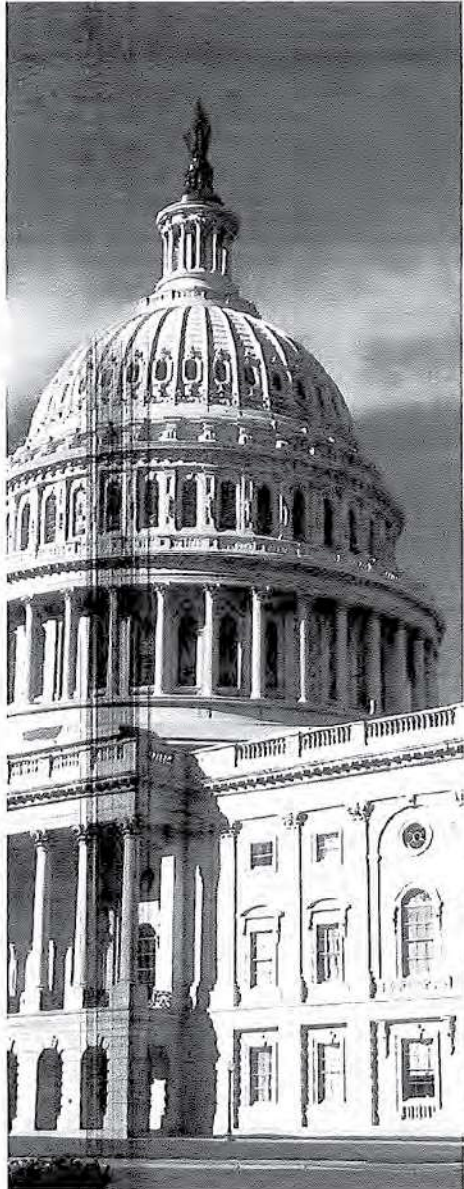


INSPECTOR GENERAL

U.S. Department of Defense

September 1, 2022



(U) Audit of Department of Defense Components' Response to the SolarWinds Orion Compromise

Released by the DoD OIG
FOIA Office under FOIA
request DODOIG-2022-001249
on September 13, 2024.

Controlled By: DoD OIG

Controlled By: Auel/Cyberspace Operations

QJH Category: ISM/OPS/EC/ECRI

Distribution/Dissemination Control: FOR ORNL//NOFORN

POC: DoD OIG (b)(6) @dodig.mil

Classified By: DoD OIG (b)(6) for Cyberpace Operations

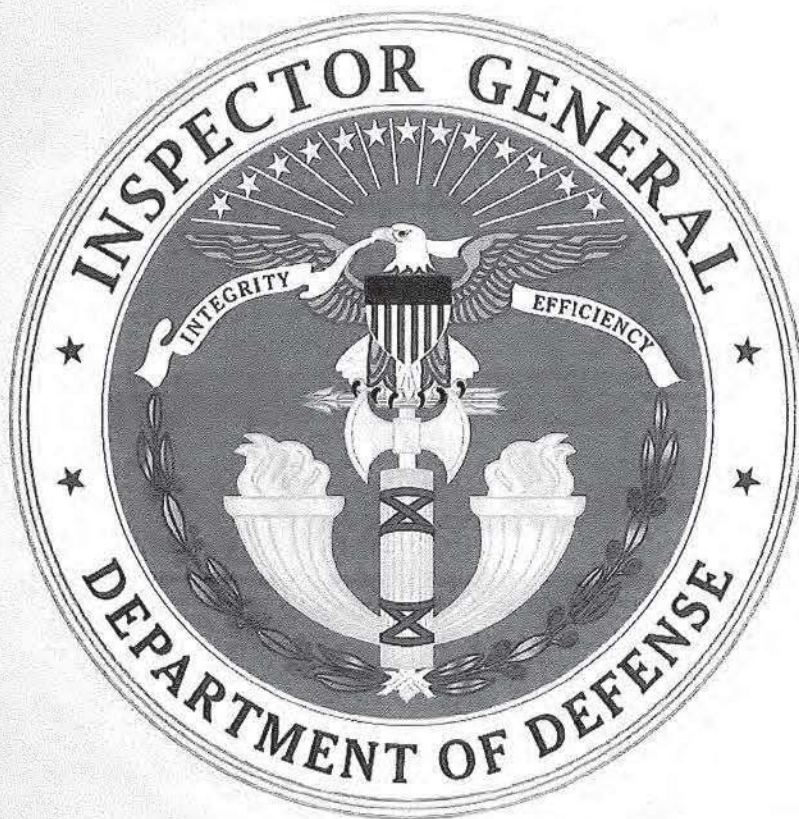
Derived From Multiple Sources

Delivered On: 20/7/2010

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Copy 72 of 150

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~



SECRET//NOFORN

(U) Results in Brief

(U) Audit of Department of Defense Components' Response to the SolarWinds Orion Compromise

(U) September 1, 2022

(U) Objective

(U) The objective of this audit was to determine the actions taken by the DoD to identify, respond to, and mitigate any compromise to DoD networks and systems that resulted from its use of SolarWinds Orion software.

(U) Background

(U) SolarWinds Orion software is used for managing network performance, analyzing network traffic, and monitoring server and application activities on devices, such as physical and virtual servers. On December 13, 2020, FireEye, a cybersecurity incident response company, reported a cyber attack on SolarWinds Orion software. FireEye reported the insertion of malicious code into SolarWinds Orion software updates. The Joint Force Headquarters DoD Information Network (JFHQ-DODIN)

CYBERCOM (b)(3) 10 USC 130e

directing commanders and directors of the Combatant Commands, Service cyber components, and DoD agencies and field activities to identify on unclassified and classified networks all devices with SolarWinds Orion software installed. CYBERCOM (b)(3) 10 USC 130e

requiring action officers, commanders, and directors to identify, analyze, and remediate activities associated with the ongoing efforts of malicious cyber actors to exploit the compromised SolarWinds Orion software.

(U) Finding

(U) While the DoD Components took action to rebuild and patch exposed devices, the DoD Components did not complete all actions required to identify, respond to, and mitigate potential compromises to DoD networks and systems resulting from the use of SolarWinds Orion software. CYBERCOM (b)(3) 10 USC 130e

(U) Finding (cont'd)

(U) CYBERCOM (b)(3) 10 USC 130e

- (S//NF) CYBERCOM (b)(1) 1 4(a)(g)

- (S//NF) CYBERCOM (b)(1) 1 4(a)(g)

- (S//NF) CYBERCOM (b)(1) 1 4(a)(g)

- (S//NF) CYBERCOM (b)(1) 1 4(a)(g)

- (S//NF) CYBERCOM (b)(1) 1 4(a)(g)

- (S//NF) CYBERCOM (b)(1) 1 4(a)(g)

(S//NF) CYBERCOM (b)(1) 1 4(a)(g)

(S//NF) CYBERCOM (b)(1) 1 4(a)(g)

SECRET//NOFORN



(S) CYBERCOM (b)(3) 10 USC 130e

(S//NF) CYBERCOM (b)(1) 1.4(g)

(S) CYBERCOM (b)(1) 1.4(a)(g)

(S) CYBERCOM (b)(3) 10 USC 130e

CYBERCOM (b)(3) 10 USC 130e

 CYBERCOM (b)(3) 10 USC 130e

(C) CYBERCOM (b)(3) 10 USC 130e



(U) Results in Brief

(U) Audit of Department of Defense Components' Response to the SolarWinds Orion Compromise

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

(U) Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, Department of Defense	None	1	None
CYBERCOM (b)(1) 1 7(e), (b)(3) 10 USC 130e	2.a, 2.b, 2.c, 2.d	None	None
	3.a, 3.b, 3.c	None	None
	4.b	4.a	None
	None	5.b	5.a, 5.c, 5.d
	6.a, 6.b	None	None
	None	7.a, 7.b	None
	None	8.a, 8.b, 8.c	None
	9.c	9.a, 9.b	None

(U) Please provide Management Comments by October 3, 2022.

Note: The following categories are used to describe agency management's comments to individual recommendations.

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



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

September 1, 2022

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF
DEFENSE
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

(U) SUBJECT: Audit of Department of Defense Components' Response to the
SolarWinds Orion Compromise (Report No. DODIG-2022-125)

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

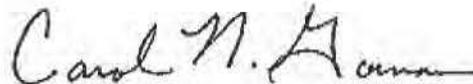
(U) This report contains 11 recommendations that are unresolved because management officials did not provide written comments on the draft report or did not fully address the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the actions are complete, the recommendations will be closed.

(U) The report contains 10 recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain open until adequate documentation has been submitted showing that the agreed-upon actions have been completed. Once we verify that the actions are complete, the recommendations will be closed.

(U) This report contains three recommendations that are considered closed as discussed in the Recommendations, Management Comments, and Our Response section of this report. Those recommendations do not require further action.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, please provide us within 90 days documentation showing that the agreed-upon actions have been completed. Send your response as a PDF file to ~~DoD OIG (b)(6)~~ @dodig.smil.mil. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET). Copies of your comments must have official letterhead and the actual signature of the authorizing official for your organization.

(U) We appreciate the cooperation and assistance received during the audit. Please direct questions to me at ~~DoD OIG (b)(6)~~ (DSN ~~DoD OIG (b)(6)~~).



Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations & Acquisition,
Contracting, and Sustainment

(U) Contents

(U) Introduction	1
(U) Objective.....	1
(U) Background.....	1
(U) Review of Internal Controls.....	5
(U) Finding	6
(U) DoD Components Did Not Take All Actions to Identify, Respond to, and Mitigate the SolarWinds Orion Software Compromise	6
(U) SECRET//NOFORN CYBERCOM (b)(3) 10 USC 130e	7
(U) SECRET//NOFORN CYBERCOM (b)(3) 10 USC 130e	14
(U) SECRET//NOFORN CYBERCOM (b)(3) 10 USC 130e	15
(U) Management Actions Taken.....	15
(U) Management Comments on the Finding and Our Response.....	16
(U) Recommendations, Management Comments, and Our Response	16
(U) Appendixes	29
(U) Appendix A. Scope and Methodology.....	29
(U) Internal Control Assessment and Compliance.....	30
(U) Use of Computer-Processed Data.....	31
(U) Use of Technical Assistance.....	31
(U) Prior Coverage	31
(U) Appendix B. Universe of DoD Components That Reported Devices to JFHQ-DODIN	32
(U) Management Comments	35
(U) Department of Defense, Chief Information Officer	35
(U) SECRET//NOFORN CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e	37
(U) SECRET//NOFORN CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e	44
(U) SECRET//NOFORN CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e	46
(U) SECRET//NOFORN CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e	48
(U) SECRET//NOFORN CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e	51

(U) Contents (cont'd)

(U) [REDACTED]	52
(U) [REDACTED]	54
(U) Acronyms and Abbreviations.....	57
(U) Glossary	58

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine the actions taken by the DoD to identify, respond to, and mitigate any compromise to DoD networks and systems that resulted from its use of SolarWinds Orion software. See Appendix A for a discussion of the audit scope and methodology and the Glossary for a definition of technical terms.

(U) Background

(U) SolarWinds Orion software is used for managing network performance, analyzing network traffic, and monitoring server and application activities on devices such as physical and virtual servers.¹ On December 13, 2020, FireEye, a cybersecurity incident response company, reported a cyber attack on SolarWinds Orion software carried out by the insertion of malicious code into SolarWinds Orion software updates. Once the software updates were loaded, malicious cyber actors could gain access to customers' networks to create new accounts, obtain sensitive data, move across networks unnoticed, and establish methods to remain on the networks. On December 14, 2020, the SolarWinds Corporation filed a report with the U.S. Securities and Exchange Commission that stated the malicious code existed in SolarWinds Orion software updates released from March 2020 through June 2020. According to the President and Chief Executive Officer of the SolarWinds Corporation, at the time of the filing, approximately 33,000 of its 300,000 customers may have installed the software updates, including several DoD Components.

(U) On December 17, 2020, the Cybersecurity Infrastructure Security Agency (CISA) issued an alert identifying an advanced persistent threat against SolarWinds Orion software that began as early as March 2020.² According to CISA, any organization that installed the compromised software updates remained at risk of attack until corrective action was taken.³

¹ (U) A physical server is hardware that is used to run an operating system such as Windows. A virtual server is a software-based representation of a physical server.

² (U) CISA supports Federal agencies ability to safeguard their networks by providing cybersecurity tools, incident response services, and assessment capabilities. An advanced persistent threat is a threat from an adversary with sophisticated levels of expertise and significant resources that executes cyber attacks to gain access to an organization's information technology infrastructure and acquire data or disrupt an organization's mission.

³ (U) *CISA Insights*, "What Every Leader Needs to Know About the Ongoing APT [Advanced Persistent Threat] Cyber Activity," December 2020.

(U) Emergency Directive to Mitigate SolarWinds Orion Compromise

(U) On December 13, 2020, CISA issued Emergency Directive 21-01, "Mitigate SolarWinds Orion Compromise." The Directive instructs Federal agencies to mitigate threats resulting from the use of specific versions of SolarWinds Orion software (versions 2019.4 through 2020.2.1 Hot Fix 1) on Federal and contractor systems that store Government data. The Directive required agencies to report to CISA the total number of devices with the vulnerable SolarWinds Orion software and forensically image the system memory of those devices by December 14, 2020.

(U) The Directive also requires agencies to analyze their networks for suspicious new users or service accounts and remove those users and service accounts, analyze networks for indicators of compromise, disconnect exposed devices with vulnerable SolarWinds Orion software from networks, and block all network communication from SolarWinds Orion devices. Although the Directive does not apply to national security systems or to systems operated by the DoD and the Intelligence Community, the Joint Force Headquarters DoD Information Network (JFHQ-DODIN) issued corresponding guidance through various Cyber Tasking and Operation Orders that applies to those systems.

(U) DoD Guidance Issued In Response to the SolarWinds Orion Compromise

(S) [REDACTED] CYBERCOM (b)(3) 10 USC 130e

directs commanders and directors of the Combatant Commands, Service cyber components, and DoD agencies and field activities within JFHQ-DODIN areas of operation to identify all SolarWinds Orion software installed, on both unclassified and classified networks.⁴ See Appendix B for a list of DoD Components that fall within JFHQ-DODIN's areas of operation.

(S) [REDACTED] CYBERCOM (b)(3) 10 USC 130e

[REDACTED] requires action officers, commanders, and directors to identify, analyze, and remediate activities associated with malicious cyber actors' ongoing efforts to exploit compromised

⁴ (U) The JFHQ-DODIN Commander is responsible for directing the execution of global DODIN operations and Defensive Cyber Space Operations-Internal Defensive Measures to ensure the effective functioning and defense of the DODIN. [REDACTED] CYBERCOM (b)(3) 10 USC 130e. The areas of operation are grouped by the DoD Component commanders and directors who have the authority to direct DODIN operations and Defensive Cyber Space Operations.

⁵ (U) [REDACTED] CYBERCOM (b)(3) 10 USC 130e. For the purpose of this report, adversaries are the same as malicious cyber actors.

(S//NF) SolarWinds Orion software.⁶ (S//NF) CYBERCOM (b)(3) 10 USC 130e identified the following categories to assign to each device using SolarWinds Orion software.

- (S//NF) Not Compromised – Devices that did not have any indications of compromise or did not have one of the vulnerable SolarWinds Orion software versions.
- (S//NF) Exposed – Devices that had SolarWinds Orion software with one of the vulnerable SolarWinds software versions.
- (S//NF) Compromised – Devices that had SolarWinds Orion software with malicious codes, and the malicious cyber actor had infiltrated the network.

(S//NF) (S//NF) CYBERCOM (b)(3) 10 USC 130e
[Redacted text block]

(U) OPORD Tasks Assessed

(S//NF) (S//NF) CYBERCOM (b)(3) 10 USC 130e
[Redacted text block]

⁶ (U) (S//NF) CYBERCOM (b)(3) 10 USC 130e [Redacted text]

(U) Table 1. Tasks Assessed and Their Importance

(U) Tasks	Importance of Task
1. Identify and report devices with SolarWinds Orion software to JFHQ-DODIN. This includes any devices with the software, not just the devices that had the malicious code.	Systems that have the SolarWinds Orion software are more likely to have been compromised.
2. Identify the presence of cross-domain systems within enclaves containing exposed devices.	Cross-domain systems provide the ability to manually or automatically access and transfer information between different security domains. Cross-domain systems can provide an attacker a way to move out of an enclave to a system otherwise unreachable. An enclave is a set of systems that operate in the same security domain and share the protection of a single, common, continuous security perimeter.
3. Disconnect (physically or logically) any exposed device.	Disconnecting the exposed devices from the DODIN will prevent malicious cyber actors from issuing further commands to those devices.
4. Create a forensic image of all exposed devices.	Forensic imaging captures the state of the system at a point in time, including any known and unknown malicious code, unauthorized accounts, connections, and processes in use. Creating a forensic image is critical for forensic analysis as the image will contain indicators of compromise, such as creation of new accounts and authentication attempts, that might otherwise be lost if the system is powered down.
5. Review network logs back to the date that the SolarWinds Orion software versions containing the malicious code were loaded.	Network logs provide details on system activity and aid in incident response and recovery activities. Review of the logs will indicate whether a device connected or tried to connect to a malicious website.
6. Block network communication to known malicious websites and Internet protocol addresses.	Blocking network communications prevents the malicious cyber actor and the malicious code on the exposed device from contacting each other.
7. Ensure continuous network monitoring for unusual user activity and indicators of compromise.	Continuous network monitoring for unusual user activity and indicators of compromise provides organizations with timely identification of malicious activity.
8. Execute full server rebuild on exposed devices.	A full server rebuild ensures destruction of any known and unknown malicious code, unauthorized accounts, unauthorized scheduled tasks, and other methods of reestablishing unauthorized communications caused by the malicious code.
9. Execute user and system credential reset for any exposed devices.	Resetting credentials ensures that any accounts created or modified by the attacker become inaccessible.

(U)

(U) Tasks	Importance of Task
10. Reset the authentication protocol (referred to as Kerberos) at least twice.	Authentication protocol (Kerberos) is a mechanism to verify a user's identity. Resetting the authentication protocol account at least twice ensures that a malicious cyber actor cannot create an account that would grant them permission to the network. The authentication protocol stores a user's current password and one previous password, so resetting it at least twice removes the passwords and invalidates the account.
11. Execute timely patching of exposed devices with the DoD patch for SolarWinds Orion software.	Patching includes the use of maintenance tools to install the latest software updates and patches. Outdated or unpatched software can provide an opportunity for adversaries to exploit vulnerabilities. Patching is usually the most effective way to mitigate software vulnerabilities and significantly reduce opportunities for exploitation.

(U)

(U) Source: The DoD OIG.

(U) Review of Internal Controls

~~(S)~~ DoD Instruction 5010.40 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.⁷

CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

⁷ (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, (Incorporating Change 1, June 30, 2020).

(U) Finding

(U) DoD Components Did Not Take All Actions to Identify, Respond to, and Mitigate the SolarWinds Orion Software Compromise

(U) While the DoD Components took action to rebuild and patch exposed devices, the DoD Components did not complete all the actions required to identify, respond to, and mitigate potential compromises to DoD networks and systems resulting from the use of SolarWinds Orion software. ~~SECRET//NOFORN~~ CYBERCOM (b)(3) 10 USC 130a

- (S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]
- (S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]
- (S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]
- (S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]
- (S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]
- (S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]

(S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]

(S//NF) ~~SECRET//NOFORN~~ CYBERCOM (b)(1) 1.4(a)(g) [Redacted]

Finding

(S//NF) CYBERCOM (b)(1) 1.4(a)(g)
 [Redacted]
 [Redacted]
 [Redacted]
 [Redacted]
 [Redacted]

(S//NF) CYBERCOM (b)(3) 10 USC 130e
 [Redacted]
 [Redacted]

(S//NF) CYBERCOM (b)(3) 10 USC 130e
 [Redacted]
 [Redacted]
 [Redacted]
 [Redacted]
 [Redacted]

(U) Table 2. Tasks Not Completed by the DoD Components Reviewed

(S//NF)	Task
CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g) [Redacted]	
	(S//NF)

(U) Legend
 (S//NF) CYBERCOM (b)(3) 10 USC 130e
 [Redacted]
 [Redacted]
 [Redacted]
 [Redacted]

(U) Source: The DoD OIG.

