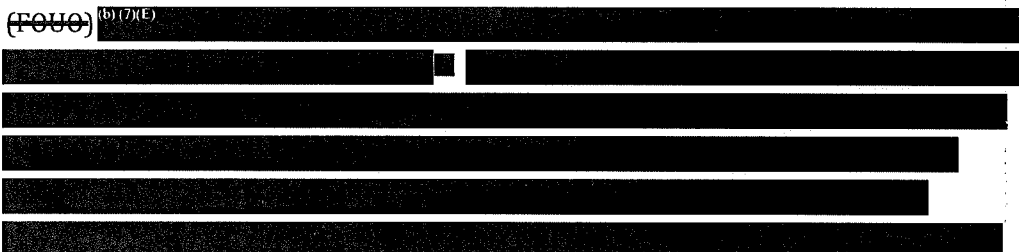
(FOUO) (b) (7)(E)

A large block of text is redacted with black bars. It consists of approximately 10 lines of text, with varying lengths of redaction.

(FOUO) (b) (7)(E)


A block of text is redacted with black bars. It consists of approximately 2 lines of text.

(FOUO) (b) (7)(E)

A large block of text is redacted with black bars. It consists of approximately 5 lines of text, with varying lengths of redaction.

(U) ²⁰ When performing the control tests, we used the control test table developed by DoD Office of Inspector General Quantitative Methods Division and published in the Council of the Inspectors General on Integrity and Efficiency, "Journal of Public Inquiry," 2012-2013.

(U) ²¹ (b) (7)(E)

A block of text is redacted with black bars. It consists of approximately 1 line of text.

(U) ²² Army Regulation 25-2, "Information Assurance," March 23, 2009.

(FOUO) (b) (7)(E) [Redacted]
[Redacted]
[Redacted]

(FOUO) (b) (7)(E) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(FOUO) (b) (7)(E) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(FOUO) (b) (7)(E) [Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) ²³(b) (7)(E) [Redacted]
[Redacted]

(U) ²⁴(b) (7)(E) [Redacted] is a network tool that compares audit log events to defined organizational rules and generates a report of reportable events.

(U) ²⁵ Boundary protection is monitoring and controlling communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications.

(FOUO) (b) (7)(E)

(U) System Access Forms Were Not Completed or Incorrectly Completed

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

officials did not review and verify that SIPRNet user access request forms were completed as required by DoD guidance, which requires each user who requests SIPRNet access to complete a:

- (U) DD Form 2875, "System Authorization Access Request (SAAR);"²⁶ and
- (U) DD Form 2842, "Department of Defense Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities," August 2009.²⁷

(U) The IA officials did not verify completion of required forms to gain SIPRNet access. We performed control tests for DD Forms 2875 and 2842 to verify whether the forms were correctly completed for:

- (U) 42 personnel at (b) (7)(E)
- (U) 35 personnel at (b) (7)(E)
- (U) 33 personnel at (b) (7)(E),
- (U) 44 personnel at (b) (7)(E),
- (U) 21 personnel at (b) (7)(E), and
- (U) 43 personnel at (b) (7)(E).

(U) ²⁶ DD Form 2875 documents supervisor, security manager, and IA officer approval for system access and need-to-know. It is required by the Defense Information Systems Agency, "Enclave" Security Technical Implementation Guide, version 4, release 5, August 21, 2014.

(U) ²⁷ DD Form 2842 is completed by users to acknowledge their responsibility to safeguard tokens and the registration official to verify the identity of the users who fill out the form.

(U) We identified errors in the forms reviewed, so the control test failed. See Appendix C for test results. Table 2 identifies the number of forms received out of the number requested and whether the forms were completed correctly.

(U) Table 2. Test Results of Forms Required for SIPRNet Access

(U)	DD Form 2875	DD Form 2842
(b) (7)(E)		
Received (out of 42)	42	31
Completed Correctly	5	4
Completed Incorrectly	37	27
Forms Not Received	0	11
(b) (7)(E)		
Received (out of 35)	35	32
Completed Correctly	26	31
Completed Incorrectly	9	1
Forms Not Received	0	3
(b) (7)(E)		
Received (out of 33)	0	29
Completed Correctly	N/A	7
Completed Incorrectly	N/A	22
Forms Not Received	33	4
(b) (7)(E)		
Received (out of 44)	23	18
Completed Correctly	7	18
Completed Incorrectly	16	0
Forms Not Received	21	26
(b) (7)(E)		
Received (out of 21)	21	19
Completed Correctly	18	8
Completed Incorrectly	3	11
Forms Not Received	0	2
(b) (7)(E)		
Received (out of 43)	8	11
Completed Correctly	0	9
Completed Incorrectly	8	2
Forms Not Received	35	32

(U)

(FOUO) System access forms were not completed or incorrectly completed because IA officials at (b) (7)(E)

did not establish and implement effective procedures to verify the forms were properly completed before granting network access. In addition, the commands did not request copies of the DD Forms 2842 from the commands that previously issued SIPRNet tokens and did not implement procedures to validate whether the tokens were properly authorized. Since personnel movements in the military are frequent, the lack of procedures to verify SIPRNet token authorizations by prior commands may represent a systemic issue across the Army. The Army Chief Information Officer should develop policy and procedures to verify whether SIPRNet users were properly authorized to access the system when transferring from one command to another.

(U) Without adequate access controls, personnel at these commands may have been granted access to classified information without a need to know. To ensure the confidentiality of the SIPRNet, a determination is needed²⁸ on whether a user has the appropriate need-to-know and authorizations to access the network. These decisions are documented on the DD Forms 2875 and 2842. (b) (7)(E)

should develop procedures to verify that access forms are properly completed before granting access to the SIPRNet.

(U) Required Security Training Was Not Conducted or Completed

(U) (b) (7)(E) did not ensure all personnel completed required initial and refresher security-related training as a condition for accessing the SIPRNet. Specifically, IA officials did not require users to complete initial and annual IA and security awareness training and did not verify that all SIPRNet users completed this training. Additionally, they did not require all personnel with SIPRNet access to complete a

(U) ²⁸ A determination of a user's need-to-know and authorization for access to SIPRNet is made by multiple personnel such as supervisors and security managers.

(U) NATO briefing. See Appendix D for test results. DoD guidance²⁹ requires all DoD civilians, military members, and onsite support contractors with access to classified information to receive annual refresher training that reinforces the policies, principles, and procedures covered in their initial and specialized training. The guidance also requires users to take IA training before being granted access to a system and annually thereafter.

(U) DoD guidance³⁰ also requires that all DoD military and civilian personnel be briefed on their responsibilities for protecting NATO information. Contractors also have access to classified information, so they are required to receive the NATO briefing. Security personnel at (b) (7)(E) did not ensure that all users completed the NATO security briefing. Specifically, these commands did not provide documentation to support that all users completed the briefing.

(FOUO) Security personnel at (b) (7)(E) stated that they did not require a NATO briefing because (b) (7)(E), and they were not aware that the briefing was required for all personnel with access to the SIPRNet. Instead, the security personnel stated that if a user required access to NATO information, (b) (7)(E) provided a NATO briefing to that specific user. In addition, the (b) (7)(E) information system security manager stated that Army policy did not specifically require NATO briefings. Although Army policy did not specifically require the NATO briefings, DoD policy requires the briefing for all civilians, military, and contractors with access to classified information. NATO information (b) (7)(E)

Also, NATO information is not always clearly marked. Therefore, SIPRNet users could potentially access NATO information, whether sent through e-mail or viewed online, or users may not be protecting the information as required by NATO standards. Table 3 identifies security training documents received out of the number requested and whether the training documents were properly completed.

(U) ²⁹ DoD Manual 5200.01, volume 3, "DoD Information Security Program: Protection of Classified Information," March 19, 2013, and Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011.

(U) ³⁰ DoD Manual 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012.

(U) Table 3. Test Results of Required Security Training

(U)	IA Training		Security Assurance Training		NATO Briefing
	Initial	Annual	Initial	Annual	
		(b) (7)(E)			
Received (out of 42)	41	42	1	42	42
Completed Correctly	34	42	1	42	31
Completed Incorrectly	7	0	0	0	11
Forms Not Received	1	0	41	0	0
		(b) (7)(E)			
Received (out of 35)	35	35	23	35	0
Completed Correctly	35	35	23	35	0
Completed Incorrectly	0	0	0	0	0
Forms Not Received	0	0	12	0	35
		(b) (7)(E)			
Received (out of 33)	0	33	8	15	18
Completed Correctly	0	33	2	7	6
Completed Incorrectly	0	0	6	8	12
Forms Not Received	33	0	25	18	15
		(b) (7)(E)			
Received (out of 44)	0	20	23	7	27
Completed Correctly	0	20	23	7	27
Completed Incorrectly	0	0	0	0	0
Forms Not Received	44	24	21	37	17
		(b) (7)(E)			
Received (out of 21)	21	21	0	21	20
Completed Correctly	21	21	0	20	19
Completed Incorrectly	0	0	0	1	1
Forms Not Received	0	0	21	0	1
		(b) (7)(E)			
Received (out of 43)	0	13	7	9	11
Completed Correctly	0	13	6	6	5
Completed Incorrectly	0	0	1	3	6
Forms Not Received	43	30	36	34	32

(U)

(U) Personnel responsible for training and granting SIPRNet access at (b) (7)(E) did not establish policies and procedures to verify that users completed all required training before being granted SIPRNet access. The requirement to complete IA, security

(U) The Commander, Network Enterprise and Technology Command, and the Commander, Army Cyber Command and Second Army, in coordination with the Commander, 7th SC(T); (b) (7)(E)

~~(FOUO)~~

~~(FOUO)~~

Report No. DODIG-2016-119 | 16

(U) Recommendations, Management Comments, and Our Response

(U) Renumbered Recommendations

(U) As a result of management comments, we renumbered draft Recommendation A.1.a as Recommendation A.1, draft Recommendation A.1.b as Recommendation A.2.b, and draft Recommendation A.2 as Recommendation A.2.a.

(U) Recommendation A.1

(U) We recommend that the Army Chief Information Officer develop and implement policies and procedures to verify whether SECRET Internet Protocol Router Network (b) (7)(E)

(U) Army Chief Information Officer Comments

(U) The Acting U.S. Army Cybersecurity Director, Headquarters Department of the Army, Chief Information Officer/G-6, responding on behalf of the Army Chief Information Officer, neither agreed nor disagreed, and stated that the Chief Information Officer would review the issue, identify policy gaps, and issue guidance to resolve the issues within (b) (7)(E) of the date of the final report.

(U) Our Response

(U) Comments from the Acting Director addressed all of the specifics of the recommendation and no further comments are required. However, we request a copy of the resulting guidance, when issued for our review and acceptance before we can close the recommendation.

(U) Recommendation A.2

~~(FOUO)~~ We recommend that the Army Chief Information Officer, in coordination with the Commander, Army Cyber Command and Second Army:

- a. (U) establish and implement procedures to (b) (7)(E)

- b. ~~(FOUO)~~ review the deficiencies identified in this report, require a thorough review of the Army SECRET Internet Protocol Router Network security safeguards performed at each command within the Army, and apply corrective actions as necessary.

(U) 7th SC(T) Comments

(U) The Commander, 7th SC(T), disagreed, stating that the 7th SC(T) had responsibility for circuits owned (b) (7)(E)

(b) (7)(E)

(U) Our Response

(U) Based on the Commander's comments, we removed the Commander, 7th SC(T), as an addressee and added the Commander, Army Cyber Command and Second Army, to Recommendations A.2.a and A.2.b. Although the Commander stated that (b) (7)(E)

(b) (7)(E)

(U) Army Chief Information Officer Comments

~~(FOUO)~~ The Acting U.S. Army Cybersecurity Director, Headquarters Department of the Army, Chief Information Officer/G-6, responding on behalf of the Army Chief Information Officer, neither agreed nor disagreed, and stated that the Chief Information Officer would review the issue, identify policy gaps, and issue guidance to resolve the issues within (b) (7)(E) of the date of the final report. In addition, the Acting Director stated that the Chief Information Officer would coordinate with Army Cyber Command and Second Army and, based on their review of Army security safeguards, identify and implement corrective actions within (b) (7)(E) of the date of the final report. Furthermore, the Acting Director stated that the Chief Information Officer would also coordinate with the Network Enterprise Technology Command to resolve issues with managing SIPRNet circuits within (b) (7)(E) of the date of the final report.

(U) Our Response

(U) Comments from the Acting Director addressed all of the specifics of the recommendation, and no further comments are required. However, we request a copy of the resulting guidance when issued for review and acceptance before we can close the recommendation.

(U) Army Cyber Command and Second Army Comments

(U) Although not required to comment, the Deputy Commanding General, Operations, Army Cyber Command and Second Army, stated that Army Cyber Command and Second Army had command authority to direct SIPRNet operations. In addition, the Deputy Commanding General stated that Army Cyber Command and Second Army would work with the Army Chief Information Officer to develop policy. The Deputy Commanding General stated that Army Cyber Command and Second Army would also work with local commands to identify (b) (7)(E) [REDACTED]

(U) Our Response

(U) Based on the Deputy Commanding General's comments, we added the Commander, Army Cyber Command and Second Army, as an addressee for Recommendations A.2.a and A.2.b. Comments from the Deputy Commanding General were responsive to the recommendation. If no further comments are provided, we will consider these comments as management's response to the final report.

