

INSPECTOR GENERAL

U.S. Department of Defense

AUGUST 29, 2016



(U//FOUO) The National Security Agency Should Take Additional Steps to Effectively Implement Its Privileged Access-Related Secure-the-Net Initiatives

Classified By: Carol N. German
Derived From: Multiple Sources
Declassify On: 20410900

Report 26 of 35

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

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

Vision

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



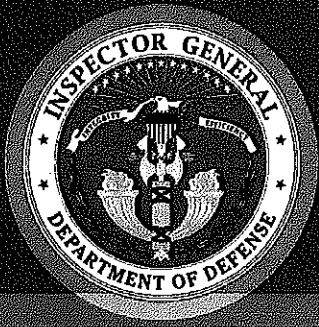
Fraud, Waste & Abuse

HOTLINE

Department of Defense

dodig.mil/hotline | 800.424.9098

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



(U) Results in Brief

(U//FOUO) The National Security Agency Should Take Additional Steps to Effectively Implement Its Privileged Access-Related Secure-the-Net Initiatives

(U) August 29, 2016

(U) Objective

~~(S//REL TO USA, FVEY)~~ We determined whether the National Security Agency (NSA) effectively implemented its privileged access¹-related Secure-the-Net (STN) initiatives. This report is one in a series in response to a congressional request in the classified annex to the Intelligence Authorization Act of FY 2016. This act requires the DoD Inspector General to assess whether NSA remedied the vulnerabilities exploited by a security breach² and completed all STN initiatives.

(U) Background

~~(S//REL TO USA, FVEY)~~ After the security breach, NSA began developing and implementing 40 STN initiatives. The STN initiatives focused on insider threats to NSA systems, data, and infrastructure. For this audit, we focused on 7 of the 40 STN initiatives that we determined presented the highest risk to NSA's ability to secure network access, protect against insider threats, and provide increased oversight of personnel with privileged access.

¹ (U) A level of access that is significantly greater than users performing normal operations.

² ~~(S//REL TO USA, FVEY)~~ Between August 2012 and May 2013, an NSA contractor in Hawaii exfiltrated about 1.5 million classified and sensitive documents from NSA systems.

Visit us at www.dodig.mil

(U) Finding

~~(U//FOUO)~~ NSA officials effectively implemented or partially implemented four of the seven privileged access-related STN initiatives included in our audit:

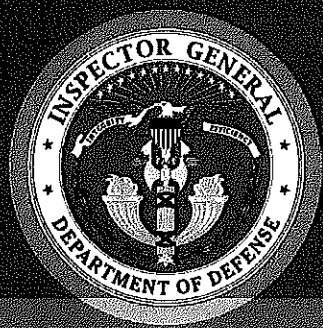
- develop and document a plan for a new system administration model;
- assess the number of system administrators³ across the enterprise;
- implement two-person access controls over data centers and machine rooms; and
- implement two-stage authentication controls for system administration.

~~(S//REL TO USA, FVEY)~~ However, NSA did not have guidance concerning key management and did not consistently secure server racks and other sensitive equipment in the data centers and machine rooms in accordance with the initiative requirements and policies, and did not extend two-stage authentication controls to all high-risk users.

~~(S//REL TO USA, FVEY)~~ In addition, NSA officials did not effectively implement three privileged access-related STN initiatives:

- fully implement technology to oversee privileged user activities;
- effectively reduce the number of privileged access users; and
- effectively reduce the number of authorized data transfer agents.

³ (U) System administrators have privileged access to maintain, configure, and operate computer systems.



(U) Results in Brief

(U//FOUO) The National Security Agency Should Take Additional Steps to Effectively Implement Its Privileged Access-Related Secure-the-Net Initiatives

(U) Findings (cont'd)

~~(S//REL TO USA, FVEY)~~ NSA did not effectively implement the three STN initiatives because it did not develop an STN strategy that detailed a structured framework and methodology to implement the initiatives and measure completeness. As a result, NSA's actions to implement STN did not fully meet the intent of decreasing the risk of insider threats to NSA operations and the ability of insiders to exfiltrate data.

(U) Recommendations

(U) We recommend that the Director, Technology Directorate, NSA/Central Security Service Chief Information Officer:

- ~~(S//REL TO USA, FVEY)~~ update NSA/Central Security Service Policy 6-16 to include procedures requiring data center and machine room managers to effectively manage keys to server racks;
- ~~(S//NF)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)
- ~~(S//REL TO USA, FVEY)~~ develop a strategy to expand two-stage authentication controls and implement automated, technology-based monitoring for all administrators;

(U) Recommendations (cont'd)

- ~~(U//FOUO)~~ NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)
- ~~(U//FOUO)~~ NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

(U) Management Comments and Our Response

~~(S//NF)~~ The Director, Technology Directorate, NSA/Central Security Service Chief Information Officer, agreed with all recommendations. However, the comments did not fully address all specifics of the recommendations. The Director did not include all system and network administrators in his strategy to expand two-stage authentication controls and did not implement capabilities to provide ~~NSA/CSS: (b) (1)~~ technology-based monitoring across the entire privileged access community. In addition, the Director did not identify specific actions NSA would take to ensure approvers used consistent processes to grant privileged access or data transfer authority. Therefore, we request that the Director, Technology Directorate, NSA/Central Security Service Chief Information Officer, provide additional documentation and comments on this final report by September 27, 2016. Please see the Recommendations Table on the back of this page.

* EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Recommendations Table

UNCLASSIFIED Management	Recommendations Requiring Comment	No Additional Comments Required
Director, Technology Directorate, NSA/CSS Chief Information Officer	2.a, 2.b, 3.a	1.a, 1.b, 3.b, 3.c UNCLASSIFIED

(U) Please provide Management Comments by September 27, 2016.



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

August 29, 2016

(U) MEMORANDUM FOR DIRECTOR, TECHNOLOGY DIRECTORATE, NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE CHIEF INFORMATION OFFICER


(U//~~FOUO~~) SUBJECT: The National Security Agency Should Take Additional Steps to Effectively
Implement Its Privileged Access-Related Secure-the-Net Initiatives
(Report No. DODIG-2016-129)

(S//~~REL TO USA, FVEY~~) We are providing this report for review and comment. We conducted this audit in response to a congressional requirement. NSA effectively implemented or partially implemented four of the seven privileged access-related Secure-the-Net initiatives included in our audit. However, NSA did not effectively implement the other three initiatives. Consequently, NSA did not fully meet the intent of decreasing the risk of insider threats to its operations and the ability of insiders to exfiltrate data.

(U) We considered management comments on a draft of this report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Director, Technology Directorate, NSA/Central Security Service Chief Information Officer, partially addressed Recommendations 2.a, 2.b, and 3.a. Therefore, we request that the Director, Technology Directorate, NSA/Central Security Service Chief Information Officer, provide additional comments on those recommendations by September 27, 2016.

(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 ^{DoD OIG: (b) (6)} [redacted] and ^{DoD OIG: (b) (6)} [redacted]. 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 329-7331).


Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) Contents

(U) Introduction.....	1
(U) Objective.....	1
(U) Background.....	1
(U) NSA Mission and Infrastructure.....	1
(U) STN Initiatives.....	2
(U) NSA Responsibilities for Implementing STN Initiatives.....	4
(U) Review of Internal Controls.....	4
(U) Finding.....	5
(U// FOUO) NSA Did Not Fully Complete and Effectively Implement All PRIVAC-Related Initiatives.....	5
(U) NSA Effectively Implemented Two and Made Progress in Completing Two PRIVAC-Related Initiatives...	6
(U// FOUO) NSA Developed a New System Administration Model.....	6
(U) NSA Assessed the Number of SAs and Removed PRIVAC for Users Who Did Not Require It.....	7
(U// FOUO) NSA Partially Implemented TPA Controls Over DCMs.....	9
(C//REL TO USA, FVEY) NSA Partially Implemented TSA Controls.....	13
(U// FOUO) NSA Did Not Effectively Implement Three PRIVAC-Related Initiatives.....	17
(U// FOUO) NSA Did Not Effectively Implement Technology to Monitor PRIVAC Activities.....	17
(U// FOUO) NSA Did Not Reduce the Number of Privileged Users.....	19
(U// FOUO) NSA Did Not Reduce the Number of DTAs.....	20
(U// FOUO) NSA Lacked a Comprehensive Strategy to Effectively Implement PRIVAC-Related STN Initiatives.....	22
(U// FOUO) Insider Threat Risks Remain Despite Implementing PRIVAC-Related STN Initiatives.....	23
(U) Management Comments on the Finding and Our Response.....	24
(U) Management Comments on NSA's Approach to Completing STN Initiatives.....	24
(U) Our Response.....	25
(U) Management Comments on Reducing Insider Threat Risks.....	25
(U) Our Response.....	26
(U) Recommendations, Management Comments, and Our Response.....	26
(U) Recommendation 1.....	26
(U) Recommendation 2.....	28
(U) Recommendation 3.....	30

(U) Appendix A 32
(U) Scope and Methodology32
(U) Use of Computer-Processed Data33
(U) Use of Technical Assistance.....34
(U) Prior Coverage.....34
(U) Appendix B 35
(U) STN Initiatives.....35
Management Comments 39
(U) National Security Agency.....39
(U) Glossary 45
(U) Source of Classified Information 48
(U) Acronyms and Abbreviations..... 50

(U) Introduction

(U) Objective

(U) Our audit objective was to determine whether the National Security Agency (NSA) Secure-the-Net (STN) initiatives were effectively implemented to improve security controls over NSA's data, systems, and personnel activities. This report is one in a series on the implementation of NSA's STN initiatives and focuses on the controls to limit privileged access (PRIVAC)⁴ to NSA systems and data, and to monitor privileged user actions for unauthorized or inappropriate activity. Please see Appendix A for scope and methodology and prior audit coverage related to the objective.

(U) The classified annex to the Intelligence Authorization Act for FY 2016 requires the DoD Office of Inspector General (OIG) to assess whether NSA remedied the vulnerabilities exploited by a security breach and completed all STN initiatives.⁵

(U) Background

(U) NSA Mission and Infrastructure

~~(C//REL TO USA, FVEY)~~ NSA/Central Security Service (CSS) leads U.S. Government cryptology⁶ operations focused on signals intelligence and information assurance products and services, and enables computer network operations to gain a decision making advantage for the United States and its allies. NSA uses advanced information technology to store, process, and protect its activities and information. NSA's enterprise

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



⁴ (U) NSA/CSS Policy Instruction 6-0001, "NSA/CSS Privileged Access," January 20, 2016, defines PRIVAC as a higher level of access than the access needed to perform normal processes and system operations.

⁵ (U) The congressional request was included in the classified annex to H.R. 114-144 to accompany H.R. 2596. H.R. 2596 was incorporated into H.R. 4127, the final version of the Intelligence Authorization Act for FY 2016. H.R. 4127 was included in P.L. 114-113, "Consolidated Appropriations Act, 2016," December 18, 2015.

⁶ (U) Cryptology is the art and science of making and breaking codes and ciphers. NSA/CSS is responsible for creating the systems that protect U.S. communications and for analyzing systems and communications used by foreign powers.

(U) Finding

~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) STN Initiatives

~~(C//REL TO USA, FVEY)~~ NSA was evaluating its security posture when the unauthorized disclosures of classified data in June 2013⁷ prompted it to implement additional processes and security measures to protect its infrastructure, systems, and data against insider threats. Specifically, in June 2013, NSA began developing and implementing 40 STN initiatives⁸ to improve controls over NSA computer systems and data, and increase oversight of its personnel. NSA's approach to implement the STN campaign was based on the size and complexity of their infrastructure and organization, and focused primarily on increasing layered protection to reduce the risk of insider threats. See Appendix B for a list and description of the 40 STN initiatives. The Director, NSA, requested completion of all STN initiatives by June 2015.⁹ In June 2015, NSA reported to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence that it had completed 34 of the 40 STN initiatives.

~~(U//FOUO)~~ For this audit, we focused on 7 of the 40 STN initiatives that we determined presented a higher risk to NSA's ability to secure network access, protect against insider threats, and provide increased oversight of personnel with PRIVAC to NSANet, network devices, and infrastructure. Those seven initiatives are as follows:

- ~~(U//FOUO)~~ develop and document a new system administration model (initiative 22 in Appendix B),
- ~~(U//FOUO)~~ assess the number of system administrators (SAs)¹⁰ across the enterprise (initiative 34),

⁷ ~~(C//REL TO USA, FVEY)~~ Between August 2012 and May 2013, an NSA contractor in Hawaii exfiltrated about 1.5 million classified and sensitive documents from NSA systems through various techniques.

⁸ ~~(U//FOUO)~~ The number of STN initiatives changed over time; however, as of June 2015, NSA reported 40 STN initiatives to the House Permanent Select Committee on Intelligence.

⁹ ~~(U//FOUO)~~ In September 2014, the NSA Chief Information Officer updated the Director, NSA on the status of completing the STN initiatives. Although NSA officials stated that the Director approved an extension for completing eight of the STN initiatives, the documentation provided did not support that decision.

¹⁰ (U) SAs have PRIVAC to maintain, configure, and operate computer systems.

- (U//~~FOUO~~) implement two-person access (TPA) control over data centers and machine rooms¹¹ (DCMs) (initiative 21),
- (U//~~FOUO~~) implement two-stage authentication (TSA) control for system administration (initiative 4),¹²
- (U//~~FOUO~~) reduce the number of personnel with PRIVAC (initiative 35),
- (U//~~FOUO~~) reduce the number of authorized data transfer agents (DTAs) (initiative 33),¹³ and
- (U//~~FOUO~~) oversee privileged user activities (initiative 36).

(U) We nonstatistically selected the following four NSA installations to include in our audit:

- (U//~~FOUO~~) NSA Washington serves as NSA headquarters, NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) and is located in the Northeast region.
- (U//~~FOUO~~) NSA Texas is one of the four NSA cryptologic centers, NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
- (U//~~FOUO~~) NSA Utah Data Center is a comprehensive national cybersecurity intelligence data center located in the West region.
- (U//~~FOUO~~) North Carolina State University Laboratory for Analytic Sciences primarily supports research and development, and is located in the Southeast region.