* (U) Joint Chiefs of Staff Memorandum, "Report to Congress on SolarWinds Compromise," February 24, 2021.

(~~CUH~~) DoD Components Did Not Provide Accurate or Timely Reporting on Devices Using SolarWinds Orion Software

(~~S//NF~~) CYBERCOM (b)(1) 1.4(a)(g); OSD/JS (b)(1) 1.4(g)

[REDACTED]

⁹

(~~S//NF~~) CYBERCOM (b)(1) 1.4(a)(g); OSD/JS (b)(1) 1.4(g)

[REDACTED]

(~~CUH~~) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

⁹ (U) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

Finding

(S//NF)

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

(S//NF)

CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(S//NF)

CYBERCOM (b)(3) 10 USC 130e

(S//NF)

CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(S//NF)

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

¹⁰ (U)

CYBERCOM (b)(3) 10 USC 130e

Finding

(S//NF) CYBERCOM (b)(1) 1 4(a)(g)

(S//NF) CYBERCOM (D)(3) TO USC 130e

12

(S) CYBERCOM (b)(3) 10 USC 130e

(S) CYBERCOM (b)(3) 10 USC 130e

11 (S//) CYBERCOM (b)(3) 10 USC 130e

12 (U) CYBERCOM (b)(3) 10 USC 130e

Finding

~~(S)~~ CYBERCOM (b)(3) 10 USC 130e

(S//NF) CYBERCOM (b)(1) 1.4(a)(g); OSD/JS (b)(1) 1.4(g)

(S//NF) CYBERCOM (b)(3) 10 USC 130a

(S) CYBERCOM (b)(1) 1.4(a)(g); OSD/JS (b)(1) 1.4(g)

(S//NF) CYBERCOM (b)(1) 1.4(a)(g)

(S) CYBERCOM (b)(3) 10 USC 130e

¹³(U) An endpoint is an end-user device, such as mobile devices, laptop, desktop computers and servers.

¹⁴ (U) Air Force Instruction 17-203, "Cyber Incident Handling," March 16, 2017.

Finding

(C) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

(S) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

(S//NF) CYBERCOM (b)(1) 1 4(a)(g), OSD/JS (b)(1) 1 4(g)

[illegible]

(S//NF) CYBERCOM (b)(1) 1.4(a)(g)

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

[illegible]

Finding

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)
[Redacted text block]

(CUI) CYBERCOM (b)(3) 10 USC 130e
[Redacted text block]

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)
[Redacted text block]

(CUI) CYBERCOM (b)(3) 10 USC 130e
[Redacted text block]

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)
[Redacted text block]

Finding

(CUI) CYBERCOM (b)(3) 10 USC 130e
[Redacted]

(CUI) CYBERCOM (b)(3) 10 USC 130e
[Redacted]

(CUI) CYBERCOM (b)(3) 10 USC 130e
[Redacted]

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)
[Redacted]

(S//NF) CYBERCOM (b)(1) 1.4(a)(g)
[Redacted]

(CUI) CYBERCOM (b)(3) 10 USC 130e
[Redacted]

(CUI) CYBERCOM (b)(3) 10 USC 130e
[Redacted]

Finding

(S//NF) CYBERCOM (b)(3) 10 USC 130e [Redacted]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [Redacted]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [Redacted]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [Redacted]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [Redacted]

[Redacted]

(U) Management Actions Taken

(S//NF) CYBERCOM (b)(1) 1 4(a)(g), OSD/JS (b)(1) 1 4(g) [Redacted]

(U) Management Comments on the Finding and Our Response

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED], provided the following comments on the Finding. For the full text of the comments, see the Management Comments section of the report.

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]	<i>Comments</i>
(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

(U) Our Response

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]

(CUI) Department of Defense Chief Information Officer Comments

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Finding

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Our Response

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) [REDACTED] Comments

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Our Response

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Recommendation 2

(S//NF) We recommend that ~~CYBERCOM (b)(3) 10 USC 130e~~ :

- a. ~~CYBERCOM (b)(3) 10 USC 130e~~
- b. ~~CYBERCOM (b)(3) 10 USC 130e~~

(U) ~~CYBERCOM (b)(3) 10 USC 130e~~ **Comments**

(S//NF) ~~CYBERCOM (b)(1) 1.4(a)(g)~~

(U) Our Response

(S//NF) Comments from the Director did not address the specifics of the recommendations; therefore, the recommendations are unresolved. ~~CYBERCOM (b)(1) 1.4(a)(g)~~

~~CYBERCOM (b)(3) 10 USC 130e~~

- c. **(S//NF)** ~~CYBERCOM (b)(3) 10 USC 130e~~

(U) ~~CYBERCOM (b)(3) 10 USC 130e~~ **Comments**

(S//NF) ~~CYBERCOM (b)(1) 1.4(a)(g)~~

(U) Our Response

(S//NF) Comments from the Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. ~~CYBERCOM (b)(1) 1.4(a)(g)~~

~~CYBERCOM (b)(3) 10 USC 130e~~

(S//NF) CYBERCOM (b)(1) 1.4(a)(g) . Therefore, we request that CYBERCOM (b)(1) 1.4(a)(g) provide additional comments on the final report describing the actions that CYBERCOM (b)(1) 1.4(a)(g) will take to address the recommendation.

- d. (S//NF) Develop a plan of action and milestones for tasks that were not completed as required CYBERCOM (b)(3) 10 USC 130e .

(U) CYBERCOM (b)(3) 10 USC 130e *Comments*

(S//NF) CYBERCOM (b)(1) 1.4(a)(g)

(U) *Our Response*

(S//NF) Although the Director agreed with the recommendation, his comments did not address the specifics of the recommendation; therefore, the recommendation is unresolved. CYBERCOM (b)(1) 1.4(a)(g)

Therefore, we request that CYBERCOM (b)(1) 1.4(a)(g) provide additional comments on the final report describing the actions will take to CYBERCOM (b)(1) 1.4(a)(g).

(U) *Recommendation 3*

(S//NF) We recommend that CYBERCOM (b)(3) 10 USC 130e coordinate with the Joint Forces Headquarters-Department of Defense Information Network Commander to:

- a. CYBERCOM (b)(3) 10 USC 130e

- b. CYBERCOM (b)(3) 10 USC 130e

- c. CYBERCOM (b)(3) 10 USC 130e

(U) CYBERCOM (b)(3) TO USC 130e *Comments*

CYBERCOM (b)(3) 10 USC 130e

(U) Our Response

(b)(3) Although the Director agreed with the recommendations, his comments did not address the specifics of the recommendations; therefore, the recommendations are unresolved. CYBERCOM (b)(3) 10 USC 130e

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Therefore, we request that [REDACTED] CYBERCOM (b)(3) 10 USC 130e
[REDACTED] provide additional comments on the final report describing the actions that
[REDACTED] will take to address the recommendations. CYBERCOM (b)(3) 10 USC 130e

(U) Recommendation 4

(S) We recommend that [REDACTED] CYBERCOM (b)(3) 10 USC 130e

a. CYBERCOM (b)(3) 10 USC 130e

CYBERCOM (b)(3) 10 USC 130e *Comments*

CYBERCOM (b)(3) 10 USC 130e

(U) Our Response

(S) Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close this recommendation once CYBERCOM (b)(3) 10 USC 130a

Finding

- b. ~~(S//NF)~~ Develop a plan of action and milestones for tasks that were not completed as required ~~CYBERCOM (b)(3) 10 USC 130e~~.

~~(S//NF)~~ ~~CYBERCOM (b)(3) 10 USC 130e~~ *Comments*
~~(S//NF)~~ ~~CYBERCOM (b)(3) 10 USC 130e~~
[Redacted]
[Redacted]
[Redacted]

(U) Our Response

~~(S//NF)~~ ~~CYBERCOM (b)(3) 10 USC 130e~~
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) Recommendation 5

~~(S//NF)~~ We recommend that ~~CYBERCOM (b)(1) 1.4(a)(g)~~
[Redacted]:

- a. ~~CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)~~
[Redacted]

~~(S//NF)~~ ~~CYBERCOM (b)(3) 10 USC 130e~~ *Authorizing
Official Comments*

~~(S//NF)~~ ~~CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)~~
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

(U) Our Response

~~(S//NF)~~ Comments from the Authorizing Official addressed the specifics of the recommendation. ~~CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)~~
[Redacted]
[Redacted]
[Redacted]. Therefore, the recommendation is closed and no further comments are required.

Finding

- b. (S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(S//NF) CYBERCOM (b)(3) 10 USC 130e

Authorizing

Official Comments

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(U) Our Response

(S//NF) Comments from the Authorizing Official addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

- c. (S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(S//NF) CYBERCOM (b)(3) 10 USC 130e

Authorizing

Official Comments

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(U) Our Response

(S//NF) Comments from the Authorizing Official addressed the specifics of the recommendation. CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

. Therefore, the recommendation is closed and no further comments are required.

- d. (S//NF) Develop a plan of action and milestones for tasks that were not completed as required CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(S//NF) CYBERCOM (b)(3) 10 USC 130e

Comments

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(S//NF) CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

(U) Our Response

(S//NF) Comments from the Authorizing Official addressed the specifics of the recommendation. CYBERCOM (b)(1) 1.4(a)(g), OSD/JS (b)(1) 1.4(g)

. Therefore, the recommendation is closed and no further comments are required.

(U) Recommendation 6

(CU) We recommend that CYBERCOM (b)(3) 10 USC 130e :

- a. CYBERCOM (b)(3) 10 USC 130e
- b. Develop a plan of action and milestones for tasks that were not completed as required CYBERCOM (b)(3) 10 USC 130e

(CU) CYBERCOM (b)(3) 10 USC 130e

Comments

(S//NF) CYBERCOM (b)(1) 1.4(a)(g)

[REDACTED]

(U) Our Response

(S//NF) Comments from CYBERCOM (b)(1) 1.4(a)(g) did not address the specifics of the recommendations; therefore, the recommendations are unresolved.