(U) Recommendation A.3

(U) We recommend that the Commander, Network Enterprise Technology Command, and the Commander, Army Cyber Command and Second Army, in coordination with the Commander, 7th Signal Command (Theater); (b) (7)(E) [REDACTED]

- a. (U) develop and implement procedures to verify that personnel and contractors requesting SECRET Internet Protocol Router Network access complete initial and annual security-related training and the North Atlantic Treaty Organization briefing as a condition for obtaining and maintaining access; and**

- b. (U) implement a process to identify and retain training records for personnel to support the requirements for accessing the SECRET Internet Protocol Router Network.**

(U) (b) (7)(E) *Comments*

(U) (b) (7)(E) , neither agreed nor disagreed, stating that the (b) (7)(E) worked with applicable security groups to develop and enforce a training plan to ensure required training was completed and properly annotated before granting SIPRNet access. The (b) (7)(E) stated (b) (7)(E) developed the plan in March 2016. In addition, the (b) (7)(E) stated that the (b) (7)(E) worked with applicable security groups to correct its process to retain training records for personnel with SIPRNet access.

(U) *Our Response*

(U) Comments from the (b) (7)(E) addressed all of the specifics of the recommendation, and no further comments are required. However, we request a copy of the approved plan to retain training records before we can close the recommendation.

(U) *Management Comments Required*

(U) The Commander, Network Enterprise Technology Command; (b) (7)(E) did not provide comments on a draft of this report. We request that the Commanders and Directors provide comments on the final report.

(U) *7th SC(T) Comments*

(U) Although not required to comment, the Commander, 7th SC(T), stated that the Network Enterprise Technology Command should coordinate with the 7th SC(T) to confirm and enforce established procedures in the continental United States. The Commander stated that 7th SC(T) had procedures to verify required training was taken and that 7th SC(T) processed all network access requests and validated security clearance eligibility for (b) (7)(E) through the 7th SC(T) security office. The Commander stated that 7th SC(T) procedures ensured all security training, including annual security refresher, derivative classification, and NATO awareness training, was completed.

(U) The Commander also stated that the 7th SC(T) security office retained security training records for (b)(7)(E) and directed the use of the Army Training and Certification Tracking System to track training required for accessing networks. The Commander stated that 7th SC(T) would ensure subordinate organizations complied with existing requirements.

(U) Our Response

(U) Based on the Commander's comments, we added the Commander, 7th SC(T), as an addressee for Recommendations A.3.a and A.3.b. Comments from the Commander were partially responsive. As previously reported, (b)(7)(E) officials could not provide support that all 42 personnel in our sample completed the required training as a condition for receiving or maintaining SIPRNet access. Therefore, the existing requirements described by the Commander were not effective in tracking training completion and should be reviewed and updated. We request additional comments on how the Commander, 7th SC(T), plans to effectively track and retain training records.

(U) Army Cyber Command and Second Army Comments

(U) Although not required to comment, the Deputy Commanding General, Operations, Army Cyber Command and Second Army, stated that the Network Enterprise Technology Command would need to coordinate with the NECs and (b)(7)(E) to implement corrective actions, which would result in circumventing several layers of command. The Deputy Commanding General stated that Army Cyber Command and Second Army would take necessary actions to ensure subordinate commands implemented the recommendations within (b)(7)(E) of the date of the final report.

(U) Our Response

(U) Based on the Deputy Commanding General's comments, we added the Commander, 7th SC(T), as an addressee for Recommendation A.3. Comments from the Deputy Commanding General were responsive to the recommendation. If no further comments are provided, we will consider these comments as management's response to the final report.

(U) Recommendation A.4

~~(FOUO)~~ We recommend that the Commander, 7th Signal Command (Theater), verify whether subordinate commands implemented a SECRET Internet Protocol Router Network (b) (7)(E)

(U) 7th SC(T) Comments

(U) The Commander, 7th SC(T), agreed, and stated that the command issued an order requiring SIPRNet (b) (7)(E)

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation, and no further comments are required. However, we request a copy of the order for our review and acceptance before we can close the recommendation.

(U) Recommendation A.5

(U) We recommend that the (b) (7)(E)

- a. (U) develop and implement procedures to verify that personnel and contractors requesting SECRET Internet Protocol Router Network access complete initial and annual security-related training and the North Atlantic Treaty Organization briefing as a condition for obtaining and maintaining access; and

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

(U) The Commander, (b) (7)(E), responding for her command and on behalf of the (b) (7)(E), agreed, stating that the (b) (7)(E) and the (b) (7)(E) modified their process for requesting SIPRNet access to require the completion of initial security awareness training and the NATO briefing before the security manager signed DD Form 2875.

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation, and no further comments are required. However, we request a copy of the modified and approved procedures for our review and acceptance before we can close the recommendation.

- b. (U) implement a process to identify and retain training records for personnel to support the requirements for accessing the SECRET Internet Protocol Router Network.**

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

(U) The Commander, (b) (7)(E), responding for her command and on behalf of the (b) (7)(E), agreed, stating that the (b) (7)(E) and the (b) (7)(E) were now using the Total Employee Development System to track security awareness training completion and the Army Training and Certification Tracking System to track IA awareness training completion. The Commander stated that SIPRNet access would not be granted until training completion was verified and the certificates were loaded in the systems of record.

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation, and no further comments are required. However, we request a copy of the approved procedures for retaining training records for our review and acceptance before we can close the recommendation.

(U) Recommendation A.6

~~(FOUO)~~ We recommend that the (b) (7)(E)

(U) Management Comments Required

(U) (b) (7)(E) did not provide comments on a draft of this report. We request that the Director provide comments on the final report.

(U) 7th SC(T) Comments

(U) Although not required to comment, the Commander, 7th SC(T), stated that Army Cyber Command and Second Army should coordinate with the Network Enterprise Technology Command and the theater signal commands to establish and implement procedures Army-wide. The Commander stated that 7th SC(T) and subordinate organizations (b) (7)(E)

(b) (7)(E) In addition, the Commander stated that 7th SC(T) was transitioning to the (b) (7)(E)

(U) Our Response

(U) We acknowledge the Commander's comments, but did not redirect the recommendation to a higher-level command because the NECs need to be involved in developing and implementing corrective actions specific to their organizations. We agree with the Commander that deficiencies identified in the report may require Army-wide action, which is why we included a recommendation for the Army Chief Information Officer and Army Cyber Command and Second Army to review Army SIPRNet safeguards at each command and apply corrective actions as necessary.

(U) Recommendation A.7

(U) We recommend that the (b) (7)(E), in coordination with the Commander, Army Cyber Command and Second Army:

- a. (S) (b) (1), EO 13526, sec. 1.4(g) (b) (7)(E)
- b. (S) (b) (1), EO 13526, sec. 1.4(g) (b) (7)(E)
- c. (FOUO) (b) (7)(E)
- d. (U) develop and implement procedures to verify that access forms are properly completed before granting access to the SECRET Internet Protocol Router Network.

(U) Management Comments Required

(U) (b) (7)(E) , did not provide comments on a draft of this report. We request that the Director provide comments on the final report.

(U) 7th SC(T) Comments

(U) Although not required to comment, the Commander, 7th SC(T), stated that Army Cyber Command and Second Army should coordinate with the Network Enterprise Technology Command and the theater signal commands to establish and implement procedures Army-wide. The Commander stated that a 7th SC(T) regulation establishes a framework for managing vulnerabilities and includes procedures for mitigating and correcting vulnerabilities. In addition, the Commander stated that 7th SC(T) and subordinate organizations (b) (7)(E)

(b) (7)(E) The Commander also stated that 7th SC(T) was transitioning to the (b) (7)(E)

(b) (7)(E) Furthermore, the Commander stated that the 7th SC(T) security office validated security clearance and access eligibility as part of the process for completing access forms.

(U) Our Response

(U) We agree with the Commander's comments, and added the Commander, Army Cyber Command and Second Army, as an addressee for Recommendations A.7.a, A.7.b, A.7.c, and A.7.d. However, we did not redirect the recommendation solely to a higher-level command because (b) (7)(E) needs to be involved in developing and implementing corrective actions specific to its organization. We agree with the Commander that deficiencies identified in the report may require Army-wide action, which is why we included a recommendation for the Army Chief Information Officer and Army Cyber Command and Second Army to review Army SIPRNet safeguards at each command and apply corrective actions as necessary. Although the Commander stated the 7th SC(T) security office validated access forms, we previously reported that 30 of the 42 SIPRNet access request forms reviewed for (b) (7)(E) were not approved by a security manager. Without the security manager's signature, there is no assurance that security clearance and access eligibility was validated.

(U) Army Cyber Command and Second Army Comments

(U) Although not required to comment, the Deputy Commanding General, Operations, Army Cyber Command and Second Army, stated that (b) (7)(E). The Deputy Commanding General stated that Army Cyber Command and Second Army would take necessary actions to ensure subordinate commands implemented the recommendations within (b) (7)(E) of the date of the final report.

(U) Our Response

(U) Based on the Deputy Commanding General's comments, we added Army Cyber Command and Second Army as an addressee for Recommendations A.7.a, A.7.b, A.7.c, and A.7.d. Comments from the Deputy Commanding General were responsive to the recommendations. If no further comments are provided, we will consider these comments as management's response to the final report.

(U) Recommendation A.8

(U) We recommend that the (b) (7)(E):

- a. ~~(FOUO)~~ develop and implement procedures (b) (7)(E) as required by DoD guidance;

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

(U) (b) (7)(E) neither agreed nor disagreed, stating that (b) (7)(E) developed an account management policy and implemented a process (b) (7)(E) and that this process was defined in standard operating procedures.

(U) Our Response

(U) Comments from (b) (7)(E) did not address the specifics of the recommendation. The standard operating procedure did not include a process for (b) (7)(E). The procedures address a process for (b) (7)(E). Therefore, we request that (b) (7)(E), provide additional comments on (b) (7)(E).

- b. (U) develop and implement procedures to verify that access forms are properly completed before granting access to the SECRET Internet Protocol Router Network; and
- c. (U) develop and implement procedures to verify personnel and contractors requesting SECRET Internet Protocol Router Network access complete the North Atlantic Treaty Organization briefing as a condition for obtaining and maintaining access.

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

(U) (b) (7)(E) neither agreed nor disagreed, stating that the command now required all access request forms to be reviewed and verified for accuracy and completeness. The (b) (7)(E) stated that individual training and certifications were verified through the Army Training and Certification Tracking System. In addition, the (b) (7)(E) stated that (b) (7)(E) began requiring annual NATO security classification training as a condition for obtaining and maintaining SIPRNet access. The (b) (7)(E) stated that (b) (7)(E) defined the processes in standard operating procedures.

(U) Our Response

(U) Comments from the (b) (7)(E) addressed all of the specifics of the recommendation, and no further comments are required.

(U) Recommendation A.9

(U) We recommend that the (b) (7)(E)

a. (FOUO) (b) (7)(E)

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

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

(b) (7)(E) neither agreed nor disagreed, stating that (b) (7)(E) in accordance with Defense Information Systems Agency Security Technical Implementation Guides.

(b) (7)(E)

(b) (7)(E)

(U) Our Response

(U) Comments from (b) (7)(E) addressed all of the specifics of the recommendation, and no further comments are required.

b. (FOUO) develop and implement procedures to (b) (7)(E)

(b) (7)(E) as required by DoD guidance;

c. (FOUO) (b) (7)(E)

(b) (7)(E) required by DoD guidance, and (b) (7)(E) as required by Army guidance;

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

(FOUO) (b) (7)(E)
(b) (7)(E), neither agreed nor disagreed, stating that the
(b) (7)(E) issued an (b) (7)(E)
(b) (7)(E) stated that since
January 2016, (b) (7)(E) has followed the policy, which also requires (b) (7)(E).

(U) Our Response

(U) Comments from the Garrison Commander and the Director addressed all of the specifics of the recommendation, and no further comments are required.

d. (FOUO) (b) (7)(E)
(b) (7)(E) and

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

(FOUO) (b) (7)(E)
(b) (7)(E), neither agreed nor disagreed, stating that the
(b) (7)(E)
(b) (7)(E) stated that
the information systems security manager (b) (7)(E) in
accordance with Defense Information Systems Agency Security Technical
Implementation Guide requirements.

(U) Our Response

(U) Comments from (b) (7)(E) addressed all of the specifics of the recommendation, and no further comments are required. However, we request a copy of the approved procedures for reviewing audit logs before we close the recommendation.

- e. (U) develop and implement procedures to verify that access forms are properly completed before granting access to the SECRET Internet Protocol Router Network.

(U) (b) (7)(E) *Comments*

(FOUO) (b) (7)(E)

(b) (7)(E), neither agreed nor disagreed, stating that the (b) (7)(E) implemented a policy for accessing the network that requires all training and access request forms to be complete and correct before granting access to a user.

(U) Our Response

(U) Comments from (b) (7)(E) addressed all of the specifics of the recommendation, and no further comments are required. However, we request a copy of the approved policy before we can close the recommendation.

(U) 7th SC(T) Comments

(U) Although not required to comment, the Commander, 7th SC(T), stated that Army Cyber Command and Second Army should coordinate with the Network Enterprise Technology Command to establish and implement procedures Army-wide.

(U) Our Response

(U) We acknowledge the Commander's comments, but did not redirect the recommendation to a higher-level command because the NECs need to be involved in developing and implementing corrective actions specific to their organizations. We agree with the Commander that deficiencies identified in the report may require Army-wide action, which is why we included a recommendation for the Army Chief Information Officer and Army Cyber Command and Second Army to review Army SIPRNet safeguards at each command and apply corrective actions as necessary.