¹¹ (U//~~FOUO~~) DCMs are facilities that host computing systems, servers, data storage, and machine rooms.

¹² (U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

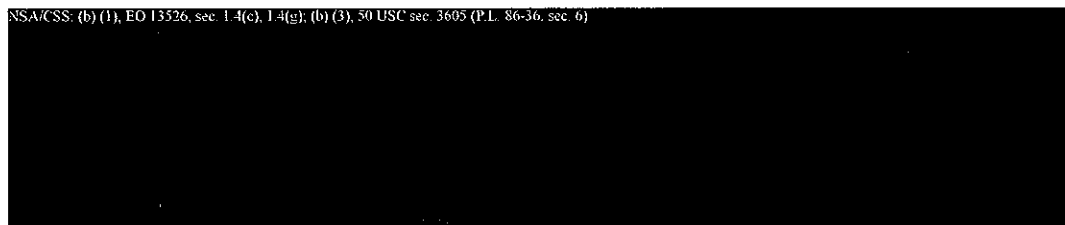
¹³ (U//~~FOUO~~) DTAs are designated personnel approved by an authorizing officer to use removable media to transfer data to or from an NSA/CSS information system.

¹⁴ (C//REL TO USA, FVEY) The four cryptologic centers are located in Texas, Georgia, Hawaii, and Colorado.

(U) NSA Responsibilities for Implementing STN Initiatives

~~(C//REL TO USA, FVEY)~~ STN is an ongoing campaign requiring involvement from all NSA directorates; however, the NSA Technology Directorate is the primary lead for implementing the initiatives.¹⁵ The Directorate, led by the Chief Information Officer,

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



~~(U//FOUO)~~ The NSA Associate Directorate for Security and Counterintelligence protects worldwide NSA/CSS information, personnel, activities, and facilities through its internal counterintelligence programs. The NSA Associate Director for Security and Counterintelligence appoints security personnel to provide guidance and assist NSA personnel in making security-related decisions.

(U) Review of Internal Controls

~~(C//REL TO USA, FVEY)~~ DoD Instruction 5010.40¹⁶ requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses related to the initiatives we reviewed. Specifically, NSA did not develop a strategy and a detailed implementation plan that clearly described the process for implementing and measuring progress toward completing the STN initiatives. Additionally, NSA did not consistently secure server racks and other sensitive equipment inside the DCMs and did not implement an

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

We will provide a copy of the report to the senior official responsible for internal controls at NSA.

¹⁵ (U) NSA is planning to restructure its organization beginning on or around August 1, 2016. The NSA nomenclatures and directorate references used in this report are based on its structure as of July 2016.

¹⁶ (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

(U) Finding

(U//~~FOUO~~) NSA Did Not Fully Complete and Effectively Implement All PRIVAC-Related Initiatives

(U//~~FOUO~~) NSA officials effectively implemented or partially implemented four of the seven PRIVAC-related STN initiatives included in our audit:

- develop and document a plan for a new system administration model;
- assess the number of all SAs across the enterprise;
- implement TPA controls over DCMs; and
- implement TSA controls for system administration.

(~~C//REL TO USA, FVEY~~) However, NSA did not have guidance concerning key management and did not consistently secure server racks and other sensitive equipment in the DCMs in accordance with requirements and policies, and did not extend two-stage authentication controls to all high-risk users.

(~~C//REL TO USA, FVEY~~) In addition, NSA officials did not effectively implement three PRIVAC-related STN initiatives:

- fully implement technology to oversee privileged user activities;
- effectively reduce the number of privileged users; and
- effectively reduce the number of authorized DTAs.

(~~C//REL TO USA, FVEY~~) NSA did not effectively implement the three initiatives because it did not develop an STN strategy that detailed a structured framework and methodology to implement the initiatives and measure completeness. As a result, NSA's actions to implement STN did not fully meet the intent of decreasing the risk of insider threats to NSA operations and the ability of insiders to exfiltrate data.

(U) NSA Effectively Implemented Two and Made Progress in Completing Two PRIVAC-Related Initiatives

(U//~~FOUO~~) NSA effectively implemented two and partially implemented two of the seven STN initiatives included in our audit. Specifically, NSA developed and implemented a new system administration model, and assessed the number of SAs across the enterprise and removed PRIVAC from users who did not require elevated levels of access. In addition, NSA partially implemented TPA controls over DCMs and TSA controls for SAs, but will not meet the full intent of the ongoing initiatives without taking additional actions.

(U//~~FOUO~~) NSA Developed a New System Administration Model

(U//~~FOUO~~) NSA developed the NSA/CSS Enterprise Administration Model for system administration (initiative 22) and implemented NSA/CSS Policy Instruction 6-0001¹⁷ to increase oversight of privileged users and define levels of PRIVAC. NSA documentation identified that it completed the initiative to develop a tiered-system administration model to limit PRIVAC based on assigned tasks in December 2014. To assess NSA's actions taken to complete the initiative, we reviewed the system administration model and verified it contained tiered levels of access and defined different types of privileged users. We also reviewed and verified the accompanying policy that defined each level of access and the overall PRIVAC process.

(C//~~REL TO USA, FVEYX~~) NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

[REDACTED]

[REDACTED]

¹⁷ (U) NSA/CSS Policy Instruction 6-0001, "NSA/CSS Privileged Access," January 20, 2016, defines privileged access, implements procedures, and assigns responsibilities for PRIVAC to NSA/CSS information systems.

~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6). In December 2014, NSA established a tiered-pyramid system administration model that identified users as either NSA/CSS: (b) (1).^{*} The new system administration model categorized users based on the following levels of access:

- (U) Tier 3 (SYS3): NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
- (U) Tier 2 (SYS2): NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
- (U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
- (U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
- (U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]

(U) NSA Assessed the Number of SAs and Removed PRIVAC for Users Who Did Not Require It

(U//FOUO) NSA assessed the number of SAs across the enterprise and removed PRIVAC based on the tiered model (initiative 34). NSA documentation identified it completed the initiative to identify the number of SAs across the enterprise and remove PRIVAC from users who did not require elevated levels of access to perform assigned duties in August 2013. To assess NSA's actions taken to complete the initiative, we met with NSA officials to determine actions taken to identify privileged users immediately following the June 2013 security breach, and reviewed the system administration model and

¹⁸ (U) Public key infrastructure supports digital signature and other security mechanisms for DoD functional enterprise programs.