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

(S//NF) CYBERCOM (b)(1) 1.4(a)(g) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Recommendation 7

(S//NF) We recommend that CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]:

- a. CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]

Comments

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]

(U) Our Response

(S//NF) Comments from CYBERCOM (b)(3) 10 USC 130e [REDACTED] addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]

- b. (S//NF) Develop a plan of action and milestones for tasks that were not completed as required CYBERCOM (b)(3) 10 USC 130e [REDACTED].

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED]

(U) Our Response

(S//NF) Comments from CYBERCOM (b)(3) 10 USC 130e [REDACTED] addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]

Finding

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED].

(U) Recommendation 8

(S//NF) We recommend that CYBERCOM (b)(3) 10 USC 130e [REDACTED]:

- a. CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED] *Comments*

(S//NF) CYBERCOM (b)(1) 1.4(a)(g) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

(U) Our Response

(S//NF) Comments from CYBERCOM (b)(3) 10 USC 130e [REDACTED] addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED].

- b. (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED] *Comments*

(S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]
[REDACTED]
[REDACTED].

(U) Our Response

(S//NF) Comments from CYBERCOM (b)(1) 1.4(a)(g) [REDACTED] addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close

(S//NF) the recommendation once CYBERCOM (b)(1) 1-4(a)(g)

- c. (S//NF) Develop a plan of action and milestones for tasks that were not completed as required CYBERCOM (b)(3) 10 USC 130e

(S//NF) CYBERCOM (b)(3) 10 USC 130e Comments

(S//NF) CYBERCOM (b)(3) 10 USC 130e

(U) Our Response

(S//NF) CYBERCOM (b)(3) 10 USC 130e

. Therefore, the recommendation is resolved but open. We will close the recommendation once

CYBERCOM (b)(3) 10 USC 130e

(U) Recommendation 9

(S//NF) We recommend that CYBERCOM (b)(3) 10 USC 130e

- a. CYBERCOM (b)(3) 10 USC 130e

(S//NF) CYBERCOM (b)(3) 10 USC 130e

Comments

(S//NF) CYBERCOM (b)(3) 10 USC 130e

(U) Our Response

(S//NF) Comments from CYBERCOM (b)(3) 10 USC 130e addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once CYBERCOM (b)(3) 10 USC 130e

b. (S//NF) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

(S//NF) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

Comments

(S//NF) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

(U) Our Response

(S//NF) Comments from CYBERCOM (b)(3) 10 USC 130e addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

c. (S//NF) Develop a plan of action and milestones for tasks that were not completed as required CYBERCOM (b)(3) 10 USC 130e.

(S//NF) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

Comments

(S//NF) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

(U) Our Response

(S//NF) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

Finding

(S//NF)

CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this audit from February 2021 through March 2022 in accordance with generally accepted government auditing standards. However, due to the DoD's implementation of maximum telework during the coronavirus disease-2019 pandemic, the audit was suspended from December 2021 through February 2022. Generally accepted government auditing standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

(~~CU~~) To understand the SolarWinds Orion Compromise and the actions needed to mitigate the impact of the compromise, we interviewed officials from CYBERCOM (b)(3) 10 USC 130e. [REDACTED]. Table 3 lists the 20 DoD Components we reviewed to determine whether the actions taken to identify, respond to, and mitigate any compromise to DoD networks and systems that resulted from the DoD's use of SolarWinds Orion software were completed as required CYBERCOM (b)(3) 10 USC 130e.

(U) Table 3. DoD Components Sampled by the DoD OIG Regarding the SolarWinds Orion Compromise

DoD Components Selected	
[REDACTED]	
	(CUI)

(U) Source: The DoD OIG.

(U) Additionally, we reviewed Federal and DoD policy concerning tasks for mitigating vulnerabilities related to the SolarWinds Orion Compromise, forensic imaging, and log management.

(U) We selected a nonstatistical sample of 20 DoD Components from the 162 DoD Components that reported the presence of the SolarWinds Orion software on their networks to JFHQ-DODIN. Of the 162 DoD Components, we excluded

CYBERCOM (b)(3) 10 USC 130e

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]. We assessed 10 DoD Components that reported having SolarWinds Orion software to JFHQ-DODIN and 10 DoD Components that reported having no SolarWinds Orion software.

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed tasks related to:

- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED];
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED]; and
- (S//NF) CYBERCOM (b)(3) 10 USC 130e [REDACTED].

(U) However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

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

(U) Use of Technical Assistance

(U) The DoD OIG Quantitative Methods Division assisted with developing a nonstatistical sampling methodology for selecting DoD Components.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) issued one report addressing the Federal response to the SolarWinds Orion Compromise.

(U) Government Accountability Office

(U) Report No. GAO 22-104746, "Federal Response to SolarWinds and Microsoft Exchange Incidents," January 2022


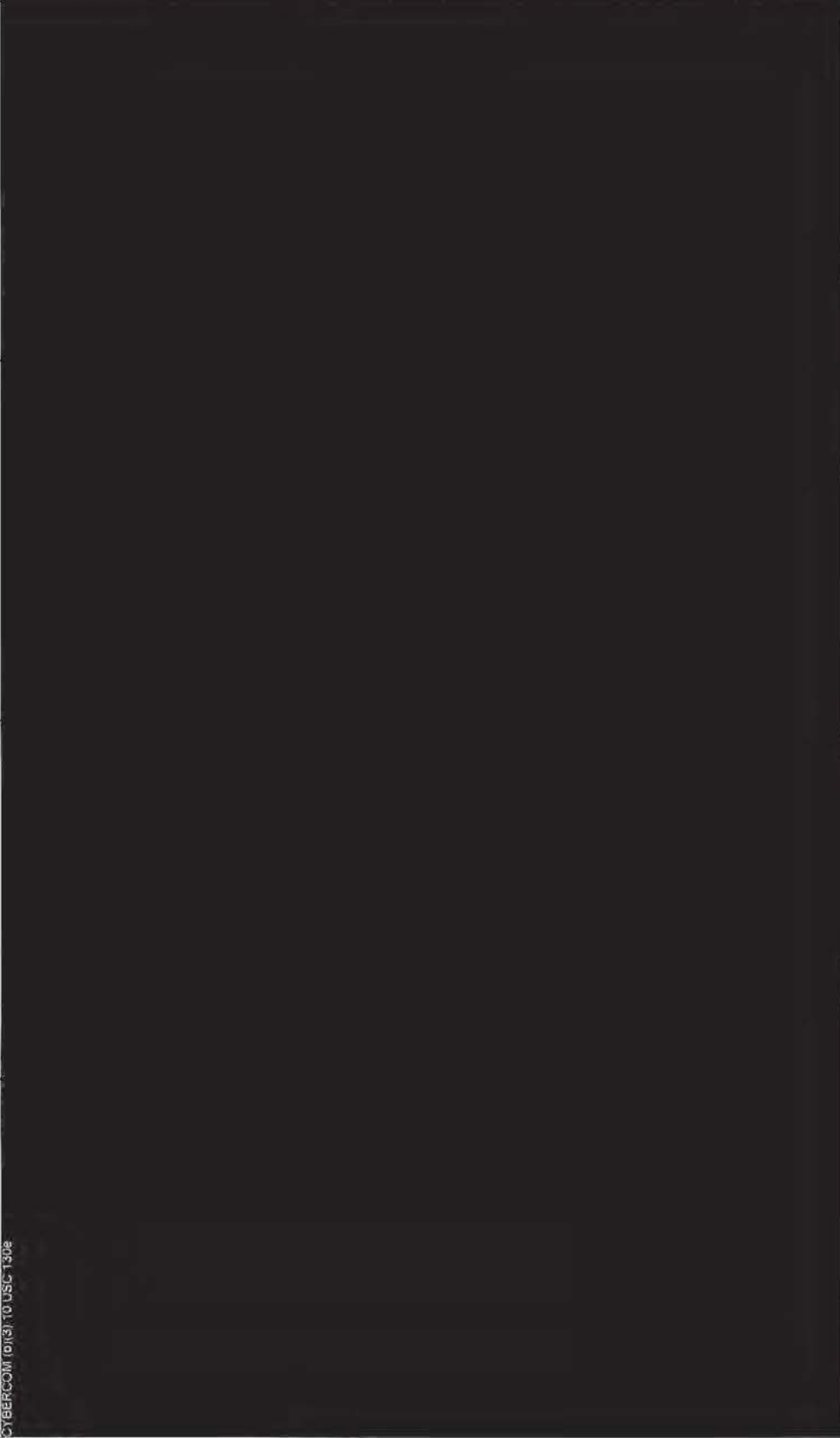
(U) The GAO determined that Federal agencies took several steps to coordinate and respond to the SolarWinds incident. The Cybersecurity and Infrastructure Systems Agency (CISA) issued emergency directives to inform Federal agencies of the vulnerabilities and the Unified Coordination Group provided guidance through advisories, alerts, and tools. The GAO concluded that even though CISA's efforts to work with agencies have provided a degree of confidence that the threat actor is no longer present, the threat actor may have established undiscovered persistent access within affected agencies' and private companies' networks. The GAO stated that failure to perform comprehensive and thorough remediation activity will expose those networks to substantial risk for long-term undetected persistent threat activity. This report did not contain recommendations.


(U) Appendix B

(U) Universe of DoD Components That Reported Devices to JFHQ-DODIN

(S//NF) CYBERCOM (b)(3) 10 USC 1302e			

Appendix B

 CYBERCOM (D13) TO USC 130e			
----------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	--	--

(S//NF) CYBERCOM (b)(3) 10 USC 130e			
			

(U) Source: The DoD OIG and JFHQ-DODIN.

(U) * Indicates that the Component falls within JFHQ-DODIN's area of operation.

(U) Management Comments

(U) Department of Defense, Chief Information Officer



CHIEF INFORMATION OFFICER

~~CONTROLLED UNCLASSIFIED INFORMATION~~
DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

June 17, 2022

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "Audit of Department of Defense Components' Response to the SolarWinds Compromise" Draft Report (D2021-D000CR-0081.000)

(U) This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Draft Report, Audit of Department of Defense Components' Response to the SolarWinds Compromise" Draft Report (D2021-D000CR-0081.000).