(U) Recommendation A.10

(U) We recommend that the (b) (7)(E) develop and implement procedures to verify that access forms are properly completed before granting access to the SECRET Internet Protocol Router Network.

(U) Management Comments Required

(U) (b) (7)(E) did not provide comments on a draft of the report. We request that the (b) (7)(E) provide comments on the final report.

(U) 7th SC(T) Comments

(U) Although not required to comment, the Commander, 7th SC(T), stated that the 7th SC(T) security office validated security clearance and access eligibility as part of its process for completing access request forms.

(U) Our Response

(U) We acknowledge the Commander's comments; however, the 7th SC(T) did not validate clearances for non-7th SC(T) personnel with SIPRNet access provided by the NECs. Although the Commander stated the 7th SC(T) security office validated access forms, (b) (7)(E) could not provide 21 of the 44 SIPRNet access forms requested. Without signed access request forms, there is no assurance that personnel were properly validated or approved for SIPRNet access.

(U) Recommendation A.11

(U) We recommend that the (b) (7)(E) develop and implement procedures to verify that access forms are properly completed before granting access to the SECRET Internet Protocol Router Network.

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

(U) (b) (7)(E) neither agreed nor disagreed, stating that the (b) (7)(E) established procedures and a local instruction requiring the (b) (7)(E) cyber security team to verify that access forms were properly completed.

(U) Our Response

(U) Comments from the Director (b) (7)(E), addressed all of the specifics of the recommendation, and no further comments are required.

(U) Recommendation A.12

(U) We recommend that the (b) (7)(E)

:(b) (7)(E)

a. (FOUO) (b) (7)(E)

(b) (7)(E) as required by DoD guidance;

- b. ~~(FOUO)~~ (b) (7)(E) [REDACTED]
[REDACTED] as required by DoD guidance, and
(b) (7)(E) [REDACTED] as required by
Army guidance; and
- c. (U) develop and implement procedures to verify that access forms are properly completed before granting access to the SECRET Internet Protocol Router Network.

(U) Management Comments Required

(U) (b) (7)(E) [REDACTED] did not provide comments on a draft of this report. We request that the Director provide comments on the final report.

(U) 7th SC(T) Comments

(U) Although not required to comment, the Commander, 7th SC(T), stated that Army Cyber Command and Second Army should coordinate with the Network Enterprise Technology Command to establish and implement procedures Army-wide. In addition, the Commander suggested combining Recommendations A.12.a, A.12.b, and A.12.c with Recommendations A.9.a, A.9.b, A.9.c, and A.9.d.

(U) Our Response

(U) We acknowledge the Commander's comments, but did not redirect the recommendation to a higher-level command or combine the recommendations because the NECs need to be involved in developing and implementing corrective actions specific to their organizations. We agree with the Commander that deficiencies identified in the report may require Army-wide action, which is why we included a recommendation for the Army Chief Information Officer and Army Cyber Command and Second Army to review Army SIPRNet safeguards at each command and apply corrective actions as necessary.

(U) Army Cyber Command and Second Army Comments

~~(FOUO)~~ Although not required to comment, the Deputy Commanding General, Operations, Army Cyber Command and Second Army, stated that Army Cyber Command and Second Army agreed with the findings and recommendations. The Deputy Commanding General stated, (b) (7)(E) [REDACTED]

(FOUO) (b) (7)(E)

Additionally, the Deputy Commanding General stated that Army Cyber Command and Second Army (b) (7)(E)

The Deputy Commanding General stated that the Commander, 7th SC(T), was in a better position to standardize practices and direct corrective actions, but also stated that Army Cyber Command and Second Army would take necessary action to ensure that subordinate commands implemented the recommendations within (b) (7)(E) of the date of the final report. Furthermore, the Deputy Commanding General acknowledged that merely correcting and reporting on the findings identified in the DoD Inspector General report was inefficient and ineffective in addressing SIPRNet security deficiencies.

(U) Our Response

(FOUO) We agree with the Deputy Commanding General's comments, but did not redirect all recommendations in the report to higher-level commands. Instead, we added the Commander, Army Cyber Command and Second Army, and the Commander, 7th SC(T), to the recommendations when appropriate. We acknowledge that 7th SC(T) may be in a better position to standardize procedures and oversee the implementation of corrective actions. Although the Deputy Commanding General stated it was inappropriate for NECs to answer the recommendations, the NECs need to be involved in developing and implementing corrective actions specific to their organizations. We also agree with the Deputy Commanding General (b) (7)(E) which is why we included a recommendation for the Army Chief Information Officer and Army Cyber Command and Second Army to review Army SIPRNet safeguards at each command and apply corrective actions as necessary.

(U) Finding B

(FOUO)

(b) (7)(E)

(FOUO) The Army

(b) (7)(E)

Specifically:

- (FOUO)

(b) (7)(E)

- (FOUO)

(b) (7)(E)

(FOUO)

(b) (7)(E)

- (FOUO)

(b) (7)(E)

- (FOUO)

(b) (7)(E)

- (FOUO)

(b) (7)(E)

(FOUO) (b) (7)(E) [Redacted]

(FOUO) (b) (7)(E) [Redacted]

(FOUO) (b) (7)(E) [Redacted]

(FOUO) (b) (7)(E) [Redacted]

(FOUO) (b) (7)(E) [Redacted]

[Redacted] in coordination with the Division Chief, Army Spectrum

(U) ³¹ National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems," December 13, 1996.

(U) ³² The Army Spectrum Management Office is the headquarters for the Frequency Management group.

(FOUO) Management Office, (b) (7)(E) as required by the National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems," December 13, 1996.

(FOUO) (b) (7)(E)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(FOUO) (b) (7)(E)
[Redacted]

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

(U) SIPRNet Physical Security Safeguards

(FOUO) (b) (7)(E)
[Redacted] DoD guidance³³ requires (b) (7)(E)
[Redacted]
[Redacted] Specifically, the (b) (7)(E)
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted] (b) (7)(E)
[Redacted]
[Redacted]
[Redacted]

(FOUO) Specifically, the
(b) (7)(E)
[Redacted]
[Redacted]
[Redacted]

(U) ³³ DoD Manual 5200.01, volume 3, "DoD Information Security Program: Protection of Classified Information," March 19, 2013.

(U) ³⁴ Tactical Local Area Network Encryption (TACLANE) is an in-line network encryptor for development in DoD tactical and strategic networks. The TACLANE is used to encrypt classified network traffic. The TACLANE is connected to SIPRNet (b) (7)(E)

(FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]

(FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Two-Factor Authentication

(FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) ³⁵ Two-factor authentication is the use of two authentication factors, such as something you know, something you have, or something you are, for example, using a combination of password/pin, token, or retina scan.

(U) ³⁶ Classified processing areas are spaces where classified information is processed or stored.

(U) ³⁷ The Defense Information Systems Agency, "Access Control In Support Of Information Systems," Security Technical Implementation Guide, version 2, release 3, October 29, 2010.

(U) End-of-Day Security Checks

(FOUO) (b) (7)(E) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(FOUO) (b) (7)(E) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted] (b) (7)(E) [Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(FOUO) (b) (7)(E) [Redacted]
[Redacted]

(FOUO) DoD must defend its information and must do more to secure its cyber infrastructure. (b) (7)(E) [Redacted]
[Redacted]
[Redacted]
(b) (7)(E) [Redacted]
[Redacted]
[Redacted]

(U) Recommendations, Management Comments, and Our Response

(U) Renumbered Recommendations

(U) As a result of management comments, we renumbered draft Recommendation B.1.a and B.1.b as Recommendation B.3.a, B.3.b, B.4.a, and B.4.b; draft Recommendation B.2.a and B.2.b as Recommendation B.1.a and B.1.b; draft Recommendation B.3 as Recommendation B.7; draft Recommendation B.4 as Recommendation B.2; draft Recommendation B.5 as Recommendation B.7; draft Recommendation B.6.a and B.6.b as Recommendations B.5.a and B.5.b; draft Recommendation B.7 as Recommendation B.6; and draft Recommendation B.8 as Recommendation B.4.c.

(U) Recommendation B.1

(U) We recommend that (b) (7)(E)

a. (FOUO) (b) (7)(E)

and

b. (U) develop and implement a training program to ensure personnel understand their responsibilities (b) (7)(E)

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

(U) (b) (7)(E), responding for her command and on behalf of the (b) (7)(E), agreed, stating that (b) (7)(E) and the (b) (7)(E) were contacting vendors and researching solutions to (b) (7)(E)

In addition, the Commander stated that initial and annual security awareness training addresses (b) (7)(E)

Furthermore, the Commander stated that the changes to (b) (7)(E) process for managing access (as part of Recommendation A.5) would ensure personnel were aware of their responsibilities before being granted SIPRNet access.

(U) Our Response

(U) Comments from the Commander addressed all of the specifics of the recommendation, and no further comments are required.

(U) Recommendation B.2

(U) We recommend that the (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED] develop and implement a training program to
ensure personnel understand their responsibilities (b) (7)(E) [REDACTED]
[REDACTED]

(U) (b) (7)(E) [REDACTED] Comments

(U) (b) (7)(E) [REDACTED]
[REDACTED] neither agreed nor disagreed, stating that the (b) (7)(E) [REDACTED]
[REDACTED] worked with applicable security groups to ensure that (b) (7)(E) [REDACTED]
[REDACTED]
(b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED] (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]

(U) Our Response

(U) Comments from (b) (7)(E) [REDACTED] addressed all of the specifics of the recommendation, and no further comments are required.

(U) Recommendation B.3

(U) We recommend that the (b) (7)(E) [REDACTED]
[REDACTED]:

- a. (FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]; and

- b. (U) develop and implement a training program to ensure personnel understand their responsibilities (b) (7)(E)

(U) Management Comments Required

(U) (b) (7)(E) did not provide comments on a draft of this report. We request that the (b) (7)(E) provide comments on the final report.

(U) Recommendation B.4

(U) We recommend that (b) (7)(E)

- a. (FOUO) (b) (7)(E)

; and

- b. (U) develop and implement a training program to ensure personnel understand their responsibilities (b) (7)(E)

- c. (FOUO) (b) (7)(E)

(U) Management Comments Required

(U) (b) (7)(E) did not provide comments on a draft of this report. We request that the (b) (7)(E) provide comments on the final report.

(U) Recommendation B.5

(U) We recommend that the Division Chief, Army Spectrum Management Office, in coordination with the (b) (7)(E)

- a. (FOUO) (b) (7)(E)

; and

b. (FOUO) (b) (7)(E)

(U) Management Comments Required

(U) (b) (7)(E) did not provide comments on a draft of this report. We request that (b) (7)(E) provide comments on the final report.

(U) 7th SC(T) Comments

(U) Although not required to comment, the Commander, 7th SC(T), stated that the (b) (7)(E) . The Commander stated that 7th SC(T) was awaiting Department of the Army, Intelligence Directorate (G2), guidance for (b) (7)(E)

(U) Our Response

(U) We agree with the Commander that (b) (7)(E)

(U) Army Spectrum Management Office Comments

(U) Although not required to comment, the Division Chief, Army Spectrum Management Office, Headquarters, Department of the Army, Chief Information Officer/G-6, neither agreed nor disagreed, stating that (b) (7)(E)

The Division Chief stated that the Army Spectrum Management Office was (b) (7)(E)

(U) ³⁸ Committee on National Security Systems Instruction 7003, "Protected Distribution Systems," September 2015.

(U) Our Response

(U) Comments from the Division Chief partially addressed the specifics of the recommendation. The comments did not address (b) (7)(E)

(b) (7)(E). We request that the Division Chief provide additional comments (b) (7)(E)

(U) Recommendation B.6

(U) We recommend that (b) (7)(E)

(U) Management Comments Required

(U) (b) (7)(E), did not provide comments on a draft of this report. We request that the (b) (7)(E) provide comments on the final report.

(U) Recommendation B.7

~~(FOUO)~~ We recommend the (b) (7)(E)

(U) Management Comments Required

(U) (b) (7)(E) did not provide comments on a draft of this report. We request that the (b) (7)(E) provide comments on the final report.

(U) 7th SC(T) Comments

(U) Although not required to comment, the Commander, 7th SC(T), stated that recommendations should be directed to the Department of the Army, Intelligence Directorate, to coordinate with Army Cyber Command and Second Army and the Network Enterprise Technology Command to establish and implement procedures Army-wide. The Commander stated that (b) (7)(E)

(b) (7)(E) He also stated that the report did not identify (b) (7)(E)

(b) (7)(E) . He stated that DoD Manual 5200.01, volume 3,³⁹ (b) (7)(E)

(b) (7)(E) The Commander stated that all non-open storage areas were restricted from openly storing classified information. He stated that (b) (7)(E)

(b) (7)(E) complied with the requirements of DoD Manual 5200.01, volume 3. In addition, he stated that 7th SC(T) was awaiting guidance, policy, or procedures from Department of the Army, Intelligence Directorate, (b) (7)(E) In addition, the Commander also stated that 7th SC(T) Intelligence Directorate published a SIPRNet training and maintenance user guide that was available to all 7th SC(T) units.

(U) Our Response

(U) We acknowledge the Commander's comments, but did not redirect the recommendation to a higher-level command because (b) (7)(E) and the NECs need to be involved in developing and implementing corrective actions specific to their organizations.