^{*} EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED] We also observed the process for requesting and approving PRIVAC [REDACTED] NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] NSA identified and categorized privileged users who performed SA functions in three distinct tiers in accordance with Office of the Director of National Intelligence requirements. [REDACTED] NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

¹⁹ (U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

²⁰ (U) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

²¹ (U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//~~FOUO~~) NSA Partially Implemented TPA Controls Over DCMs

(~~C//REL TO USA, FVEY~~) NSA made progress in implementing TPA controls over DCMs (initiative 21), but may not meet the full intent of the initiative without taking additional actions. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

- (U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED]
- (U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED]
- (U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED]
- (U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED]

(U//~~FOUO~~) To assess NSA's actions taken to complete the initiative at the four sites visited, we reviewed NSA policies and site standard operating procedures, interviewed DCM managers and other personnel NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED] We also conducted walkthroughs of the DCMs NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED] conducted tests to NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED] and reviewed logs NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED]

[REDACTED] Furthermore, we attempted to access server racks NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) [REDACTED]

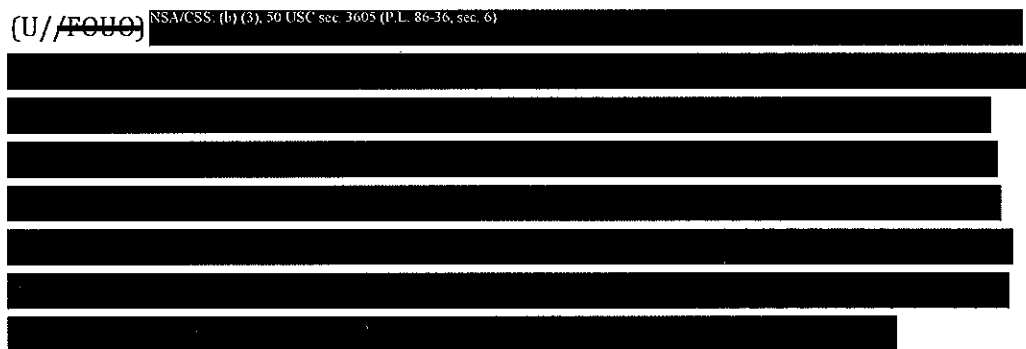
(U) NSA Updated Procedures to Access DCMs

~~(S//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



(U) Consistent Processes to Authorize Access to DCMs Were Followed

~~(U//FOUO)~~ NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



²² (U) NSA/CSS Policy 6-16, "Management of Information Technology Data Centers," July 31, 2010 (revised on May 27, 2014), establishes policy for securing and managing NSA/CSS information technology data centers.

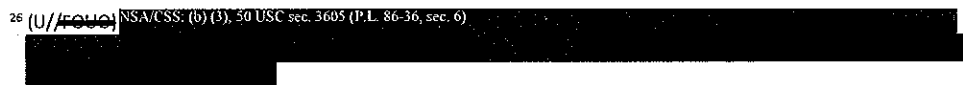
²³ ~~(U//FOUO)~~ NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



²⁴ (U) NSA-controlled sites are locations where NSA is the host. Non-NSA-controlled sites are locations where NSA is the tenant.

²⁵ (U) We visited three NSA-controlled sites (NSA Washington, NSA Texas, and the Utah Data Center) and one non-NSA-controlled site (North Carolina State University Laboratory of Analytic Sciences).

²⁶ ~~(U//FOUO)~~ NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



(U) Finding

~~(U//FOUO)~~

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(U//FOUO)~~

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

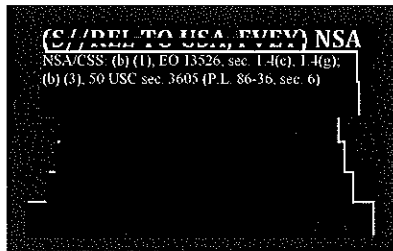
~~(S//REL TO USA, FVEY)~~

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(S//REL TO USA, FVEY)~~

NSA did not consistently secure server racks and other sensitive equipment in the DCMs in accordance with the initiative

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



~~(S//NF)~~

At NSA Texas, the Utah Data Center, and North Carolina State University Laboratory of Analytic Sciences, we observed unlocked server racks and sensitive equipment.

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Finding

(S//NF) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6); (b) (5)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S//NF) NSA also was not providing sufficient oversight of personnel and equipment inside DCMs. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

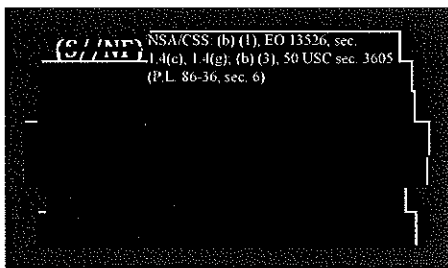
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Not locking server and equipment racks and [REDACTED]

²⁷ (U) NSA Inspector General Report No. AU-14-0005, "Audit of NSANet Server Security," June 19, 2015.

* EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(S//NF)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~(C//REL TO USA, FVEY)~~ **NSA Partially Implemented TSA Controls**

~~(C//REL TO USA, FVEY)~~ NSA made progress in implementing TSA controls for its highest risk administrators ~~(S//NF)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), * but may not meet the full intent of the initiative (initiative 4) without taking additional actions. NSA began implementing the

NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~(C//REL TO USA, FVEY)~~ To assess NSA's actions taken to complete the initiative, we reviewed policies and procedures for monitoring and auditing privileged user activities.

NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] We also tested whether TSA controls prevented personnel from accessing systems, devices, or networks not previously approved.

²⁸ ~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

²⁹ ~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

* 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Finding

(S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

(S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

(S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

30 (U) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

31 (S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

32 (U) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

33 (U) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(C//REL TO USA, FVEY)~~ TSA Controls Were Not Fully Implemented for High-Risk Administrators

~~(C//REL TO USA, FVEY)~~ NSA did not fully implement TSA controls for its highest risk administrators. NSA/CSS (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

[REDACTED]. NSA officials stated that they did not follow a formal process or define specific parameters to assess which SYS2 users to include in their initial deployment of the additional authentication requirements.

~~(C//REL TO USA, FVEY)~~ NSA officials stated that they did not follow a formal process or define specific parameters to assess which SYS2 users to include in their initial deployment of the additional authentication requirements.

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

[REDACTED] additional actions are needed to ensure all high risk administrators are required to use TSA controls. Table 1 NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Table 1 NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(C//REL TO USA, FVEY)	[REDACTED]	[REDACTED]	[REDACTED]
NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)			
[REDACTED]	[REDACTED]	[REDACTED]	(C//REL TO USA, FVEY)

*~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Finding

~~(C//REL TO USA, FVEY)~~ NSA Did Not Implement TSA Controls for All System and Network Administrators

~~(S//REL TO USA, FVEY)~~ NSA did not implement TSA controls for all its system and network administrators. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted text block]

~~(C//REL TO USA, FVEY)~~ NSA
NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3),
50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Table 2. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

Table with redacted content and classification markings.

³⁴ ~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//~~FOUO~~) NSA Did Not Effectively Implement Three PRIVAC-Related Initiatives

~~(C//REL TO USA, FVEY)~~ NSA did not effectively implement three PRIVAC-related initiatives. Specifically, NSA did not effectively implement technology to provide oversight of all privileged user activities, and did not reduce the number of users with PRIVAC and data transfer authority.