~~(S)~~ DoD IG RECOMMENDATION: CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

~~(S)~~ DoD CIO RESPONSE: CYBERCOM (b)(3) 10 USC 130e

(U) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

• (U) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

• (U) CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

Controlled by: DCIO-CS
Category: PRIVILEGE
LDC: FEDCON
POC: DCIO-CS-RA&OI, [REDACTED]

~~CONTROLLED UNCLASSIFIED INFORMATION~~

Management Comments

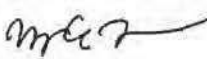
(U) Department of Defense, Chief Information Officer (cont'd)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

- (U) CYBERCOM (b)(3) 10 USC 130e [REDACTED]

- (U) CYBERCOM (b)(3) 10 USC 130e [REDACTED]

(U) The point of contact for this matter is [REDACTED] who may be reached at [REDACTED]


John B. Sherman

~~CONTROLLED UNCLASSIFIED INFORMATION~~

Management Comments

(U) CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e [Redacted]

~~SECRET//NOFORN~~



THE JOINT STAFF
WASHINGTON, DC

DJSM 0098-22
7/2/22

Reply Zip Code:
20318-0300

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: (U) Audit of Department of Defense Components' Response to the SolarWinds
Compromise (Project No. D2021-D000CR-0081.000)

1. (U) This memorandum is in response to the Office of the Inspector General of the Department of Defense request for comments on the subject report.
2. (U) The Joint Staff concurs with the report and submits the attached comments for consideration.
3. (U) The Joint Staff point of contact is [Redacted], J-6, Cybersecurity, Modernization & Governance Division; [Redacted]

JAMES J. MINGUS, LTG, USA
Director, Joint Staff

Classified By: OSDJS (b)(6)
Derived From: Multiple Sources
Declassify On: 2046/719 UNCLASSIFIED When Separated From Attachments

~~SECRET//NOFORN~~

Management Comments

(U)

CYBERCOM (b)(1) 1.7(e) (b)(3) 10 USC 130e

(cont'd)

~~SECRET//NOFORN~~

COMPONENT COORDINATOR RESPONSE

June 27, 2022

SUBJECT: Proposed Change in Item DODIG Draft Report "Audit of Department of Defense Components' Response to the SolarWinds Compromise, Project No. D2021- D000CR-0081.000.

On behalf of my Component, my formal response to this issuance is: Concur with comment. Below are comments for your consideration from ODJS/DIG MILSEC, CYBERCOM (b)(3) 10 USC 130e

My point of contact for this action is [REDACTED]

OSD/JS (b)(6)

Coordinating Official's Component: JS J6

DD FORM 818, AUG 2016

REPLACES SD FORM 818, WHICH IS OBSOLETE

(U) CYBERCOM (b)(1) 1 7(e) (b)(3) 10 USC 130e (cont'd)

SECRET//NOFORN						
DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title"						
CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
	1	25	1	<input type="checkbox"/>	Coordinator Comment and Justification: OSD/JS (b)(5) Coordinator Recommended Change: Originator Response: Choose an item. Originator Reasoning:	Joint Staff Assistant IG [Redacted Signature]
	2	25	1	<input type="checkbox"/>	Coordinator Comment and Justification: CYBERCOM (b)(3) 10 USC 130e, OSD (b)(5) Coordinator Recommended Change: Originator Response: Choose an item. Originator Reasoning:	Joint Staff Assistant IG [Redacted Signature]
	3	25	1	<input type="checkbox"/>	Coordinator Comment and Justification: CYBERCOM (b)(3) 10 USC 130e, OSD (b)(5) Coordinator Recommended Change: Originator Response: Choose an item. Originator Reasoning:	Joint Staff Assistant IG [Redacted Signature]

DD FORM 818, AUG 2016

REPLACES SD FORM 818, WHICH IS OBSOLETE

1

(U) ~~CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e~~ (cont'd)

DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title"						
CLASS	#	PAGE	PARA	BASIS FOR NON-CONCURRENCE	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
1	4			<input type="checkbox"/>	<p>Coordinator Comment and Justification: OSD (b)(5)</p> <p>Coordinator Recommended Change:</p> <p>Originator Response: Choose an item.</p> <p>Originator Reasoning:</p>	<p>Joint Staff Legal Counsel</p> <p>[Redacted]</p>
2	5	16	2a/2b	<input type="checkbox"/>	<p>Coordinator Comment and Justification: CYBERCOM (b)(1) 1.4(a)(9)</p> <p>Coordinator Recommended Change:</p> <p>Originator Response: Choose an item.</p> <p>Originator Reasoning:</p>	<p>CYBERCOM (b)(3) 10 USC 130e</p> <p>[Redacted]</p>
3	6	16	2c	<input type="checkbox"/>	<p>Coordinator Comment and Justification: CYBERCOM (b)(1) 1.4(a)(9)</p> <p>Coordinator Recommended Change:</p> <p>Originator Response: Choose an item.</p> <p>Originator Reasoning:</p>	<p>CYBERCOM (b)(3) 10 USC 130e</p> <p>[Redacted]</p>

DD FORM 818, AUG 2016 REPLACES SD FORM 818, WHICH IS OBSOLETE

~~SECRET//NOFORN~~

2

(U)

CYBERCOM (b)(1) 1.7(e) (b)(3) 10 USC 130e

(cont'd)

DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title"						
CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
	7	16	2d	<input type="checkbox"/>	<p>Coordinator Comment and Justification: CYBERCOM (b)(1) 1.4(a)(9)</p> <p>Coordinator Recommended Change:</p> <p>Originator Response: Choose an item</p> <p>Originator Reasoning:</p>	<p>CYBERCOM (b)(1) 1.4(a)(9)</p> <p>USC 130e</p>
	8	16	3	<input type="checkbox"/>	<p>Coordinator Comment and Justification: CYBERCOM (b)(1) 1.4(a)(9)</p> <p>Coordinator Recommended Change:</p> <p>Originator Response: Choose an item.</p> <p>Originator Reasoning:</p>	<p>CYBERCOM (b)(1) 1.4(a)(9)</p> <p>USC 130e</p>

DD FORM 818, AUG 2016 REPLACES SD FORM 818, WHICH IS OBSOLETE

3

(U)

CYBERCOM (b)(1) 1.7(e) (b)(3) 10 USC 130e

(cont'd)

DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title"						
CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
	9	16	3	<input type="checkbox"/>	<p>Coordinator Comment and Justification: CYBERCOM (b)(1) 1.4(a)(g)</p> <p>[REDACTED]</p> <p>Coordinator Recommended Change:</p> <p>Originator Response: Choose an item.</p> <p>Originator Reasoning:</p>	<p>CYBERCOM (b)(3) 10 USC 130e</p> <p>[REDACTED]</p>
	10	16	3	<input type="checkbox"/>	<p>Coordinator Comment and Justification: CYBERCOM (b)(3) 10 USC 130e</p> <p>[REDACTED] reviewed the documentation and recommends concur with recommendation #3 including parts a, b and c listed on page 16 of the Draft report.</p>	<p>CYBERCOM (b)(3) 10 USC 130e</p> <p>[REDACTED]</p>

DD FORM 818, AUG 2016

REPLACES SD FORM 818, WHICH IS OBSOLETE

4

(U)

CYBERCOM (b)(1) 1.7(e) (b)(3) 10 USC 130e

(cont'd)

DoD ISSUANCE COORDINATION RESPONSE: Issuance Type and Number, "Title"						
CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					Coordinator Recommended Change: Originator Response: Choose an item Originator Reasoning:	
	11	16	3	<input type="checkbox"/>	Coordinator Comment and Justification: CYBERCOM (b)(3) 10 USC 130e - Concur no critical comments to add Coordinator Recommended Change: Originator Response: Choose an item Originator Reasoning:	CYBERCOM (b)(3) 10 USC 130e
	12	16	1	<input type="checkbox"/>	Coordinator Comment and Justification: CYBERCOM (b)(3) 10 USC 130e, OSD (b)(5) Coordinator Recommended Change: CYBERCOM (b)(3) 10 USC 130e, OSD (b)(5) Originator Response: Choose an item. Originator Reasoning:	Joint Staff J6 Chief of Staff

Management Comments

(U)

CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130a

CYBERCOM (b)(3) 10 USC 130a



Management Comments

(U) CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e [REDACTED] (cont'd)

CYBERCOM (b)(3) 10 USC 130e

[REDACTED]

Management Comments

(U)

CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e

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



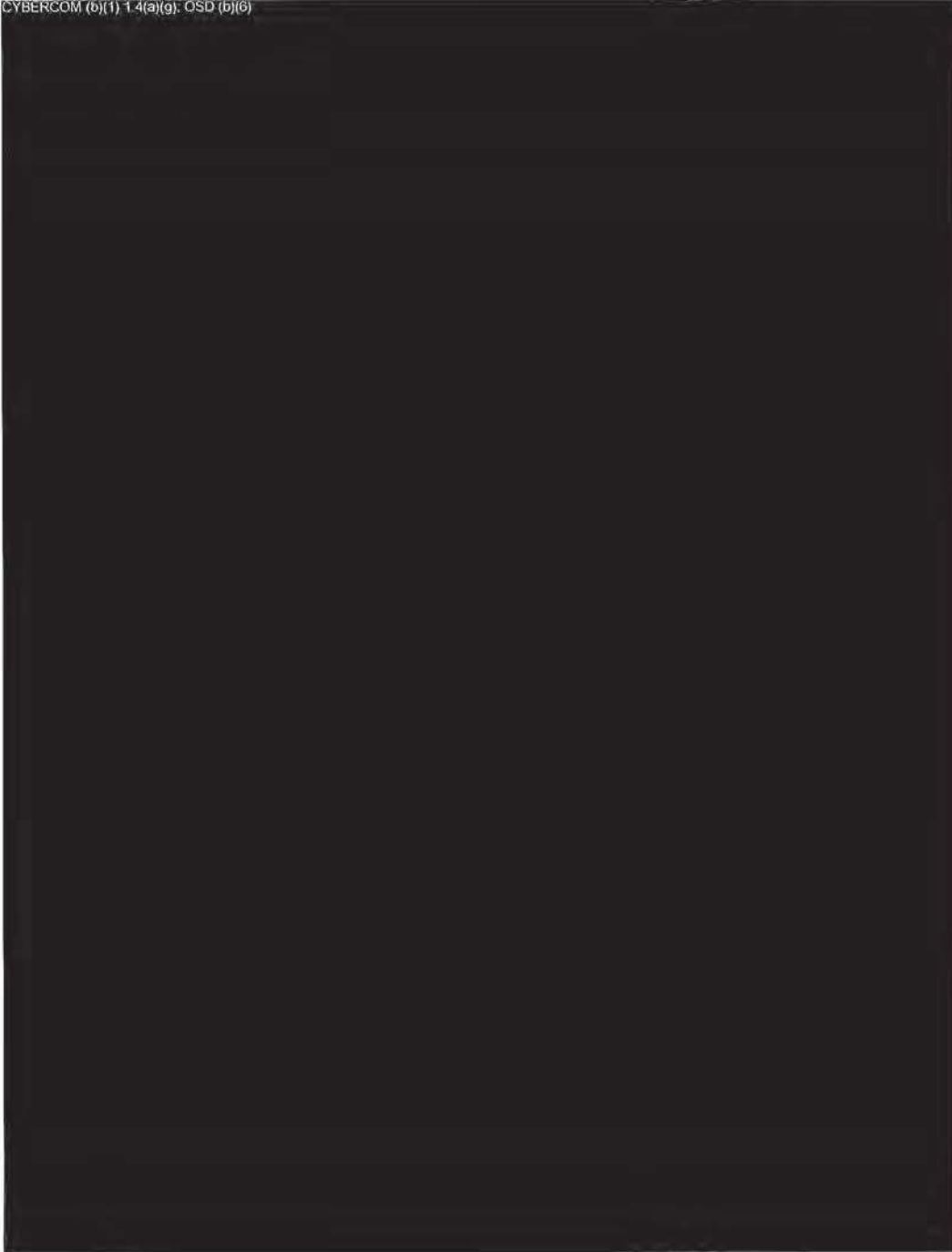
Management Comments

(U)

CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130a

(cont'd)

CYBERCOM (b)(1) 1.4(a)(g); OSD (b)(6)



Management Comments

(U)

CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130a

CYBERCOM (b)(1) 1.4(a)(g), (b)(3) 10 USC 130a

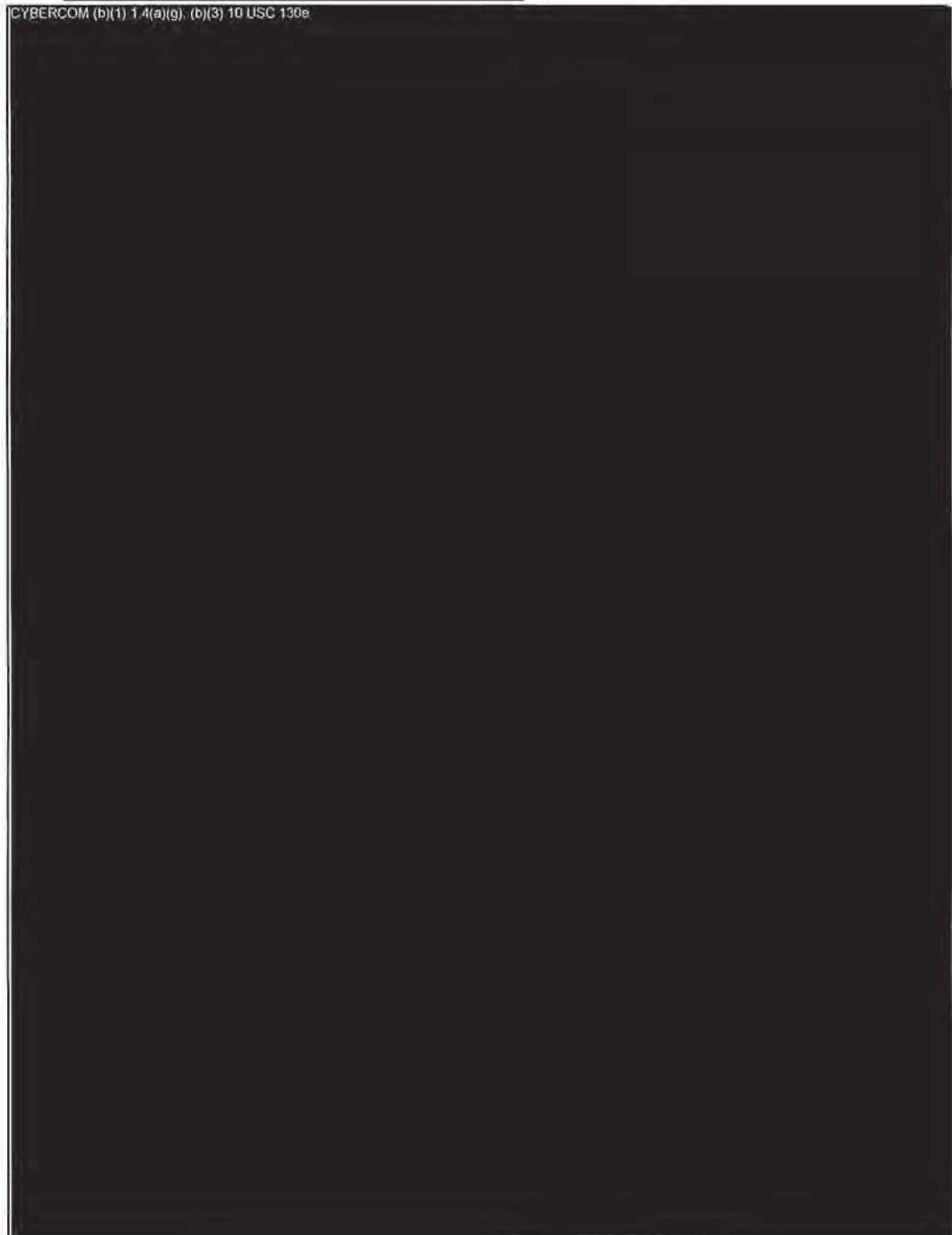


(U)

CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e

(cont'd)

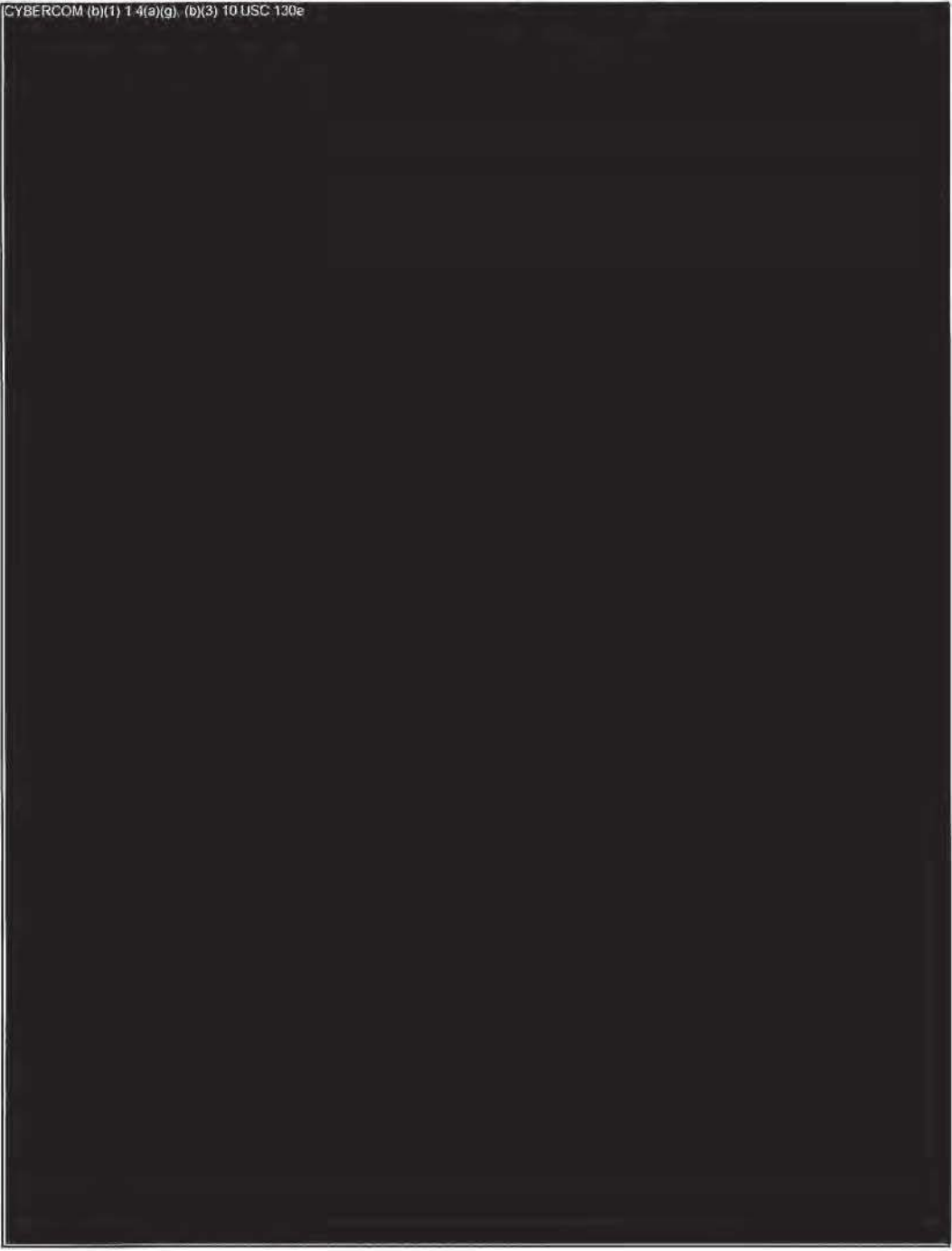
CYBERCOM (b)(1) 1.4(a)(g), (b)(3) 10 USC 130e