(U) We agree the report did not specifically identify the areas requiring (b) (7)(E) (b) (7)(E) . We also acknowledge and agree that DoD Manual 5200.01, volume 3⁴⁰ applies only to open storage areas. (b) (7)(E)

(U) ³⁹ DoD Manual 5200.01, volume 3, "DoD Information Security Program: Protection of Classified Information," March 19, 2013.

(U) ⁴⁰ The Commanding General referenced the appendix to enclosure 3, paragraph 3.a.(2).

(U) (b) (7)(E) [REDACTED]
[REDACTED] according to the Defense Information Systems Agency Security Technical Implementation Guide.⁴¹ The areas where we identified deficiencies (b) (7)(E) [REDACTED]
[REDACTED] For example, the (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]

(U) Installation Management Command Comments

(U) Although not required to comment, the Deputy Commanding General, Installation Management Command, stated that (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]. In addition, the Deputy Commanding General stated (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]. The Deputy Commanding General recommended redirecting the recommendations to other responsible commands instead of the Garrison Commanders based on requirements in Army Regulations 380-5, "Department of the Army Information Security Program," September 29, 2000, and 25-1, "Army Information Technology," June 25, 2013.

(U) Our Response

(U) Although the Deputy Commanding General suggested removing Garrison Commanders from the recommendations and redirecting them to other commands, we did not remove the Garrison Commanders from the recommendations. We acknowledge that the Garrison Commanders (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]. In responding to a draft of this report, the Garrison Commander, (b) (7)(E) [REDACTED]
[REDACTED]. In addition, the Commanding General, Operations, Army Cyber Command and Second Army, provided comments on a draft of the report stating that the command would ensure subordinate commands and organizations implemented corrective actions within (b) (7)(E) [REDACTED] of the date of the final report.

(U) ⁴¹ Defense Information Systems Agency, "Access Control In Support Of Information Systems," Security Technical Implementation Guide, version 2, release 3, October 29, 2010.

(U) Army Cyber Command and Second Army Comments

~~(FOUO)~~ Although not required to comment, the Deputy Commanding General, Operations, Army Cyber Command and Second Army, stated that Army Cyber Command and Second Army would take necessary actions to ensure subordinate commands implemented the recommendations requiring NECs to coordinate with Garrison Commanders within (b) (7)(E) of the date of the final report. In addition, the Deputy Commanding General stated (b) (7)(E) that should be addressed by the Commander, Installation Management Command.

(U) Our Response

~~(FOUO)~~ We commend Army Cyber Command and Second Army for taking the lead in ensuring corrective actions are taken to address the reported deficiencies. We also agree (b) (7)(E) that require higher-level command assistance to correct.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from September 2015 through May 2016 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 reviewed the Land Warrior Network managed by 7th SC(T) and locations independent of Land Warrior Network. We nonstatistically selected a sample of seven Army locations (b) (7)(E)

(b) (7)(E) to determine whether Army commands properly implemented logical and physical security safeguards to protect SIPRNet access points. The locations chosen represented different SIPRNet management structures. We reviewed logical and physical security safeguards at each location and the certification and accreditation packages for each network.

(U) We interviewed personnel at:

- (U) Army Chief Information Officer/G6 to discuss SIPRNet responsibilities;
- (U) Army Cyber Command and Second Army to discuss SIPRNet (b) (7)(E) ;
- (U) Army Network Enterprise Technology Command to discuss SIPRNet management and responsibilities;
- (U) 7th SC(T) to discuss SIPRNet management;
- (U) (b) (7)(E) to discuss (b) (7)(E) ;
- (U) Regional NEC at (b) (7)(E) to discuss (b) (7)(E) ; and

- (U) (b) (7)(E) [REDACTED]
[REDACTED] (b) (7)(E) [REDACTED]
[REDACTED] (b) (7)(E) [REDACTED]
[REDACTED], and required security training.

At the locations visited, we performed various tests, to include:

- (U) observing physical security for SIPRNet access points;
- (U) performing control tests for write privileges, background checks, and the completion of DD Form 2875, DD Form 2842, and nondisclosure agreements; and
- (U) selecting a random⁴² sample of accounts to perform control tests as follows:
 - (U) 42 accounts from a universe of [REDACTED] SIPRNet accounts at (b) (7)(E) [REDACTED];
 - (U) 33 accounts from a universe of [REDACTED] SIPRNet accounts at (b) (7)(E) [REDACTED];
 - (U) 44 accounts from a universe of [REDACTED] SIPRNet accounts at (b) (7)(E) [REDACTED];
 - (U) 43 accounts from a universe of [REDACTED] SIPRNet accounts at (b) (7)(E) [REDACTED] and (b) (7)(E) [REDACTED];
 - (U) 21 accounts from a universe of [REDACTED] SIPRNet accounts at (b) (7)(E) [REDACTED]; and
 - (U) 35 accounts from a universe of [REDACTED] SIPRNet accounts at (b) (7)(E) [REDACTED];

(U) ⁴² We randomized the universe to reduce bias during sample selection.

(U) These decision rules applied for our control tests: if the sample had no errors, the control passed. If the sample had one or more errors, the control failed. For our control tests we used the sample size given in Figure 3 of the Journal of Public Inquiry, Fall/Winter 2012-2013, "Statistical Sampling: Choosing the Right Sample Size."⁴³

(FOUO) (b)(7)(E)

(U) In addition, we tested whether the DD Forms 2875 were appropriately completed and approved by verifying whether:

- (U) the user, IA Officer, and security manager signed the form;
- (U) IA training was completed within a year of the IA manager signature; and
- (U) boxes were checked to confirm that the user had a need-to-know and authorized access.

(U) Furthermore, we tested whether DD Forms 2842 were appropriately completed and approved by verifying that the user and registration official signed and dated the form.

To determine whether the NECs (b)(7)(E)

(U) ⁴³ Journal of Public Inquiry, Fall/Winter 2012-2013, "Statistical Sampling: Choosing the Right Sample Size," Figure 3: The Population and the Sample Size for Internal Control Test, Dr. Kandasamy Selvavel and James Hartman Jr.

(U) Use of Computer-Processed Data

(FOUO) We used computer-processed data from the Assured Compliance Assessment Solution, a DoD tool managed by Defense Information Systems Agency in coordination with the Army Network Enterprise Technology Command. We obtained and analyzed Assured Compliance Assessment Solution vulnerability scans from (b) (7)(E) [REDACTED]. We used the data to determine whether commands (b) (7)(E) [REDACTED]. The Assured Compliance Assessment Solution tool (b) (7)(E) [REDACTED]. We interviewed personnel from (b) (7)(E) [REDACTED] included in the vulnerability scans. We determined that Assured Compliance Assessment Solution vulnerability scans were sufficiently reliable for the purpose of this report.

(FOUO) (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(FOUO) We obtained and analyzed data from the Joint Personnel Adjudication System to determine whether personnel obtained background checks and signed nondisclosure agreements. We interviewed security managers about the data contained in the Joint Personnel Adjudication System and observed the managers querying the data. We determined that these data were sufficiently reliable for the purpose of this report.

(U) Use of Technical Assistance

(U) We obtained support from the DoD Office of Inspector General Quantitative Methods Division to develop a random sample for review. We obtained support from the DoD Office of Inspector General Technical Assessment Directorate to define SIPRNet access points.

(U) Prior Coverage

(U) No prior coverage has been conducted on Army SIPRNet access points during the last 5 years.

(U) Appendix B

(U) Transition to Risk Management Framework

(U) The networks we reviewed were granted authorizations to operate under DIACAP. The authorizations were valid for up to 3 years until the networks were recertified. According to the RMF,⁴⁴ system owners were required to develop a strategy and schedule for transitioning to RMF if a system had a current DIACAP or equivalent accreditation decision or if the system owners began executing the DIACAP Implementation Plan. The schedule for transitioning to RMF must not exceed the system reauthorization timeline. The authorizations to operate at each of the Army locations visited were valid under DIACAP as follows:

- (U) (b) (7)(E) - April 1, 2016;
- (U) (b) (7)(E) - August 14, 2016;
- (U) (b) (7)(E) - November 12, 2017;
- (U) (b) (7)(E) - July 16, 2017;⁴⁵
- (U) (b) (7)(E) - April 19, 2018; and
- (U) (b) (7)(E) - November 13, 2017.

(U) ⁴⁴ DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014.

(U) ⁴⁵ (b) (7)(E) and (b) (7)(E) are both included in (b) (7)(E) Authorization to Operate.

(U) Appendix C

(U) Control Test Results of System Access Forms

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

(U) At (b) (7)(E) we received and reviewed all 42 requested DD Forms 2875 or the similar form (b) (7)(E) officials stated they used FH Form 25-29-R-E, "User Access Request and Responsibilities Statement," before the DD Form 2875 was created). Of the 42 forms reviewed, 5 were properly completed and 37 had errors. Specifically:⁴⁶

- (U) 15 forms were missing the initial IA training date;
- (U) 4 forms were not signed by the user;
- (U) 6 forms were signed by the IA manager before the user signed the form;
- (U) 9 forms were missing an IA manager signature;
- (U) 1 form was signed by the IA manager over a year after the user signed the form;
- (U) 30 forms were missing a security manager signature;
- (U) 20 forms did not indicate that access to classified information was required; and
- (U) 16 forms did not indicate that the user had a need-to-know.

(U) At (b) (7)(E) we received and reviewed 31 of the 42 requested DD Forms 2842. Of the 31 forms reviewed, 4 were properly completed and 27 had errors. Specifically, 27 were not witnessed by the registration official as required.

(U) ⁴⁶ Some forms had multiple errors, so the total number of individual errors may not equal the total number of forms with errors.

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

(U) At (b) (7)(E) we received and reviewed 35 of the 35 requested DD Forms 2875. Of the 35 forms reviewed, 26 were properly completed and 9 had errors. Specifically:

- (U) 1 form did not have a date with the user signature;
- (U) 1 form was missing the security manager signature;
- (U) 2 forms included initial IA training dates that were after the date the user signed the form; and
- (U) 5 forms did not indicate that the user had a need-to-know.

(U) At (b) (7)(E) we received and reviewed 32 of the 35 requested DD Forms 2842. Of the 32 forms reviewed, 31 were properly completed and 1 had an error. Specifically, the registration official signed the form on a different day than the user.

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

(U) At (b) (7)(E) we did not receive any of the 33 requested DD Forms 2875 so we could not assess their completeness or accuracy.

(U) At (b) (7)(E) we received 29 of the 33 requested DD Forms 2842. Of the 29 forms reviewed, 7 were properly completed and 22 had errors. Specifically:

- (U) 1 form was not filled out until after we arrived onsite on January 4, 2016; and
- (U) 21 forms were not witnessed by the registration official as required. Specifically:
 - (U) 1 form was not signed by the registration official;
 - (U) 2 forms were signed 2 months after the user signed the form and not until after we arrived onsite on January 4, 2016; and
 - (U) 18 forms were signed 1 or more days after the user signed the form.

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

(U) At (b) (7)(E) we received and reviewed 23 of the 44 requested DD Forms 2875. Of the 23 forms reviewed, 7 were properly completed and 16 had errors. Specifically:

- (U) 7 forms did not pertain to classified information systems (1 form had “classified” and “SIPRNet” access hand-written on the mostly-typed form);
- (U) 2 forms did not indicate that the user had a need-to-know;
- (U) 1 form was not signed by the IA officer;
- (U) 1 form included an initial IA training date that was after the date the user signed the form; and
- (U) 8 forms were signed by the IA officer after we arrived onsite.

(U) At (b) (7)(E) we received and reviewed 18 of the 44 requested DD Forms 2842. Of the 18 forms reviewed, all were properly completed.

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

(U) At (b) (7)(E), we received and reviewed 21 of the 21 requested DD Forms 2875. Of the 21 forms reviewed, 18 were properly completed and 3 had errors. Specifically:

- (U) 1 form included an IA training date that was more than a year before the user signed the form; and
- (U) 2 forms did not indicate that the user had a need-to-know.

(U) At (b) (7)(E), we received and reviewed 19 of the 21 requested DD Forms 2842. Of the 19 forms reviewed, 8 were properly completed and 11 had errors. Specifically:

- (U) 1 form was not signed until after we received the sample of users on February 3, 2016;

- (U) 2 forms were not signed by the registration official to witness the user's signature; and
- (U) 8 forms were signed by the registration official on a different day than the user.

(U)

(b) (7)(E)

(U) At (b) (7)(E), we received and reviewed 8 of the 43 requested DD Forms 2875. Of the 8 forms reviewed, none were properly completed. Specifically, all 8 forms were for access to unclassified systems and not the SIPRNet.

(U) At (b) (7)(E) we received and reviewed 11 of the 43 requested DD Forms 2842. Of the 11 forms reviewed, 9 were properly completed and 2 had errors. Specifically, one form was not signed by the user and the other form was signed by the registration official on a different day than the user.

(U) Appendix D

(U) Control Test Results of Required Security-Related Training

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

(U) At (b) (7)(E) we requested training records for all 42 users in the sample. We found:

- (U) 1 user did not complete initial IA training and 7 users did not properly complete initial IA training,
- (U) all users completed annual IA training,
- (U) 1 user completed initial security awareness training,
- (U) all users completed annual security awareness training, and
- (U) 11 users did not complete the NATO briefing properly.

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

(U) At (b) (7)(E) we requested training records for all 35 users in the sample. We found:

- (U) all users completed initial IA training,
- (U) all users completed annual IA training,
- (U) 12 users did not complete initial security awareness training,
- (U) all users complete annual security awareness training, and
- (U) none of the users completed the NATO briefing.