(U//~~FOUO~~) NSA Did Not Effectively Implement Technology to Monitor PRIVAC Activities

~~(C//REL TO USA, FVEY)~~ NSA did not fully implement technology-based capabilities to oversee the activities of privileged users (initiative 36). NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

[REDACTED]

[REDACTED] To assess NSA's actions taken to complete the initiative, we reviewed the system administration model and verified it contained tiered levels of access and defined different types of privileged users. NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Finding

(S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

NSA did not implement technology-based capabilities to monitor privileged users.

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(S//REL TO USA, FVEY) NSA

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

35 (S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

36 (U//FOUO) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

37 (S//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

38 (U) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(U//FOUO)~~ NSA Did Not Reduce the Number of Privileged Users

~~(C//REL TO USA, FVEY)~~ NSA took steps to identify, but not to reduce, the number of privileged users across its enterprise (initiative 35). NSA documentation identified that it completed the initiative to reduce the number of privileged users from ~~NSA/CSS: (b) (1), *~~ in July 2013. Although repeatedly requested, NSA officials could not provide supporting documentation that showed the number of privileged users before and after the purge or the actual number of users purged. Therefore, to assess NSA's actions taken to complete the initiative, we requested prior reports or spreadsheets supporting the number of privileged users and interviewed NSA officials to identify the process they followed for establishing a baseline. We used e-mails that included statistics for specific points in time beginning in March 2014 to validate the number of privileged users.

~~(C//REL TO USA, FVEY)~~
NSA did not support its preliminary baseline of privileged users or its goal for reducing privileged users to ~~NSA/CSS: (b) (1), *~~

~~(C//REL TO USA, FVEY)~~ Before implementing the initiative, the NSA did not know how many users had PRIVAC across the enterprise. In June 2013, shortly after the security breach, NSA reported to the Office of the Director of National Intelligence that it had ~~NSA/CSS: (b) (1), *~~ privileged users. NSA officials

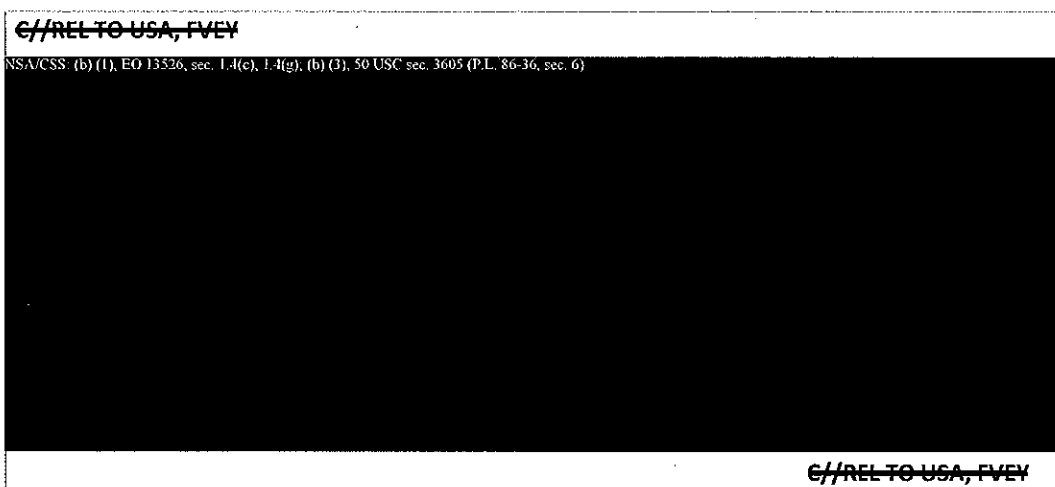
stated that they used a manually kept spreadsheet, which they no longer had, to identify the initial number of privileged users. In addition to not being able to support the number of privileged users reported to the Office of the Director of National Intelligence, NSA did not support its preliminary baseline of ~~NSA/CSS: (b) (1), *~~ privileged users or its goal for reducing privileged users to ~~NSA/CSS: (b) (1), *~~. The NSA DCIO stated that NSA arbitrarily removed PRIVAC from ~~NSA/CSS: (b) (1), *~~ users and required those users to submit e-mail requests to the NSA Associate Directorate for Security and Counterintelligence and the CIO's office to re-obtain PRIVAC between July 2013 and September 2013. The NSA DCIO stated that NSA considered the individual e-mails and justification before reauthorizing PRIVAC for any user.

~~(C//REL TO USA, FVEY)~~ NSA took a zero-based approach to remove PRIVAC from the ~~NSA/CSS: (b) (1), *~~ users and required them to re-enroll using ~~NSA/CSS: (b) (1), *~~ however, NSA did not use a zero-based approach for the remaining privileged users. Several NSA privileged users we interviewed confirmed that NSA removed their PRIVAC and required them to

* EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(C//REL TO USA, FVEY)~~ submit a justification in ~~NSA/CSS: (b) (1), *~~ to re-obtain PRIVAC. Although the actions taken by NSA established a baseline of the number of personnel with PRIVAC, NSA should have used the baseline as its starting point to reduce privileged users instead of using the baseline to report a reduction in privileged users. Figure 1 shows a timeline of NSA's actions between June 2013 and May 2016 to identify privileged users as well as a continued and consistent increase in the number of privileged users once the ~~NSA/CSS: (b) (1), *~~ enrollment process began.

(U) Figure 1. Timeline of NSA Actions to Identify and Reduce Privileged Users



(U) Source: DoD OIG

(U//FOUO) NSA Did Not Reduce the Number of DTAs

~~(C//REL TO USA, FVEY)~~ NSA did not reduce the number of DTAs (initiative 33). NSA documentation identified that it completed the initiative to reduce the number of DTAs in March 2014. Although repeatedly requested, NSA officials could not provide supporting documentation for the total number of DTAs before and after the purge or the actual number of users purged. Therefore, to assess NSA's actions taken to complete the initiative, we requested prior reports or spreadsheets supporting the number of DTAs and interviewed NSA officials to identify the process they followed for establishing a baseline. To validate the number of DTAs, we reviewed e-mails that included statistics for specific points in time to identify the number of DTA requests and approvals because ~~NSA/CSS: (b) (1), *~~ could not generate a report covering previous periods.

* EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(C//REL TO USA, FVEY)~~ Before the STN campaign, NSA did not know how many DTAs it had because the manually kept list was corrupted during the months leading up to the security breach. After the STN campaign began, NSA officials estimated that they had about ^{NSA/CSS:} ~~(b) (1), *~~ personnel with DTA privileges across the enterprise; they also acknowledged the number was unsubstantiated. In January 2014, NSA took a zero-based approach to identify the actual number of authorized DTAs across the enterprise by requiring all users to submit a request for DTA privileges ^{NSA/CSS: (b) (1), *}. NSA officials stated that they received ^{NSA/CSS: (b) (1), *} DTA requests between January 2014 and March 2014. Rather than using that number as a baseline, NSA officials determined that the ^{NSA/CSS: (b) (1), *} DTA requests represented a reduction from their original unsupported estimate and, therefore, they considered the initiative completed.