Management Comments

(U) CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e (cont'd)

CYBERCOM (b)(1) 1.4(e)(g), (b)(3) 10 USC 130e



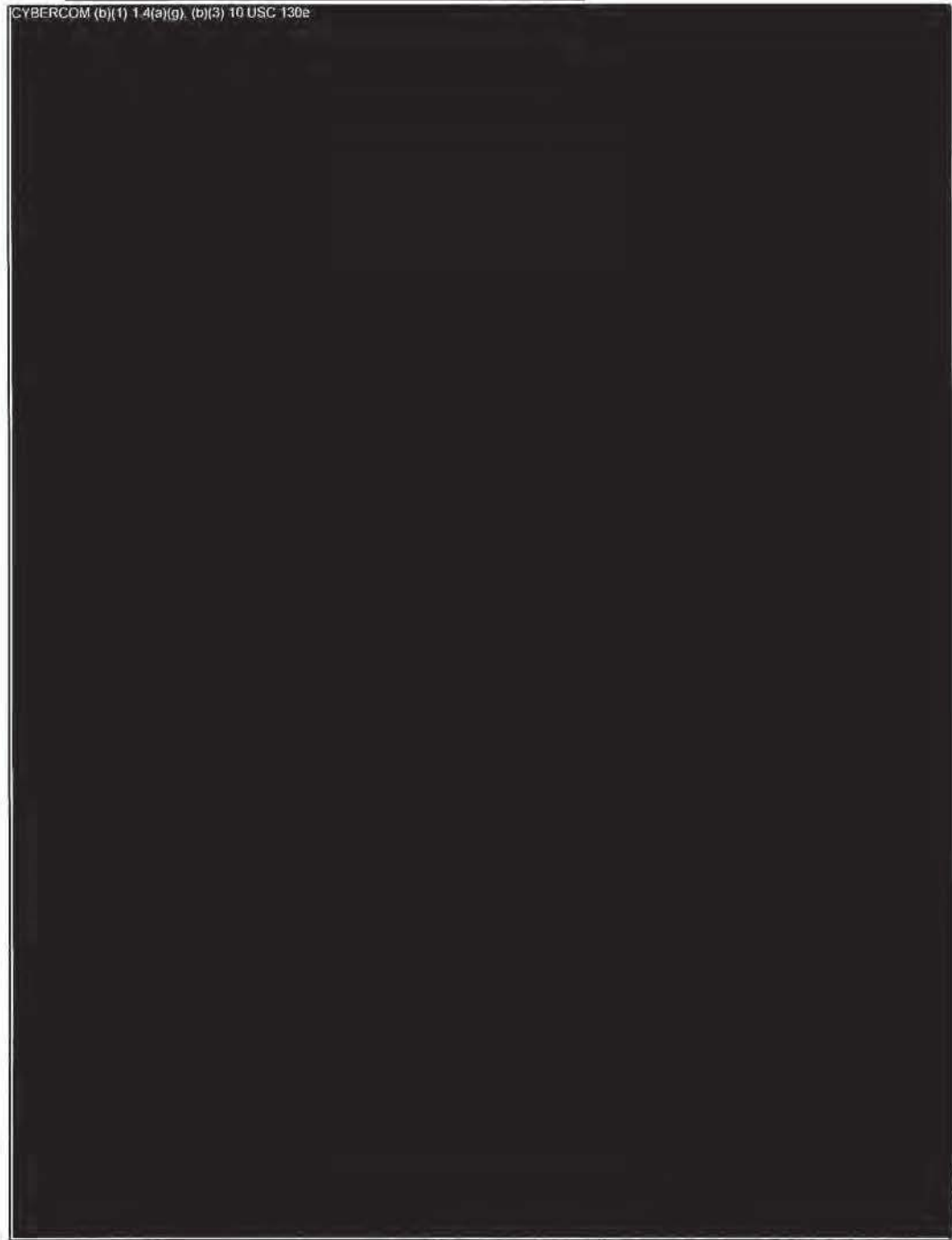
Management Comments

(U) ~~CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e~~

~~CYBERCOM (b)(3) 10 USC 130e~~

Management Comments

(U)  CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e

 CYBERCOM (b)(1) 1.4(a)(g), (b)(3) 10 USC 130e

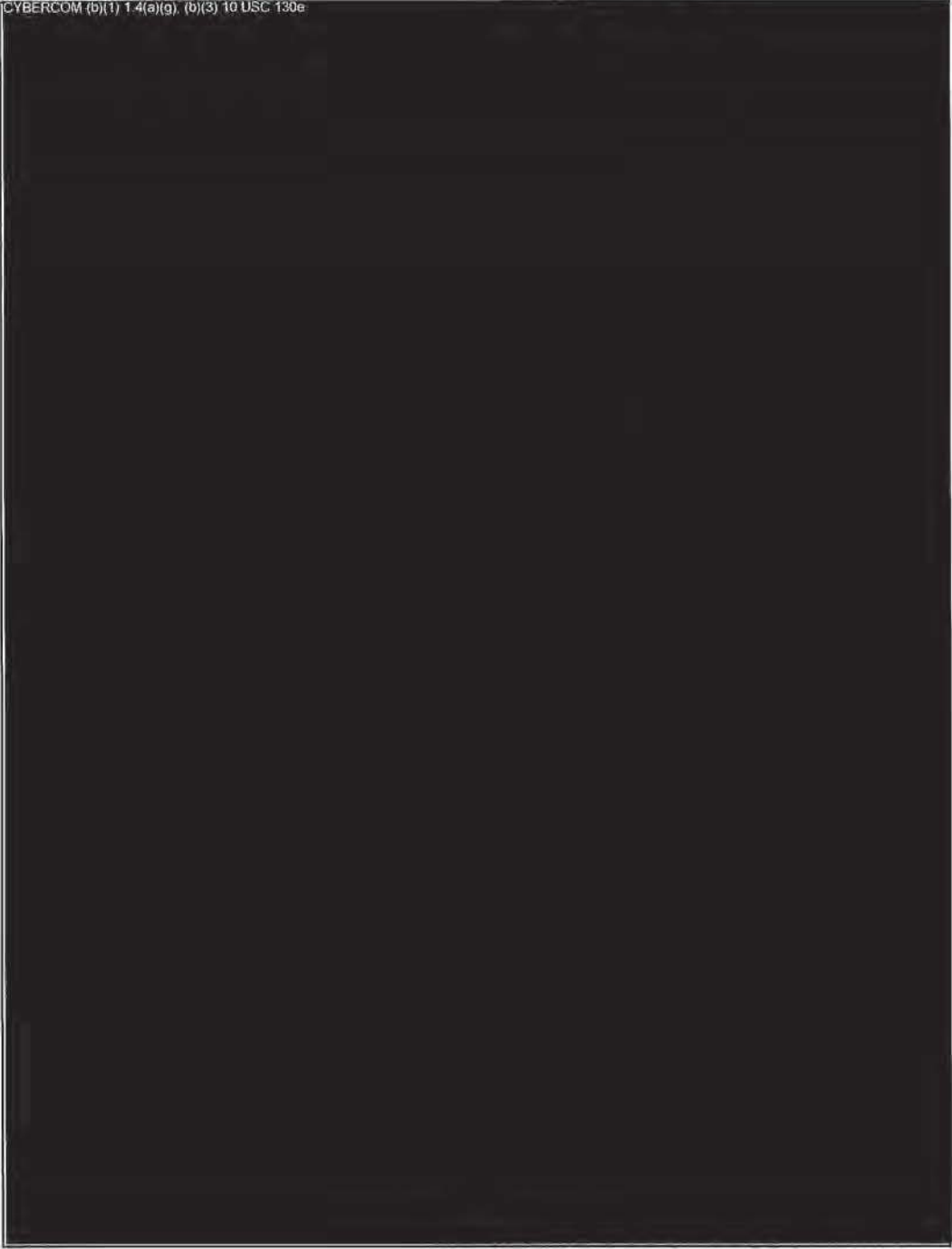
Management Comments

(U)

CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e

(cont'd)

CYBERCOM (b)(1) 1.4(a)(g), (b)(3) 10 USC 130e



Management Comments

(U)

CYBERCOM (b)(1) 1.7(e), (b)(3) 10 USC 130e

CYBERCOM (b)(3) 10 USC 130e

Management Comments

(U) CYBERCOM (b)(1) 1 7(e), (b)(3) 10 USC 130e

(cont'd)

CYBERCOM (b)(3) 10 USC 130e

Management Comments

(U)

CYBERCOM (b)(1) 1 7(e), (b)(3) 10 USC 130e

(cont'd)

CYBERCOM (b)(3) 10 USC 130e



(U) Acronyms and Abbreviations

- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) **CISA** Cybersecurity Infrastructure Security Agency
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) **DODIN** Department of Defense Information Network
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) **IP** Internet Protocol
- (U) **JFHQ** Joint Force Headquarters
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) **NIST** National Institute of Standards and Technology
- (U) **OPORD** Operation Order
- (U) ~~CYBERCOM (b)(3) 10 USC 130e~~
- (U) **POA&M** Plan of Action and Milestones
- (U) **SP** Special Publication

(U) Glossary

(U) Authentication Protocol Resets. Ensure that an attacker cannot create a valid account, which would grant them permission to the domain.

(U) Advanced Persistent Threat. A threat from an adversary with sophisticated levels of expertise and significant resources that executes cyber attacks to gain access into an organization's information technology infrastructure so that it can acquire data or disrupt an organization's mission.

(U) Assured Compliance Assessment Solution. An integrated software solution that provides automated network vulnerability scanning, configuration assessment, and network discovery.

(U) Closed Loop Environment. Has no external connection to an Internet provider and provides encryption for all network traffic.

(U) Command and Control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

(U) Compromise. Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

(U) Cross-Domain Solutions. A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.

(U) Cyber Attack. An attack, through cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure, destroying the integrity of the data, or stealing controlled information.

(U) Department of Defense Information Network (DODIN). A globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to Service members, policy makers, and support personnel, including owned and leased communications and computing systems and services, software, data, security services, other associated services and national security systems.

(U) Domain Name System (DNS). Translates human readable domain names to machine readable Internet protocol addresses.