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

(U) At (b) (7)(E) [REDACTED] we requested training records for all 33 users in the sample.

We found:

- (U) (b) (7)(E) [REDACTED] could not provide training records to support that users complete initial IA training before being granted SIPRNet access,
- (U) all users completed annual IA training,
- (U) 25 users did not complete initial security awareness training and 6 users did not properly complete initial security awareness training,
- (U) 18 users did not complete annual security awareness training and 8 users did not properly complete annual security awareness training, and
- (U) 15 users did not complete the NATO briefing and 12 users did not properly complete the NATO briefing.

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

(U) At (b) (7)(E) [REDACTED], we requested training records for all 44 users in the sample.

We found:

- (U) (b) (7)(E) [REDACTED] could not provide training records to support that users complete initial IA training before being granted SIPRNet access,
- (U) 24 users did not complete annual IA training,
- (U) 21 users did not complete initial security awareness training,
- (U) 37 users did not complete annual security awareness training, and
- (U) 17 users did not complete the NATO briefing.

(U)

(b) (7)(E)

(U) At (b) (7)(E), we requested training records for all 21 users in the sample. We found:

- (U) all users completed initial IA training,
- (U) all users completed annual IA training,
- (U) none of the users completed initial security awareness training,
- (U) 1 user did not properly complete annual security awareness training, and
- (U) 1 user did not complete the NATO briefing and 1 user did not properly complete the NATO briefing.

(U)

(b) (7)(E)

(U) At (b) (7)(E), we requested training records for all 43 users in the sample. We found:

- (U) none of the users completed initial IA training,
- (U) 30 users did not complete annual IA training,
- (U) 36 users did not complete initial security awareness training and 1 user did not properly complete initial security awareness training,
- (U) 34 users did not complete annual security awareness training and 3 users did not properly complete annual security awareness training, and
- (U) 32 users did not complete the NATO briefing and 6 users did not properly complete the NATO briefing.

(U) Appendix E

(U) Criteria

(U) We used the following guidance throughout the audit.

(U) National Security Telecommunications and Information Systems Security Committee

(U) National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems," December 13, 1996, outlines the approval authority, standards, and guidance for PDS design, installation, and maintenance.

(U) Chairman of the Joint Chiefs of Staff

(U) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, provides joint policy and responsibilities for IA and support to computer network defense.

(U) DoD

(U) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, provides guidance for reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other Federal agencies, for the authorization and connection of information systems.

(U) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007, establishes a certification and accreditation process to implement IA capabilities and services and provide visibility over accreditation decisions for operating DoD information systems. This instruction was reissued and renamed the RMF.

(U) DoD Manual 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, implements policy, assigns responsibilities, and provides procedures for designating, marking, protecting, and disseminating controlled unclassified information and classified information. DoD Manual 5200.01, volume 3, "DoD Information Security Program: Protection of Classified Information," March 19, 2013, provides guidance for safeguarding, storing, destroying, transmitting, and transporting classified information and identifies security education and training requirements and processes for handling security violations and compromised classified information.

(U) Army

(U) Army Regulation 25-2 "Information Assurance," March 23, 2009, establishes IA policy, roles, and responsibilities.

(U) Defense Information Systems Agency

(U) Defense Information Systems Agency "Enclave" Security Technical Implementation Guide, Version 4, Release 4, January 9, 2014, provides assistance to meet minimum requirements, standards, controls, and options for securing an enclave as a whole and provides technical guidance to secure specific enclave components in detail.

(U) Defense Information Systems Agency, "Access Control in Support of Information Systems," Security Technical Implementation Guide, Version 2, Release 3, October 29, 2010, provides details for a security framework to use when planning and selecting access controls for protecting DoD sensitive and classified information. It provides background and context for access control issues including the process of identifying, authenticating, and authorizing access to protected assets.

~~SECRET~~

Management Comments

(U) Management Comments

(U) 7th Signal Command (Theater) Comments

UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, 7TH SIGNAL COMMAND (THEATER)
423 22ND STREET - BUILDING 21715
FORT GORDON, GEORGIA 30905-5832

NETC-SFC-CG

7 July 2016

MEMORANDUM THRU Commanding General, U.S. Army Network Enterprise
Technology Command, 2133 Cushing Street, Fort Huachuca, AZ 85613-7070

THRU Commanding General, U.S. Army Cyber Command and Second Army, 8825
Beulah Street, Fort Belvoir, VA 22350-1500

FOR Director, Department of Defense, Office of Inspector General, 4800 Mark Center
Drive, Alexandria, VA 22350-1500

SUBJECT: 7TH SC(T) Command Reply to the SIPRNet Access Points Audit Report

1. References.

a. (U) Memorandum, Department of Defense Office of Inspector General (DoDIG),
Alexandria, VA, 24 May 16, Subject: Command Comments to Draft Report on Army
Commands Need to Improve Logical and Physical Security Safeguards That Protect
SIPRNet Access Points

b. (U) Memorandum, U.S. Army Cyber Command and Second Army, Fort Belvoir,
VA, 27 Jun 16, Subject: Draft Report on Army Commands Need to Improve Logical and
Physical Security Safeguards That Protect SIPRNet Access Points

2. (U) Purpose. The 7TH Signal Command (Theater) Command provides a response to
DoDIG findings and recommendations in the enclosure.

3. (U) Audit Objective. To determine whether the Army effectively protected SECRET
Internet Protocol Router Network (SIPRNet) access points. The DoDIG sampled the
security safeguards protecting SIPRNet access points at selected Army locations.

4. (U) Responsible agencies:

a. (U) The DoDIG Audit Team incorrectly identified the responsible agency for
several recommendations. Additionally, the team directed recommendations to a level
that would only affect one installation. The goal of the audit was to improve safeguards
across the Army.

UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE

Report No. DODIG-2016-119 | 62

~~SECRET~~

~~SECRET~~

Management Comments

(U) 7th Signal Command (Theater) Comments (cont'd)

UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE

NETC-SFC-CG

SUBJECT: 7th SC(T) Command Reply to the SIPRNet Access Points Audit Report

b. (U) In accordance with Reference b, the 7th Signal Command (Theater) agrees with, and defers to Army Cyber Command's comments. The DoDIG recommendations should target Command-level organizations to address identified problems throughout the Army. The enclosure outlines specific details.

5. (U) The 7th Signal Command (Theater) will direct corrective actions to subordinates for appropriate implementation.

6. (U) The 7th Signal Command (Theater) will provide oversight to ensure enforcement of procedures for SIPRNet accountability and protection.

7. (U) My point of contact is [REDACTED]

(b) (6)

Encl: 7th SC(T) Command Reply to [REDACTED]

CF
NETCOM Internal Review Section
7th SC(T) ACofS G3
7th SC(T) ACofS G2

2

UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE

Report No. DODIG-2016-119 | 63

~~SECRET~~

~~SECRET~~

Management Comments

(U) 7th Signal Command (Theater) Comments (cont'd)

Final Report
Reference

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

7th Signal Command Reply to:

DoDIG Draft Report on Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points

DoDIG Audit Objective

(U) Determine whether the Army effectively protected SECRET Internet Protocol Router Network (SIPRNet) access points. DoDIG sampled the security safeguards protecting SIPRNet access points at selected Army locations.

DoDIG Findings and Recommendations

FINDINGS-A: DoDIG identified Army-wide internal control weaknesses for managing SIPRNet circuits:

- (U) (b) (7)(E)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U) SIPRNet user access request forms were not completed, or completed incorrectly
- (U) Required initial and refresher Security Training was not conducted or completed
- (U) (b) (7)(E)

DoDIG recommendations for Commanding General, 7th Signal Command (Theater)

Recommendation A-2

(U) Army Chief Information Officer, in coordination with the Commander, 7th Signal Command (Theater), establish and implement procedures to identify who owns each SIPRNet circuit and the Component responsible for managing and securing each circuit.

Renumbered as
Recommendation A.2.a

Command Comments

(U) Concur with DoDIG finding, but not Recommendation A-2. DISA, Army CIO/G6 and ARCYBER/2A have visibility of all Army circuits. 7th SC(T) has visibility of circuits owned by the Network Enterprise Centers. 7th SC(T) (b) (7)(E)

~~SECRET~~

~~SECRET~~

(U) 7th Signal Command (Theater) Comments (cont'd)

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

Recommendation A-3

(U) Commander, Network Enterprise and Technology Command (NETCOM), in coordination with the (b) (7)(E) [REDACTED]
(b) (7)(E) [REDACTED]
(b) (7)(E) [REDACTED]

a. (U) develop and implement procedures to verify that personnel and contractors requesting SIPRNet access complete initial and annual security related training and the North Atlantic Treaty Organization briefing as a condition for obtaining and maintaining access; and

b. (U) implement a process to identify and retain training records for personnel to support the requirements for accessing the SIPRNet.

Command Comments

(U) Concur with DoDIG finding, but not Recommendation A-3. Address recommendations to ARCYBER or NETCOM, in coordination with the Theater Signal Commands. The 7th SC(T) will confirm and enforce established procedures/processes in the CONUS Theater.

a. (U) 7th SC(T) has procedures for verification of required training and directs compliance for existing requirements for the sites and organizations. 7th SC(T) processes all requests for network access (DD2875) for the (b) (7)(E) [REDACTED] regardless of the network, through the 7th SC(T) G2 Security office for validation of security clearance eligibility. The standing process at the Command level ensures completion of all security related training. This training includes annual Security Refresher Training, biennial Derivative Classification Training and NATO Awareness upon arrival and in-processing the unit.

b. (U) 7th SC(T) G2 Security retains records of completed security related training. The HHC Training element retains the (b) (7)(E) [REDACTED] training records. 7th SC(T) directed the use of the Army Training and Certification Tracking System (ATCTS) for tracking required training for access to networks. 7th SC(T) will ensure subordinate organizations comply with the existing requirement.

Recommendation A-4

(U) Commander, 7th Signal Command (Theater), verify whether subordinate commands implemented a SIPRNet (b) (7)(E) [REDACTED]
(b) (7)(E) [REDACTED]

Command Comments

(U) Concur with DoDIG Recommendation A-4. 7th SC(T) issued an order requiring the (b) (7)(E) [REDACTED]
(b) (7)(E) [REDACTED]

~~SECRET~~

Management Comments

(U) 7th Signal Command (Theater) Comments (cont'd)

Final Report
Reference

Unsolicited
Comments to
Recommendations A.6,
A.7, A.9, A.10,
and A.12

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

Recommendation A-6

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

Command Comments

(U) Concur with the DoDIG finding, but not Recommendation A-6. Address recommendations to ARCYBER/2A, in coordination with NETCOM and the Theater Signal Commands to establish and implement procedures Army-wide.

(U) The 7th SC(T) and subordinate organizations (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Command is transitioning to (b) (7)(E)
(b) (7)(E)

The

Recommendation A-7

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

a. (U) (b) (1), EO 13526, sec. 1.4(g)
(b) (1), EO 13526, sec. 1.4(g)

b. (U) (b) (1), EO 13526, sec. 1.4(g)
(b) (1), EO 13526, sec. 1.4(g)

c. (U) (b) (7)(E)

d. (U) develop and implement procedures to verify that access forms are properly completed before granting access to the SIPRNet.

Command Comments

(U) Concur with DoDIG finding, but not Recommendation A-7. Address recommendations to ARCYBER/2A, in coordination with NETCOM and the Theater Signal Commands to establish and implement procedures Army-wide.

a. and b. (S) 7th SC(T) Regulation 25-2 contains the program framework for vulnerability management and associated procedures to correct and mitigate vulnerabilities;

c. (U) See Recommendation A-6 Command Comments.

d. (U) 7th SC(T) G2 validates Security Clearance and Access eligibility as part of the access form completion.

~~SECRET~~

~~SECRET~~

~~SECRET~~

Management Comments

(U) 7th Signal Command (Theater) Comments (cont'd)

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

Recommendation A-9

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

a. (U) (b) (7)(E)

(b) (7)(E)

b. (U) (b) (7)(E) as required by DoD guidance;

(b) (7)(E)

c. (U) (b) (7)(E) as required by DoD guidance, and (b) (7)(E) as required by Army guidance;

(b) (7)(E)

d. (U) (b) (7)(E) and

e. (U) develop and implement procedures to verify that access forms are properly completed before granting access to the SIPRNet.

Command Comments

(U) Concur with DoDIG finding, but not Recommendation A-9. Address recommendations to ARCYBER/2A, in coordination with NETCOM to establish and implement procedures Army-wide.

Recommendation A-10

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

develop and implement procedures to verify that access forms are properly completed before granting access to the SIPRNet.

Command Comments

(U) Concur with DoDIG Recommendation A-10. NOTE: 7th SC(T) ACofS, G2 validates user Security Clearance and Access eligibility as part of the form completion.

Recommendation A-12

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

a. (U) (b) (7)(E)

(b) (7)(E) as required by DoD guidance;

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

(b) (7)(E) as required by DoD guidance, and (b) (7)(E) as required by Army guidance; and

c. (U) develop and implement procedures to verify that access forms are properly completed before granting access to the SIPRNet.

~~SECRET~~

~~SECRET~~

(U) 7th Signal Command (Theater) Comments (cont'd)

**Final Report
Reference**

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

Command Comments

(U) Concur with DoDIG finding, but not Recommendation A-12. Combine recommendation with Recommendation A-9; and address to ARCYBER/2A, in coordination with NETCOM to establish and implement procedures Army-wide.