~~(C//REL TO USA, FVEY)~~ NSA officials determined that the ^{NSA/CSS: (b) (1), *} DTA requests represented a reduction from their original unsupported estimate and, therefore, they considered the initiative completed.

~~(C//REL TO USA, FVEY)~~ The NSA DCIO stated that although the initiative focused on reducing the number of DTA, the actions taken by NSA were not designed to reduce the number of DTAs; rather, they were taken to overhaul the DTA process to identify and vet all DTAs through ^{NSA/CSS: (b) (1), *}. Contrary to the initiative's intent, NSA continued to consistently increase the number of DTAs throughout the next 12 months. Table 3 identifies the starting point after conducting the initial baseline and the steady increase of approved DTAs after the zero-based approach.

(U) Table 3. Number of Approved DTAs Since March 2014

C//REL TO USA, FVEY Date	Number of Approved DTA General* <small>NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)</small>
March 2014	
September 2014	
March 2015	

*(U) Number represents a cumulative total as of a point in time.

* EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(S//REL TO USA, FVEY)~~

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~(U//FOUO)~~ NSA Lacked a Comprehensive Strategy to Effectively Implement PRIVAC-Related STN Initiatives

~~(S//NF)~~ NSA did not effectively implement three PRIVAC-related STN initiatives because it lacked a comprehensive strategy and implementation plan. Specifically, NSA did not develop a detailed, structured methodology to implement and measure the completion of the initiatives before it took action to complete them. NSA identified STN initiatives and activities it considered sufficient to implement each initiative through working groups and other ad hoc processes, but these discussions were not documented. When the initiatives were developed, NSA officials also did not address necessary actions to effectively measure completeness. The NSA DCIO consistently stated that NSA was more concerned with taking an action than assessing specific risks and developing a plan to mitigate them. Although NSA eventually assessed the risks to its operating environment in April 2016, this assessment was completed after the STN initiatives were being implemented. Consequently, NSA officials lacked a framework for implementing TPA and TSA controls and technology-based monitoring for all privileged users, and for reducing the number of privileged users and DTAs needed to support mission requirements.

~~(S//NF)~~ The NSA DCIO consistently stated that NSA was more concerned with taking an action than assessing specific risks and developing a plan to mitigate them.

³⁹ ~~(S//REL TO USA, FVEY)~~ A user can have DTA general and privileged access simultaneously and, therefore, could be double-counted.

~~(S//REL TO USA, FVEY)~~ NSA did not keep accurate and detailed documentation that identified its methodology for completing each initiative and did not describe how it measured the initiatives' completeness and effectiveness. Instead, NSA developed internal reports that had only limited information about the actions taken to complete the initiatives. NSA officials stated that, in some instances, they developed the internal reports after reporting the initiative as complete. NSA's unstructured approach to implement the initiatives resulted in reporting the initiatives as complete when only partial progress had been made or the intent of the initiative had not been fully met. While NSA acted to complete the initiatives, the lack of a comprehensive strategy hindered its ability to determine whether the actions were sufficient to effectively reduce the risk of insider threats.

~~(S//REL TO USA, FVEY)~~ Although NSA has begun to implement its broader Secure-the-Enterprise campaign, it has yet to effectively complete all the STN initiatives. Therefore, the Director, Technology Directorate, NSA/CSS Chief Information Officer, should develop a strategy with milestones and metrics to expand TSA controls and implement automated, technology-based monitoring for all system and network administrators; develop and implement procedures to ensure approvers use consistent processes to grant privileged access or data transfer authority based on mission needs; and, periodically assess and reconcile the number of privileged users and DTAs needed to support NSA mission requirements.

~~(U//FOUO)~~ Insider Threat Risks Remain Despite Implementing PRIVAC-Related STN Initiatives

~~(S//REL TO USA, FVEY)~~ NSA's actions to implement PRIVAC-related STN initiatives did not fully decrease the risk of insider threats or the ability of insiders to exfiltrate data. The STN campaign was established in response to the June 2013 security breach in which an NSA contractor exfiltrated about 1.5 million sensitive and classified documents. NSA designed the STN initiatives to reduce the vulnerabilities exploited during this breach.

~~(S//NF)~~ NSA/CSS (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

NSA did not align its resources and ensure that the actions taken were sufficient to fully implement the intent of the initiatives and reduce the vulnerabilities it identified. NSA also did not have a defined strategy or an

~~(S//NF)~~ NSA is still at risk of personnel with nefarious intentions exploiting vulnerabilities and again compromising highly classified national security information.

implementation plan to monitor completion of the initiatives. As a result, NSA did not complete all the initiatives by June 2015 as required by the Director, NSA, and some initiatives that NSA considered fully completed were only partially completed.

~~(S//NF)~~ NSA is still at risk of personnel with nefarious intentions exploiting vulnerabilities and again compromising highly classified national security information.

NSA is still at risk of personnel with nefarious intentions exploiting vulnerabilities and again compromising highly classified national security information.

(U) Management Comments on the Finding and Our Response

(U) Management Comments on NSA's Approach to Completing STN Initiatives

~~(S//REL TO USA, FVEY)~~ The Director, Technology Directorate, NSA/CSS Chief Information Officer, requested that we consider rewording the following sentence on page 22 of the report: "The NSA DCIO consistently stated that NSA was more concerned with taking an action than assessing specific risks and developing a plan to mitigate them." The Director requested that we revise the sentence using the words "tactical steps," "sense of urgency," or "reactionary," and stated that NSA took a tactical and reactionary approach to implementing the STN initiatives instead of planning and strategizing how to implement the initiatives because of the urgency of limiting the risk of insider threats after the June 2013 security breach.

(U) Finding

~~(C//REL TO USA, FVEY)~~ The Director also stated that NSA officials provided e-mail documentation showing that the Director and Deputy Director, NSA, supported moving forward with only two of the remaining initiatives, ^{NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}

^{NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}
The Director stated that completing the remaining STN initiatives by June 2015 was not feasible.

(U) Our Response

~~(C//REL TO USA, FVEY)~~ We agree that NSA took a tactical and reactionary approach to limit the risk of insider threats when implementing STN initiatives based on the circumstances surrounding the security breach. Although NSA worked in a fluid situation, NSA should have developed a strategy that detailed a structured framework and methodology for implementing STN to ensure its actions were effective and mitigated vulnerabilities exploited during the security breach. Therefore, we did not revise the report.