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

(U) Endpoint. An end-user device, such as a mobile device, laptop, desktop computer, or server.

(U) Exposed. The condition of being in a vulnerable position or situation.

(U) Forensic Image. A duplicate copy of the original system or server.

(U) Host. Any hardware device that has the capability of permitting access to a network by a user interface, specialized software, network address, protocol stack, or any other means. Some examples include computers, personal electronic devices, thin clients, and multi-functional devices.

(U) Internet Protocol (IP). Standard protocol for transmission of data between entities that communicate over the Internet.

(U) Internet Protocol (IP) Address. A unique address that identifies a device on the Internet or a local network. It allows a system to be recognized by other systems connected by the IP.

(U) Kerberos. A computer-network authentication protocol that works on the basis of tickets to allow connection points over a non-secure server to prove their identity to one another in a secure manner.

(U) Malicious Cyber Actor. An individual or organization that uses technology with the intent to cause harm.

(U) Patch. A repair for a piece of programming; also known as a "fix." A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's website.

(U) Plan of Action and Milestones (POA&M). A document that identifies the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

(U) Risk Management. The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organization assets, individuals, other organizations, and the Nation. Includes establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time.

(U) Safeguards. Protective measures prescribed to meet the security requirements specified for an information system. Safeguards may include security features,

(U) management constrains, personnel security, and security of physical structures, areas, and devices.

(U) **Server.** A system entity that provides a service in response to requests from users.

(U) **Sunburst.** A threat actor cluster that is tracked and the behavior is consistent with nation-state activity. The actors behind this campaign have gained access to numerous public and private organizations around the world. They have gained access to victims by trojanized updates to SolarWinds Orion monitoring and management software.

(U) **User Credential Resets.** Ensure that accounts created or modified by the attacker become inaccessible.

(U) **Vulnerability.** Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

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

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

Congressional Liaison

703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists

www.dodig.mil/Mailing-Lists/

Twitter

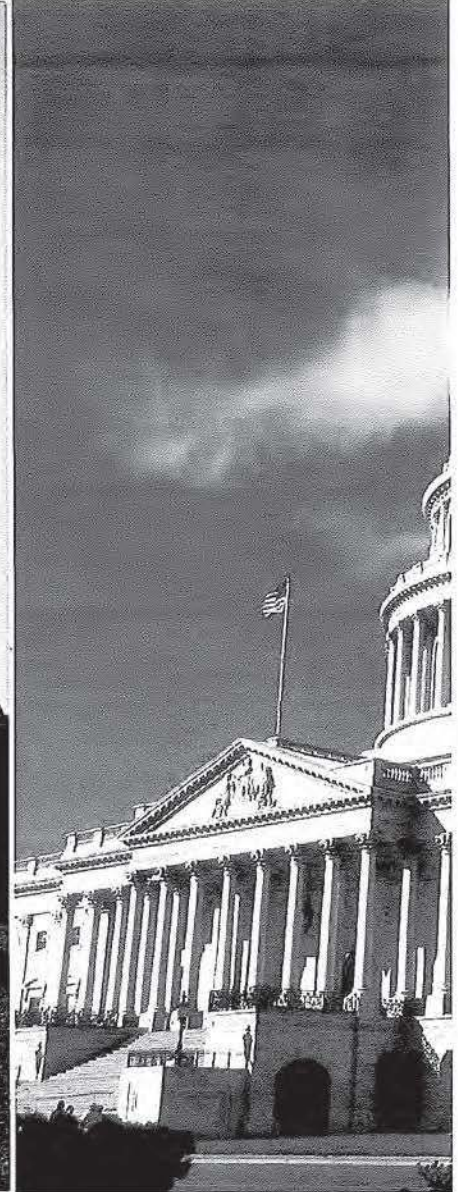
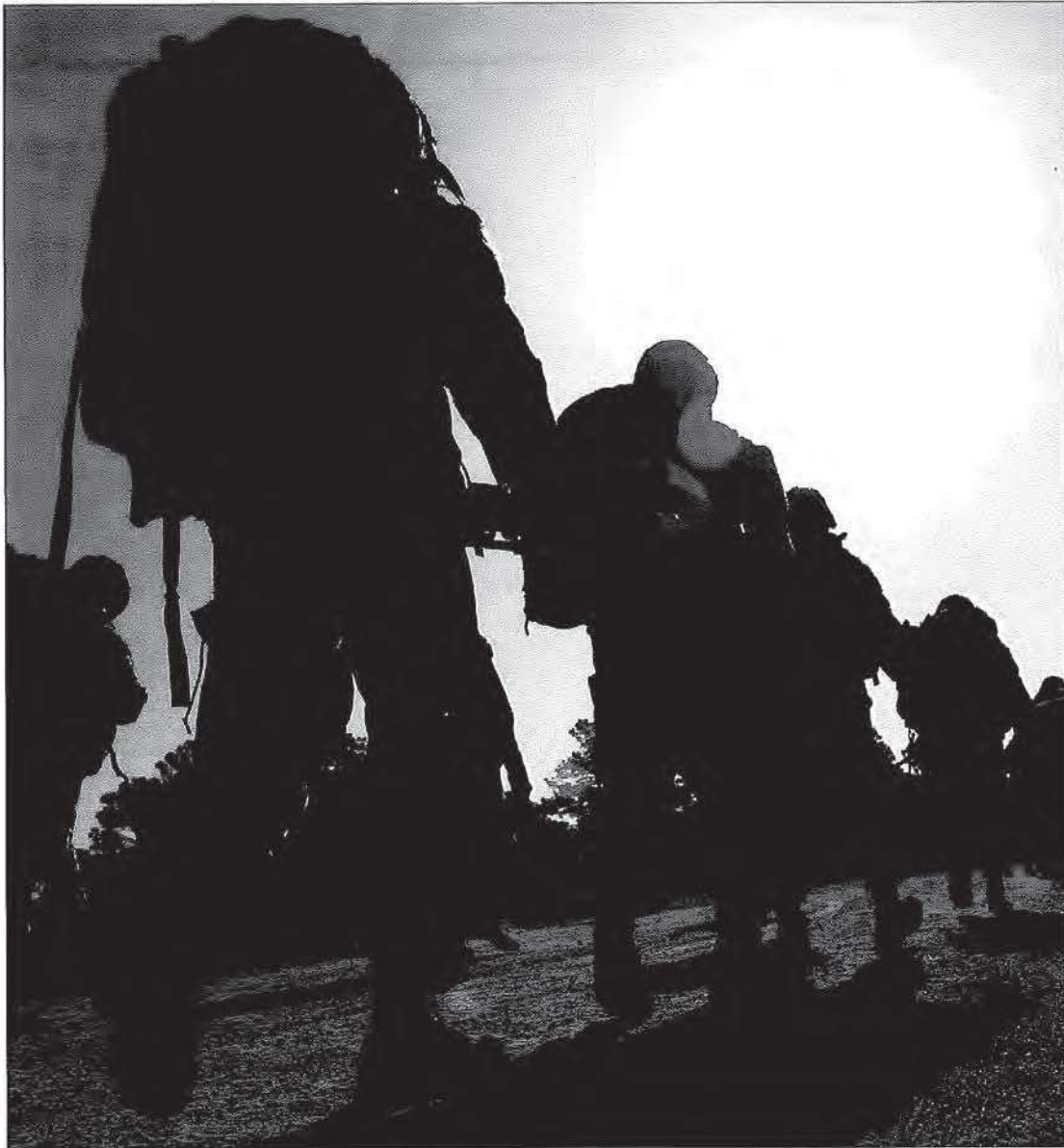
www.twitter.com/DoD_IG

DoD Hotline

www.dodig.mil/hotline

~~SECRET//NOFORN~~

~~SECRET~~//NOFORN



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~SECRET~~//NOFORN

(U) Dissemination List

(U) This is a controlled report and dissemination beyond the groups listed below must be approved.

(U) COMMITTEE ON ARMED SERVICES, UNITED STATES SENATE;

(U) COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, UNITED STATES SENATE;

(U) SUBCOMMITTEE ON DEFENSE, COMMITTEE ON APPROPRIATIONS, UNITED STATES SENATE;

(U) COMMITTEE ON ARMED SERVICES U.S. HOUSE OF REPRESENTATIVES;

(U) COMMITTEE ON OVERSIGHT AND REFORM, U.S. HOUSE OF REPRESENTATIVES;

(U) SUBCOMMITTEE ON DEFENSE, COMMITTEE ON APPROPRIATIONS, U.S. HOUSE OF REPRESENTATIVES;

(U) SECRETARY OF DEFENSE;

(U) DEPUTY SECRETARY OF DEFENSE;

(U) JOINT STAFF;

(U) CYBERCOM (b)(3) 10 USC 130e ;

(U) CYBERCOM (b)(3) 10 USC 130e ;

(U) DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER;

(U) OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT;

(U) HEADQUARTERS U.S. MARINE CORPS;

(U) NATIONAL SECURITY AGENCY;

(U) CYBERCOM (b)(3) 10 USC 130e ;

(U) CYBERCOM (b)(3) 10 USC 130e ;

(U) CYBERCOM (b)(3) 10 USC 130e ;

(U) CYBERCOM (b)(3) 10 USC 130e ;

(U) JOINT FORCE HEADQUARTERS DOD INFORMATION NETWORK;

(U) OFFICE OF THE INSPECTOR GENERAL OF THE UNITED STATES ARMY;

(U) CYBERCOM (b)(3) 10 USC 130e ;

(U) DEPARTMENT OF THE AIR FORCE INSPECTOR GENERAL;

(U) CYBERCOM (b)(3) 10 USC 130e ;

~~SECRET//NOFORN~~

(U) ~~CYBERCOM (b)(3) 10 USC 130e~~;

(U) U.S. ARMY AUDIT AGENCY;

(U) AIR FORCE AUDIT AGENCY;

(U) NAVAL AUDIT SERVICE;

(U) ~~CYBERCOM (b)(3) 10 USC 130e~~;

(U) ~~CYBERCOM (b)(3) 10 USC 130e~~; AND

(U) ~~CYBERCOM (b)(3) 10 USC 130e~~

~~SECRET//NOFORN~~