FINDINGS-B: DoDIG found:

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

DoDIG recommendations for Commanding General, 7th Signal Command (Theater)

Recommendation B-1

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

a. (U) (b) (7)(E)

(b) (7)(E) and

b. (U) develop and implement a training program to ensure personnel understand their responsibilities (b) (7)(E)

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency. Address Recommendation B-1 to Department of Army (DA) G2, in coordination with ARCYBER/2A and NETCOM to establish and implement procedures Army-wide.

a. (U) (b) (7)(E)

(b) (7)(E)

**Renumbered as
Recommendations B.3.a
and B.3.b and
Recommendations B.4.a
and B.4.b**

**Unsolicited
Comments to
Recommendations B.1
to B.7**

~~SECRET~~

Management Comments

(U) 7th Signal Command (Theater) Comments (cont'd)

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

b. (U) Current references include multiple DoD references within DISA Security Technical Implementation Guides (STIGs). Awaiting any DA G2 produced guidance, policy, or procedures (b)(7)(E)

NOTE: (U) 7th SC(T) G2 published a SIPRNet Training and Maintenance user guide; available via email, 7th SC(T) SharePoint portal, or hard copy to all 7th SC(T) units.

Recommendation B-2

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

a. (U) (b)(7)(E)
(b)(7)(E)

and

b. (U) develop and implement a training program to ensure personnel understand their responsibilities (b)(7)(E)

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency. See Command Comments for Recommendation B-1.

Recommendation B-3

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

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency. See Command Comments for Recommendation B-1.

Recommendation B-4

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

develop and implement a training program to ensure personnel understand their responsibilities (b)(7)(E)

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency. See Command Comments for Recommendation B-1.

~~SECRET~~

**Final Report
Reference**

**Renumbered as
Recommendations B.1.a
and B.1.b**

**Renumbered as
Recommendation B.7**

**Renumbered as
Recommendation B.2**

~~SECRET~~

~~SECRET~~

Management Comments

(U) 7th Signal Command (Theater) Comments (cont'd)

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

Recommendation B-5

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

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency. See Command Comments for Recommendation B-1.

Recommendation B-6

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

a. (U) (b) (7)(E) as
required by Federal guidance; and

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

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency.

a. (U) Per CNSSI 7003, dated Sep 2015, (b) (7)(E)
(b) (7)(E)

b. (U) Awaiting any DA G2 produced ARMY guidance covering policies and
procedures (b) (7)(E)
(b) (7)(E)

Recommendation B-7

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

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency. See Command Comments for Recommendation B-1.

~~SECRET~~

**Final Report
Reference**

**Renumbered as
Recommendation B.7**

**Renumbered as
Recommendations B.5.a
and B.5.b**

**Renumbered as
Recommendation B.6**

~~SECRET~~

~~SECRET~~

Management Comments

(U) 7th Signal Command (Theater) Comments (cont'd)

~~SECRET~~

Enclosure to 7th SC(T) Reply Memorandum to the SIPRNet Access Point Audit

Recommendation B-8

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

Command Comments

(U) Non-Concur with DoDIG recommended responsible agency. See Command Comments for Recommendation B-6.

Final Report
Reference

Renumbered as
Recommendation B.4.c

Classified by: (b) (6)
Derived from: ~~24 May 2016 - Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points Draft Report~~
Declassify on: 24 May 26
Date of source: 24 May 10

~~SECRET~~

~~SECRET~~

~~SECRET~~

Management Comments

(U) Program Executive Officer Enterprise Information Systems Comments



REPLY TO
ATTENTION OF

UNCLASSIFIED
DEPARTMENT OF THE ARMY
OFFICE OF THE PROGRAM EXECUTIVE OFFICER
ENTERPRISE INFORMATION SYSTEMS
(PEO EIS)
9350 HALL ROAD
FORT BELVOIR, VIRGINIA 22060-5526

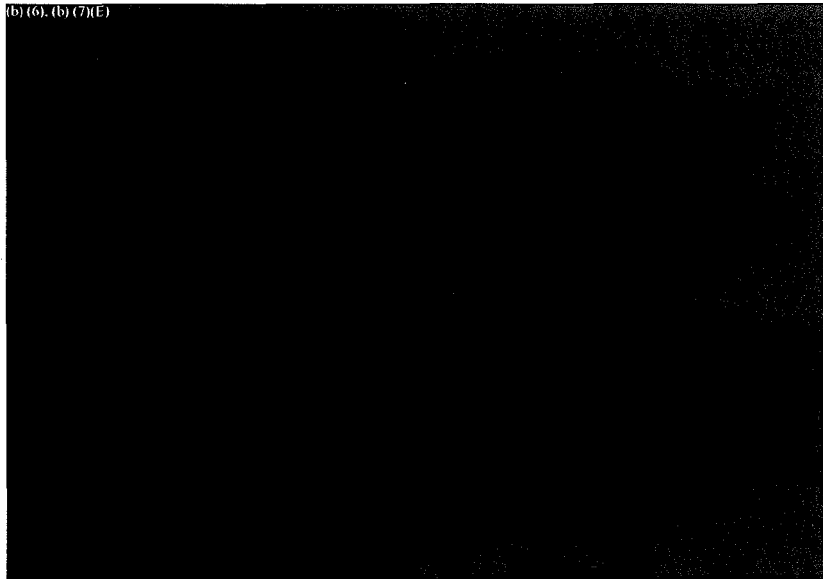
SFAE-PS

24 June 2016

MEMORANDUM FOR RECORD

SUBJECT: Project Lead Acquisition, Logistics, Technology, Enterprise, Systems Services (PL
ALTESS) Plan of Action

(b) (6), (b) (7)(E)

A large rectangular area of the document is completely blacked out, indicating redacted content. The redaction covers the majority of the page's body text.

UNCLASSIFIED

Report No. DODIG-2016-119 | 72

~~SECRET~~

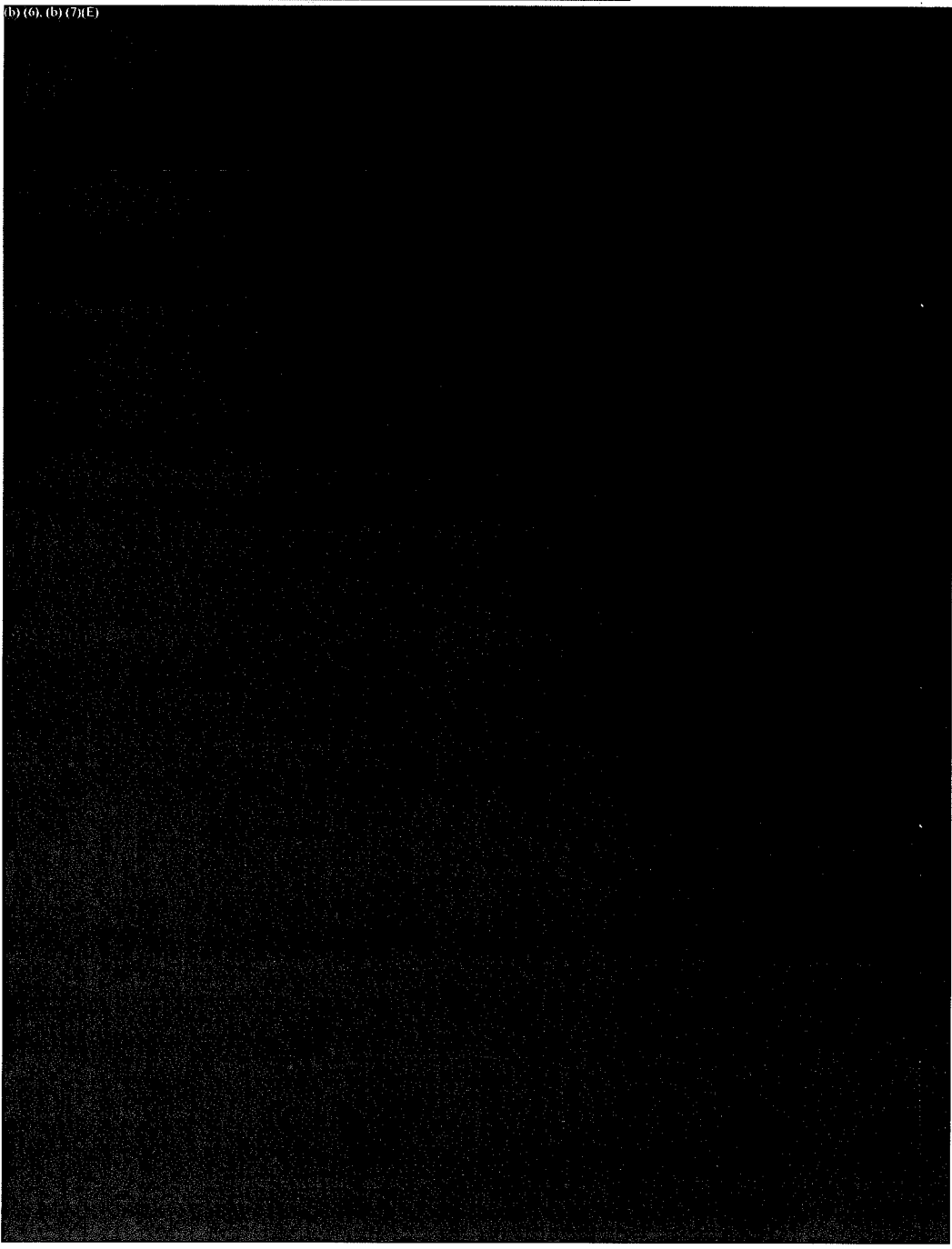
~~SECRET~~

Management Comments

(U)

(b) (7)(E)

(b) (6), (b) (7)(E)

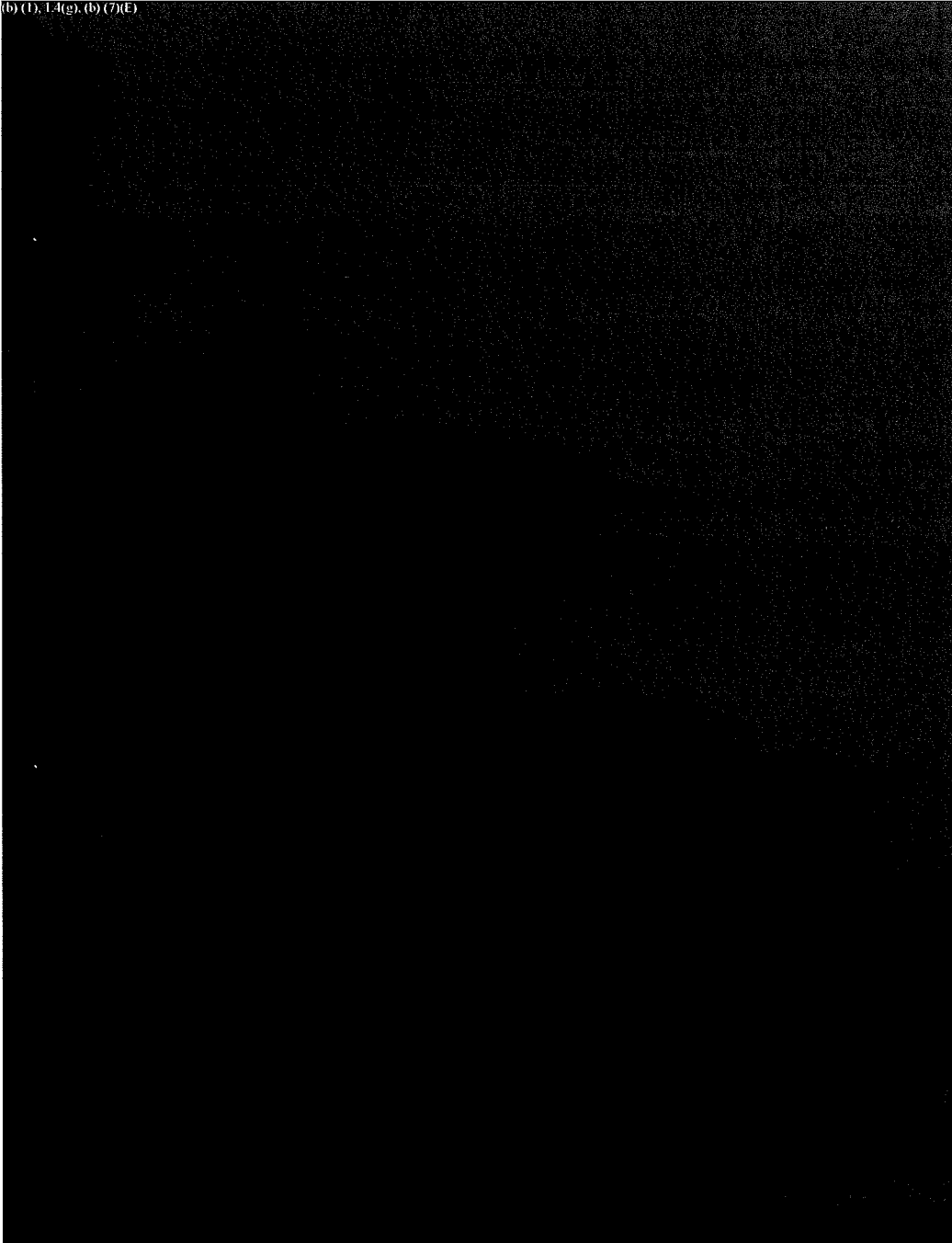


~~SECRET~~

(U)