~~(C//REL TO USA, FVEY)~~ We acknowledge that NSA provided documentation regarding the Director's approval to move forward with two STN initiatives. ^{NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}

(U) Management Comments on Reducing Insider Threat Risks

~~(U//FOUO)~~ The Director, Technology Directorate, NSA/CSS Chief Information Officer, requested that we consider rewording a paragraph in the report section titled "Insider Threat Risks Remain Despite Implementing PRIVAC-Related STN Initiatives." The Director stated that the paragraph was misleading because it implied that insider threat

⁴⁰ (U) ^{NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}

⁴¹ (U) ^{NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}

(U) Finding

(U//~~FOUO~~) risks could be eliminated at a point in time. The Director stated that eliminating all risk of insider threats was not feasible, ^{NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}

(U) Our Response

(S//~~NF~~) We agree that insider threat risks cannot all be eliminated, and that ^{NSA/CSS: (b) (1) EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}

reduced some of the insider threat risks. However, as stated in the report, NSA did not effectively implement or complete three of the seven initiatives included in the audit scope. We believe NSA could have taken additional actions to further mitigate insider threat risks, therefore, we did not revise the report.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Director, Technology Directorate, National Security Agency/Central Security Service Chief Information Officer, in coordination with the Director, Associate Directorate for Security and Counterintelligence:

- a. (S//~~REL TO USA, FVEY~~) ^{NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6); (b) (5)}

(U) NSA Comments

(S//~~REL TO USA, FVEY~~) The Director, Technology Directorate, NSA/CSS Chief Information Officer, agreed, ^{NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)}

~~(S//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]

(U) Our Response

(U//~~FOUO~~) Comments from the Director, Technology Directorate, NSA/CSS Chief Information Officer, addressed all specifics of the recommendation, and no further comments are required. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

b. ~~(S//NF)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6); (b) (5)

[Redacted]

(U) NSA Comments

~~(S//REL TO USA, FVEY)~~ The Director, Technology Directorate, NSA/CSS Chief Information Officer, agreed. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

(U) Our Response

(U) Comments from the Director, Technology Directorate, NSA/CSS Chief Information Officer, addressed the specifics of the recommendation, and no further comments are required.

⁴² ~~(S//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]

(U) Recommendation 2

(U) We recommend that the Director, Technology Directorate, National Security Agency/Central Security Service Chief Information Officer, develop a strategy that includes milestones and metrics to:

- a. ~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[Redacted]

(U) NSA Comments

~~(C//REL TO USA, FVEY)~~ The Director, Technology Directorate, NSA/CSS Chief Information Officer, agreed, NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[Redacted]

(U) Our Response

~~(C//REL TO USA, FVEY)~~ Comments from the Director, Technology Directorate, NSA/CSS Chief Information Officer, partially addressed the recommendation. Although

NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)
[Redacted]

Therefore, we request that the Director reconsider his position and provide additional comments on the final report.

b. ~~(S//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

(U) NSA Comments

~~(S//REL TO USA, FVEY)~~ The Director, Technology Directorate, NSA/CSS Chief Information Officer, agreed. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Our Response

~~(S//REL TO USA, FVEY)~~ Comments from the Director, Technology Directorate, NSA/CSS Chief Information Officer, partially addressed the recommendation. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

Therefore, we request that the Director provide additional comments and documentation on the final report that identify the specific

~~(S//NF)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(S//NF) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

Therefore, we request that the Director reconsider his position and provide additional comments on the final report describing how NSA plans to meet the intent of the recommendation.

(U) Recommendation 3

(U) We recommend that the Director, Technology Directorate, National Security Agency/Central Security Service Chief Information Officer, in coordination with system owners:

- a. **(U//FOUO)** NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

(U) NSA Comments

(U//FOUO) The Director, Technology Directorate, NSA/CSS Chief Information Officer, agreed with the recommendation.

(U) Our Response

(U//FOUO) Although the Director, Technology Directorate NSA/CSS Chief Information Officer, agreed, he did not address all specifics of the recommendation. Therefore, we request that the Director provide additional comments on the final report that identify specific actions NSA will take

- b. **(U//FOUO)** NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

(U) NSA Comments

(U//FOUO) The Director, Technology Directorate, NSA/CSS Chief Information Officer, agreed,

(U) Our Response

(U) Comments from the Director, Technology Directorate, NSA/CSS Chief Information Officer, addressed all specifics of the recommendation, and no further comments are required.

c. (U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[REDACTED]

(U) NSA Comments

(U//~~FOUO~~) The Director, Technology Directorate, NSA/CSS Chief Information Officer, agreed, NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Our Response

(U) Comments from the Director, Technology Directorate, NSA/CSS Chief Information Officer, addressed all specifics of the recommendation, and no further comments are required.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from January 2016 through July 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 objective.

(U//~~FOUO~~) We initiated this audit in response to a congressional request included in the classified annex to the Intelligence Authorization Act for FY 2016, which requires the DoD OIG to assess whether NSA remedied the vulnerabilities exploited by the June 2013 security breach and completed all STN initiatives. We focused on 7 of the 40 STN initiatives that we determined presented a higher risk to NSA's ability to secure network access, protect against insider threats, and provide increased oversight of personnel with PRIVAC.

(~~C//REL TO USA, FVEY~~) We met with officials at NSA headquarters from the Technology Directorate, the Associate Directorate for Security and Counterintelligence Center, and other directorates responsible for developing, monitoring, implementing, and overseeing completion of PRIVAC-related STN initiatives.

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

(U//~~FOUO~~) We nonstatistically selected and visited four NSA installations located in Washington D.C., Texas, Utah, and North Carolina. We conducted walkthroughs of the DCMs [REDACTED]. We met with officials responsible

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

We

(U//FOUO) nonstatistically selected and interviewed NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) privileged users about their

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Table 4. Privileged Users Interviewed

U//FOUO									
NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)									
[Redacted Table Content]									
									U//FOUO

*(U) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//FOUO) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted Content]

(U) Use of Computer-Processed Data

(U//FOUO) We used computer-processed data NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6) to

identify and validate privileged users based on assigned responsibilities. NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted Content]

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

We determined that NSA/CSS: (b) (3), * data were

* 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//~~FOUO~~) sufficiently reliable to determine a user's PRIVAC level. NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[REDACTED]

(U) Use of Technical Assistance

(U) The DoD OIG Quantitative Methods Division assisted in selecting a nonstatistical sample of privileged users we used in selecting users to interview at the sites visited.

(U) Prior Coverage

(U) During the last 5 years, the NSA Inspector General issued one classified report related to NSA's ability to implement STN campaign initiatives.