(b) (7)(E)

(b) (1), 1.4(g), (b) (7)(E)



~~SECRET~~

Management Comments

(U)

(b) (7)(E)

(b) (7)(E)

**Final Report
Reference**

**Renumbered as
Recommendations B.1.a
and B.1.b**

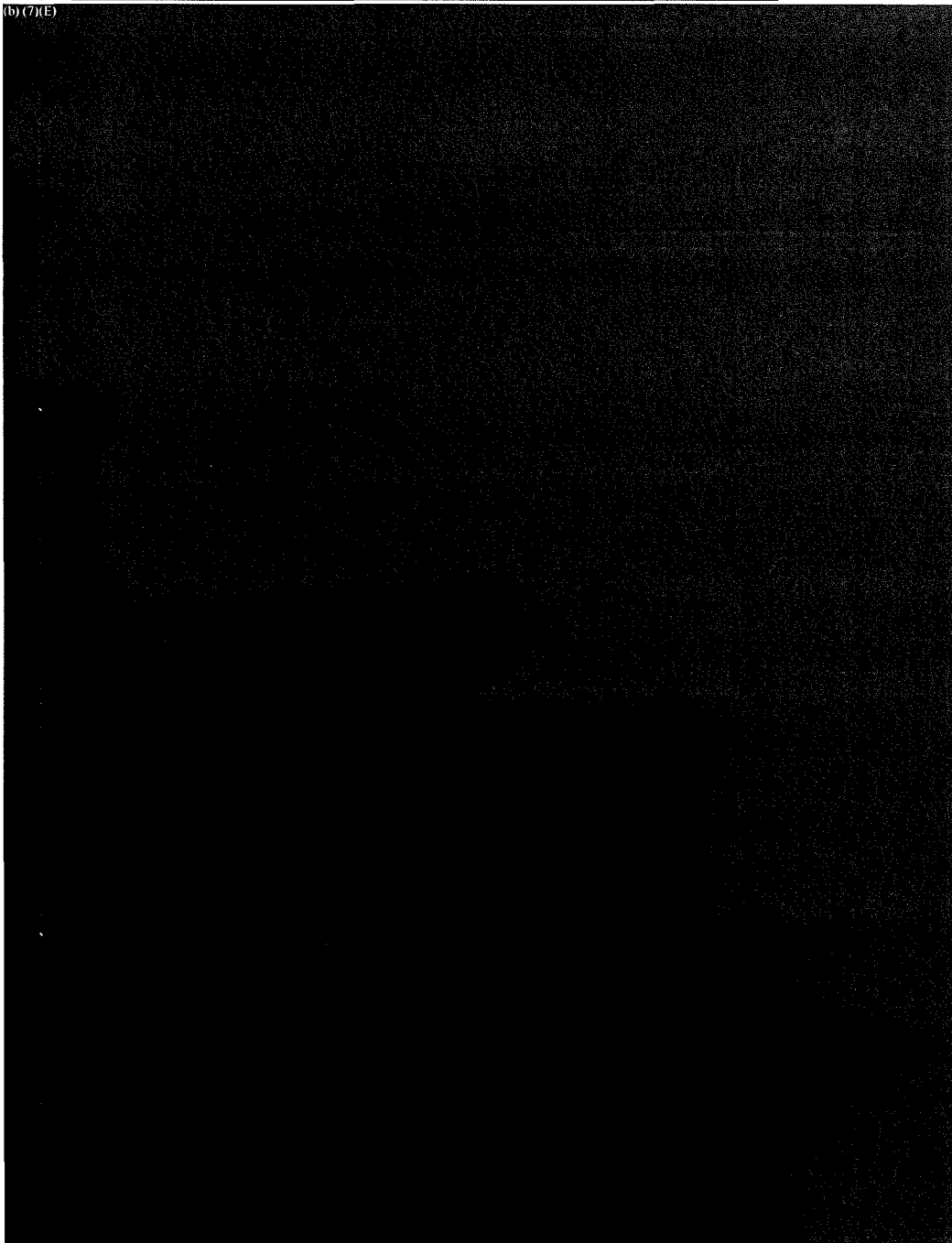
~~SECRET~~

Management Comments

(U)

(b) (7)(E)

(b) (7)(E)



~~SECRET~~

Management Comments

(U) Army Chief Information Officer Comments



Office, Chief Information Officer (IG-6)
SAIS-CB

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

MEMORANDUM FOR Department of Defense (DoD) Inspector General (IG), ATTN: [REDACTED] 4800 Mark
Center Drive, Alexandria, Virginia 22350-1500

SUBJECT: (U//~~FOUO~~) CIO/G-6 Comments to DoDIG Draft Report: "(U) Army
Commands Need to Improve Logical and Physical Security Safeguards that protect
SIPRNet Access Points (Project No. D2015-D000RC-0241.000) dated 24 May 2016

1. (U) HQDA CIO/G-6 appreciates the opportunity to review the draft report on the audit
of logical and physical security safeguards that protect the SIPRNet access points and
concurs with the findings and recommendations with comments.

2. (U) Recommendation A.1 a. requires CIO/G-6 to develop and implement policies and
procedures to (b) (7)(E)
(b) (7)(E)

3. (U//~~FOUO~~) Recommendation A.1.b. requires CIO/G-6 to review the deficiencies
identified in the report, require a thorough review of the Army SECRET Internet Protocol
Router Network security safeguards performed at each command within the Army, and
apply corrective actions as necessary. CIO/G-6 will review the issues, identify policy
gaps, and issue memoranda to resolve the issues. Additionally, CIO/G-6 will coordinate
with ARCYBER/2nd Army to identify and implement corrective actions within (b) (7)(E)
from the date of the final report.

4. (U//~~FOUO~~) Recommendation A.2. requires CIO/G-6 to coordinate with the
Commander 7th Signal Command (Theater) establish and implement procedures to
(b) (7)(E)

5. (U) The point of contact for this action is [REDACTED]

(b) (6)

Acting U.S. Army Cybersecurity Director

Final Report
Reference

Renumbered as
Recommendation A.1

Renumbered as
Recommendation A.2.b

Renumbered as
Recommendation A.2.a

~~SECRET~~

(U)

(b) (7)(E)

(b) (7)(E)

[REDACTED]

~~SECRET~~

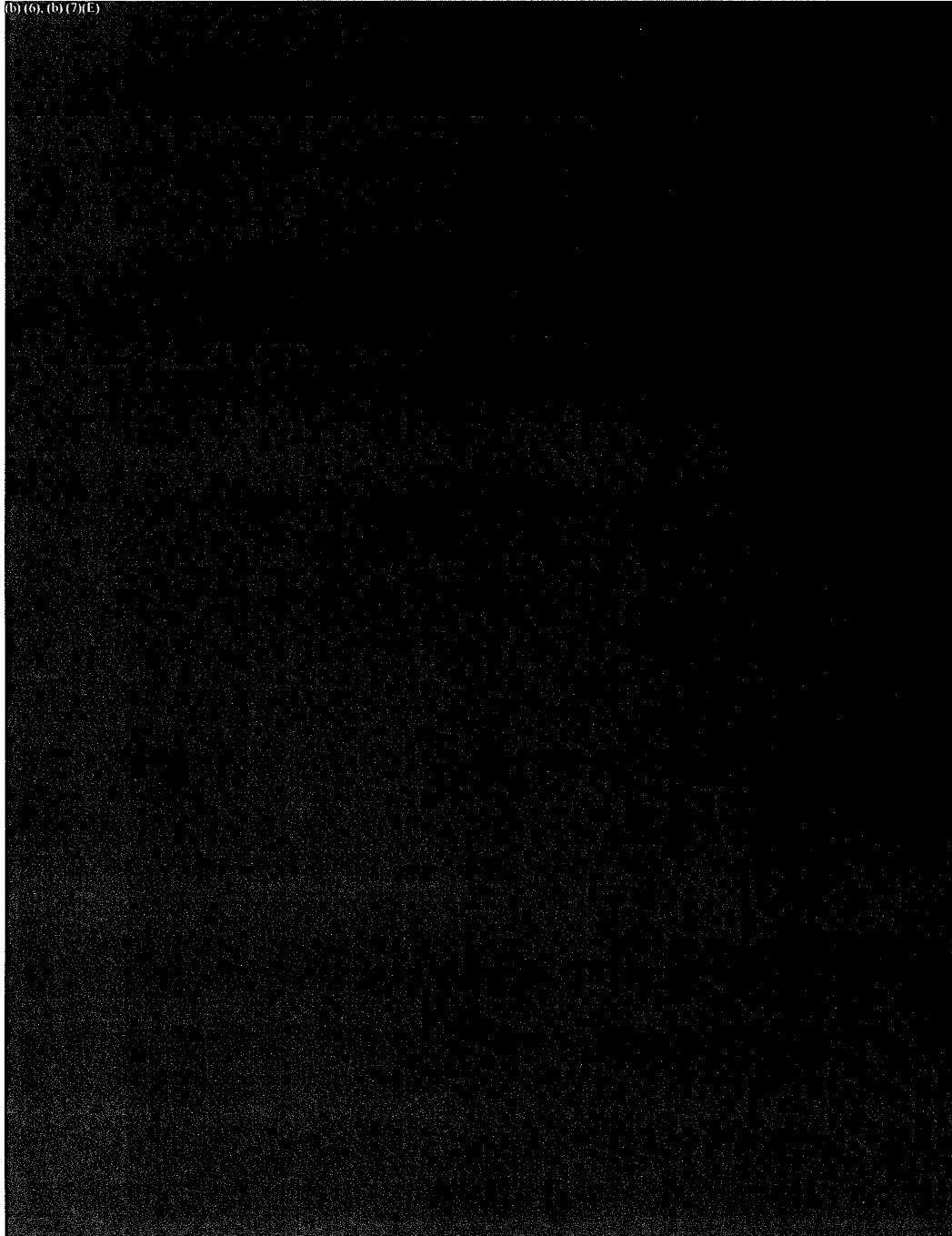
Management Comments

(U)

(b) (7)(E)



(b) (6), (b) (7)(E)



**Final Report
Reference**

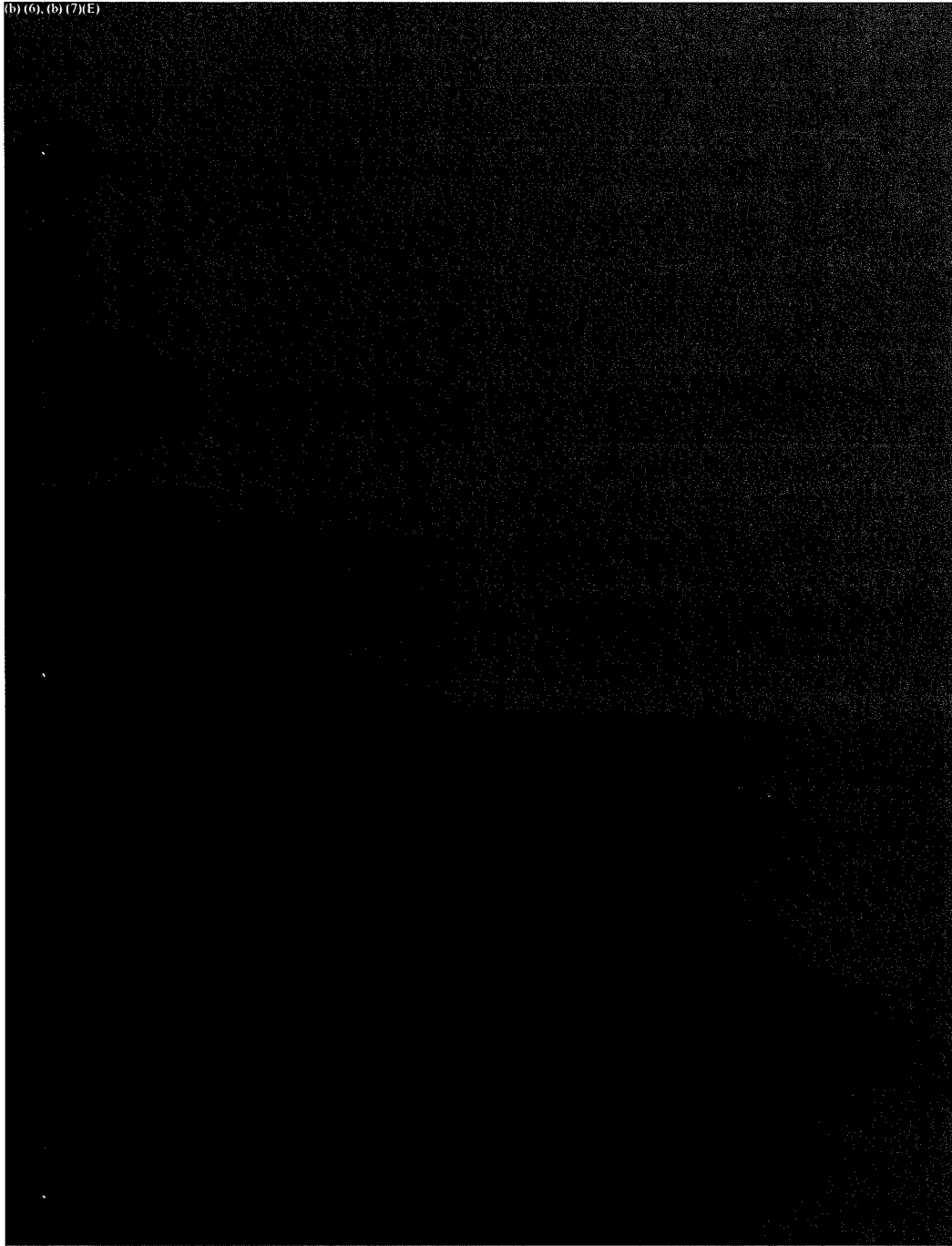
**Renumbered as
Recommendation B.2**

~~SECRET~~

(U)

(b) (7)(E)

(b) (6), (b) (7)(E)



~~SECRET~~

Management Comments

(U) US Army Installation Management Command Comments

~~FOR OFFICIAL USE ONLY~~



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
2405 GUN SHED ROAD
JOINT BASE SAN ANTONIO FORT SAM HOUSTON, TX 78234-1223

IMIR

JUN 17 2016

MEMORANDUM FOR Inspector General, Department of Defense, 4800 Mark Center Drive, Alexandria, Virginia 22350-1500

SUBJECT: Draft Report, Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points (D2015-D000RC-0241)

1. I received the subject draft report. The report contains five recommendations directed to subordinate US Army Installation Management Command (IMCOM) Garrison Commanders (encl). IMCOM doesn't have responsibility or own the processes to implement the recommendations. We recommend you redirect the recommendations to the responsible commands. The United States Army Network Enterprise Technology Command (NETCOM), and local Network Enterprise Centers (NECs) implement access controls on SIPR networks. (b)(7)(E)

2. The IMCOM point of contact is [REDACTED]

End
as

LAWARREN V. PATTERSON
Major General, USA
Deputy Commanding General

~~FOR OFFICIAL USE ONLY~~

~~SECRET~~

**(U) US Army Installation Management
Command Comments (cont'd)**

**Final Report
Reference**

**Renumbered as
Recommendations B.3.a,
B.3.b, B.4.a and B.4.b**

**Renumbered as
Recommendation B.7**

**(U) US Army Installation Management
Command Comments (cont'd)**

(b) (7)(E)



~~SECRET~~

Management Comments

(U) Army Cyber Command and Second Army Comments



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF THE ARMY
U.S. ARMY CYBER COMMAND AND SECOND ARMY
8825 BEULAH STREET
FORT BELVOIR, VIRGINIA 22060-5246

ARCC-IR

27 June 2016

MEMORANDUM FOR Department of Defense (DoD) Inspector General (IG) [REDACTED]

SUBJECT: (U//~~FOUO~~) Command Comments to DoDIG Draft Report: "(U) Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points (Project No. D2015-D000RC-0241.000) dated 24 May 2016 (S)

1. (U) U.S. Army Cyber Command (ARCYBER) and Second Army (2A) reviewed the subject draft report and your recommendations. Although no recommendations were directed to the Commander, ARCYBER & 2A, recommendations were directed to our subordinates, the US Army Network Enterprise Technology Command (NETCOM), 7th Signal Command (Theater) (7th SC(T)), [REDACTED] and several Network Enterprise Centers (NECs). In our role as higher headquarters for the aforementioned organizations, we view your findings within our purview to evaluate, respond to, and assist in the execution of corrective actions.

2. (U) We concur with comments.

3. (U) Recommendation A.1.b. is directed to the Army Chief Information Officer (CIO/G6) but states in part "require a thorough review of the Army SECRET Internet Protocol Router Network security safeguards performed at each command within the Army, and apply corrective actions as necessary." The Army CIO/G6 develops policies and policies in this area are needed. [REDACTED] (b)(5), (b)(7)(E)

[REDACTED] ARCYBER.
ARCYBER concurs with this recommendation and in conjunction with the Army Chief Information Officer (CIO/G6) will implement the recommendation within [REDACTED] (b)(7)(E) from the date of the final report.

4. (U) Recommendation A.2. recommends "that the Army Chief Information Officer in coordination with the Commander, 7th Signal Command (Theater), establish and implement procedures to identify [REDACTED] (b)(5), (b)(7)(E)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Final Report
Reference

Renumbered as
Recommendation A.2.b

Renumbered as
Recommendation A.2.a

~~SECRET~~

~~SECRET~~

Management Comments

(U) Army Cyber Command and Second Army Comments (cont'd)

Final Report
Reference

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

ARCC-IR

SUBJECT: (U//~~FOUO~~) Command Comments to DoDIG Draft Report: "(U) Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points (Project No. D2015-D000RC-0241.000) dated 24 May 2016 (S)

(b) (S), (b) (7)(E) [REDACTED] ARCYBER concurs with this recommendation and in conjunction with the Army Chief Information Officer (CIO/G6) will implement the recommendation within (b) (7)(E) from the date of the final report.

5. (U//~~FOUO~~) Recommendation A.3 involves the Commander, NETCOM coordination with NECs and (b) (7)(E) (b) (S), (b) (7)(E) [REDACTED]

(b) (7)(E) [REDACTED] ARCYBER & 2A concurs with this recommendation and will take such actions as may be necessary to ensure that all subordinate elements implement the recommendation within (b) (7)(E) from the date of the final report.

6. (U//~~FOUO~~) Recommendations A.3.a, A.3.b, A.6, A.9.a, A.9.b, A.9.c, A.9.d, A.9.e, A.10, A.12.a, A.12.b, A.12.c, B.1.a, B.1.b, B.3, B.4, B.5, B.6.a, B.6.b, B.7, and B.8 were directed to individual NEC Directors.

a. (U//~~FOUO~~) NEC Directors (b) (S), (b) (7)(E) [REDACTED]

[REDACTED] The Commander, 7th SC(T) is in a much better position to standardize practices and direct the correction of deficiencies.

b. (U//~~FOUO~~) (b) (S) [REDACTED]

c. (U//~~FOUO~~) ARCYBER & 2A concurs with these findings and recommendations; however, disagrees with the recommendation's addressee. ARCYBER & 2A will take such actions as may be necessary to ensure that all subordinate elements implement the recommendations within (b) (7)(E) from the date of the final report.

d. (U//~~FOUO~~) Where the recommendations are for Army Installation Management Command elements (e.g. Garrison Commanders) to "coordinate" with a NEC, we concur with the recommendation as stated and will take such actions as may be necessary to ensure that all subordinate elements implement the recommendations within (b) (7)(E) from the date of the final report.

7. (U//~~FOUO~~) Recommendation A.7 is directed to (b) (7)(E) [REDACTED] ARCYBER & 2A concurs with this recommendation and will take such actions as may be necessary to ensure that all subordinate elements implement the recommendation within (b) (7)(E) from the date of the final report.

2

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Recommendations B.1.a
and B.1.b renumbered
as Recommendations
B.3.a, B.3.b, B.4.a,
and B.4.b;
Recommendation B.3 as
Recommendation B.7;
Recommendation B.4 as
Recommendation B.2;
Recommendation B.5 as
Recommendation B.7;
Recommendations B.6.a
and B.6.b as
Recommendations B.5.a
and B.5.b;
Recommendation B.7 as
Recommendation B.6;
and
Recommendation B.8 as
Recommendation B.4.c

Report No. DODIG-2016-119 | 85

~~SECRET~~

(U) Army Cyber Command and Second Army Comments (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

ARCC-IR

SUBJECT: (U//~~FOUO~~) Command Comments to DoDIG Draft Report: "(U) Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points (Project No. D2015-D000RC-0241.000) dated 24 May 2016 (S)

8. (U//~~FOUO~~) ARCYBER & 2A is concerned that recommendations (b) (7)(E)

[REDACTED]

9. (U//~~FOUO~~) ARCYBER & 2A notes that (b) (7)(E)

[REDACTED]

10. (U//~~FOUO~~) ARCYBER & 2A concurs with the remainder of the report without comment and will ensure corrective actions are directed to the appropriate activities for implementation.

11. (U) If you have any questions, please contact [REDACTED]

CF:
HQDA (SAIS-CB)
HQDA (SAAG-ACFO)

(b) (6)

[REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~SECRET~~

Management Comments

(U) Army Spectrum Management Office Comments

UNCLASSIFIED



DEPARTMENT OF THE ARMY
ARMY SPECTRUM MANAGEMENT OFFICE
6916 COOPER AVE., OPERATIONS BUILDING
FORT MEADE, MD 20755-7901

REPLY TO
ATTENTION OF

SAIS-AOS

6 June 2016

MEMORANDUM FOR DoD Office of Inspector General (OIG)

SUBJECT: FUNDING SUPPORT FOR DoD AF C AZ SIPRNet MODIFICATION

1. I understand that (b) (7)(E) [redacted] was identified in your DoD OIG draft report entitled "Army Commands Need to Improve Logical and Physical Security Safeguards That Protect SIPRNet Access Points" as requiring modification of the SIPRNet Protective Distribution System (PDS).
2. (b) (5), (b) (7)(E) [redacted]
3. [redacted]
4. I would request that the negative finding in the OIG draft report include a statement that the a plan is in place to correct the deficiency.

(b) (6) [redacted]

(b) (6) [redacted]

Army Spectrum Management Office
HQDA CIO/G-6

UNCLASSIFIED

~~SECRET~~

(U) Glossary

(U) **Active Directory.** A special purpose database that is designed to handle a large number of read and search operations. The database is used by network users and administrators to store data.

(U) **Authorization to Operate.** Authorization granted by a designated accrediting authority for a DoD information system to process, store, or transmit information; an Authorization to Operate indicates a DoD information system has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the designated accrediting authority. ATOs may be issued for up to 3 years.

(U) **Boundary Protection.** Monitoring and controlling communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications.

(U) **Category I.** Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumptions of super-user privileges.

(U) **DoD Components.** Combatant commands, Military Services, DoD agencies, and field activities.

(U) **Enclave.** A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

(U) **Firewalls.** Hardware and software that limits access between networks or systems (or both) in accordance with a specific security policy.

(U) **Logical Safeguards.** System-based mechanisms such as firewalls, permission settings, usernames and passwords, and SIPRNet tokens that are used to designate who or what has access to a specific system or function.

(U) **Information Assurance.** Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

(U) **Internet Protocol Address.** An identifier assigned to equipment connected to the network.

(U) **Media Access Control Address.** Common device identifier, for example, a unique identifier that is inherent to a computer, printer, or other network device.

(U) **Physical Safeguards.** Locks, guards, and security containers used to deter or delay an adversary's access to the network.

(U) **Plan of Action and Milestones.** A permanent record that identifies tasks to be accomplished to resolve vulnerabilities and is required for any accreditation decision that requires corrective actions. A Plan of Action and Milestones specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; it is also used to document designated accrediting authority accepted noncompliant IA controls and baseline IA controls that are not applicable.

(U) **Port Security.** A security practice in which network ports are locked electronically so they can be used only by approved devices.

(U) **Protected Distribution System.** A system used to transmit encrypted classified National Security Information through an area of lesser classification or control.

(U) Acronyms and Abbreviations

(b) (7)(E)

7th SC(T) 7th Signal Command (Theater)

(b) (7)(E)

CAT Category

DIACAP DoD Information Assurance Certification and Accreditation Program

(b) (7)(E)

IA Information Assurance

NATO North Atlantic Treaty Organization

NEC Network Enterprise Center

PDS Protected Distribution System

RMF Risk Management Framework

SIPRNet SECRET Internet Protocol Router Network

TACLANE Tactical Local Area Network Encryption

~~SECRET~~

Annex

(U) Annex

(U) Source

~~(FOUO)~~ Source 1: (b) (7)(E) (Document classified SECRET)

Declassify On: 20260129

Date of Source: January 29, 2016

~~SECRET~~

~~SECRET~~

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal.

The DoD Hotline Director is the designated ombudsman.

For more information, please visit the Whistleblower webpage at 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

For Report Notifications

http://www.dodig.mil/pubs/email_update.cfm

Twitter

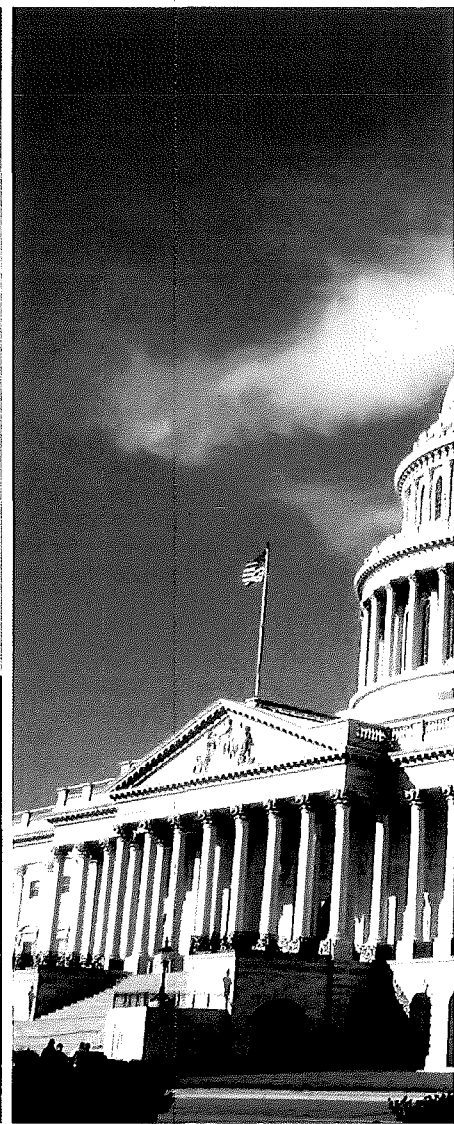
twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline

~~SECRET~~

SECRET



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

SECRET