(U) NSA Inspector General

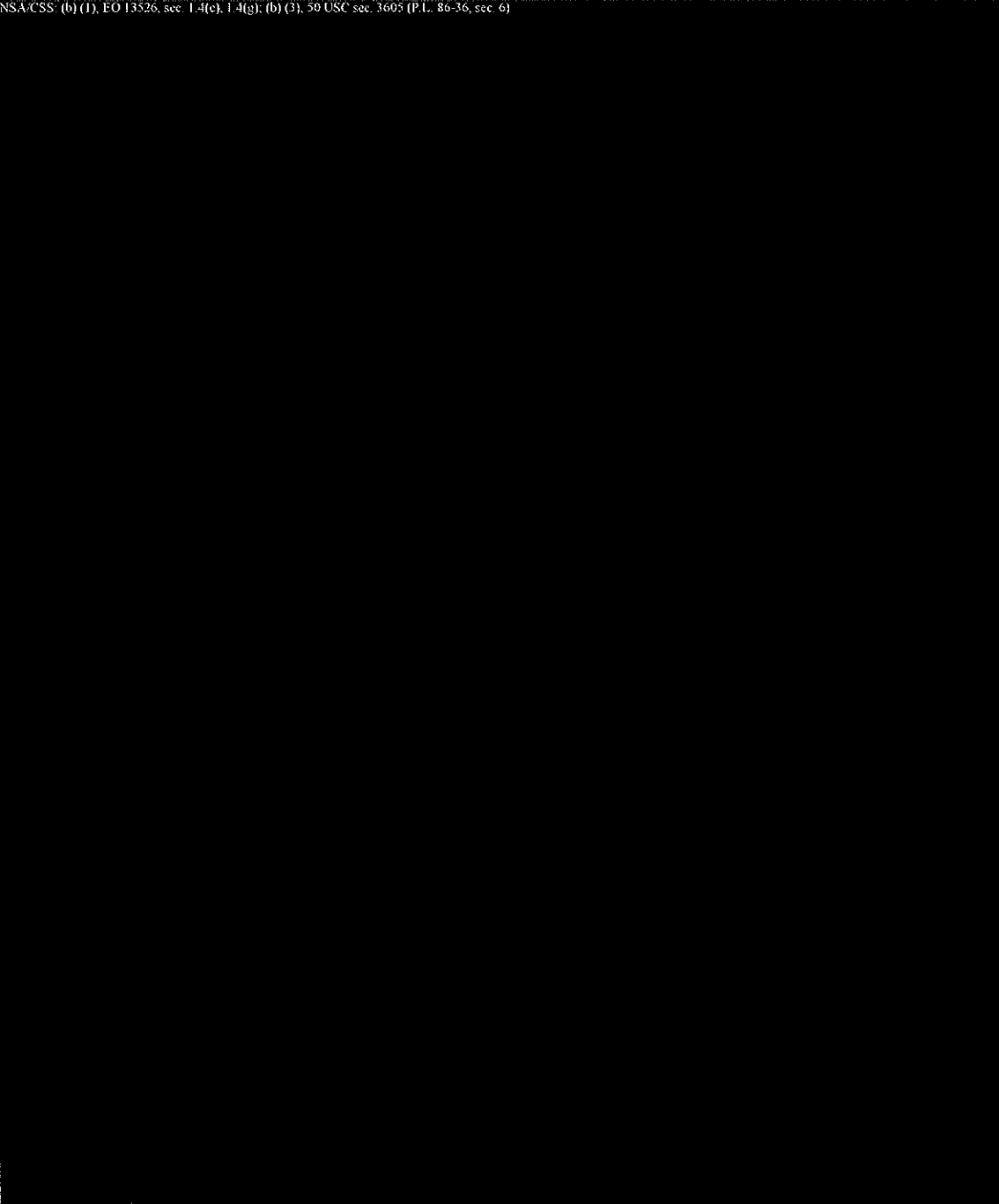
(U) Report No. AU-14-0005, "Audit of NSANet Server Security," June 2015 (Document classified CONFIDENTIAL//REL TO USA, FVEY)

(U) Appendix B

(U) STN Initiatives

(U//~~FOUO~~) NSA completed or is in the process of implementing 40 STN initiatives in response to the June 2013 security breach. NSA categorized the initiatives in three major areas: tighten controls on computer systems, tighten controls on data, and increase oversight of its personnel. The table below describes the STN initiatives.

SECRET//REL TO USA, EVEV STN Initiative	Initiative Description
4. Implement TSA Control for System Administration Policies	

SECRET//REL TO USA, FVEY STN Initiative	Initiative Description
<small>NSA/CSS (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)</small> 	
	SECRET//REL TO USA, FVEY

SECRET//REL TO USA, FVEY	
STN Initiative	Initiative Description
21. Implement TPA Control Over DCMs	NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
22. Develop and Document a New System Administration Model	
NSA/CSS: (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)	
33. Reduce the Number of Authorized DTAs	
	SECRET//REL TO USA, FVEY

SECRET//REL TO USA, FVEY STN Initiative	Initiative Description
34. Assess the Number of SAs Across the Enterprise	NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
35. Reduce the Number of Personnel With PRIVAC	
36. Oversight of Privileged User Activities	
NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)	
	SECRET//REL TO USA, FVEY

(U) Management Comments

(U) National Security Agency



~~SECRET//NOFORN~~
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G MEADE, MARYLAND 20755-6000

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL -
INFORMATION MEMORANDUM

SUBJECT: (U//FOUO) NSA Response to Discussion Draft for DoD IG Project No.
D2016-D000RC-0072.000

(U//FOUO) NSA welcomes the observations and opportunities for improvement offered by the DoD IG to benefit our continuing effort to mitigate insider threat across the enterprise. While the Media Leak events that led to Secure the Net (STN) were both unforeseen and serious, we consider the extensive progress we made in a short time to be a "good news" story. We are very proud of the improvements to our security posture we have been able to achieve, all while sustaining and advancing our vital mission, across our vastly complex network, NSANet. That, coupled with the fact that NSA's mission requirements shift daily as a result of world events, creates an extremely dynamic environment that must balance mission needs with security requirements.

(U//FOUO) All of these Information Technology (IT) components and the knowledgeable people to administer the systems must flex to meet the changing mission needs and interoperate successfully, constantly re-prioritizing decisions to impact IT services that must be delivered 24/7. In addition, policy changes resulting from 9/11 (such as "need to share" versus "need to know" and ODNI's launch of an IC-wide IT environment, IC ITE) have completely changed, in scope and method, how IT must work to support its customers. NSA bears the lion's share of technical work to adapt its IT systems to effect the needed changes to successfully operate - and operate securely - across the IC.

(U//FOUO) We recognize that there are no silver bullets in information or network security - no tactic or plan that can wholly eliminate the potential for harm by myriad threats. By employing a layered defense approach rather than relying on a single initiative to protect our networks, systems, and data, we have been able to significantly reduce the risks inherent in the operation of a global, dynamic enterprise. Further, the combination of initiatives we have implemented and are continuing to develop ensure that the activities of a nefarious actor,

Classified By: DoD OIG: (b)
Derived From: NSA/CSSM 1-82
Dated: 20180930
Declassify On: 20410701

~~SECRET//NOFORN~~

(U) National Security Agency (cont'd)

~~SECRET//REL TO USA, FVEY~~

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

~~(U//FOUO)~~

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

~~(U//FOUO)~~

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

[Redacted]

(U) We appreciate the time, energy, and commitment of the audit team, as they worked to understand the measures and capabilities we have implemented over the last three years. We hope they came to appreciate the depth and breadth of the enterprise we are defending, and the complexities inherent in that defense.

~~SECRET//REL TO USA, FVEY~~

(U) National Security Agency (cont'd)

~~SECRET//REL TO USA, FVEY~~

(U) NSA respectfully offers the following related to the three recommendations.

(U) Response to Recommendations

(U) Recommendation 1

~~(S//REL)~~ We recommend that the Director, Technology Directorate, National Security Agency / Central Security Service Chief Information Technology Officer, in coordination with the Director, Associate Directorate for Security and Counterintelligence:

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

a.

~~(S//REL)~~ NSA Response: NSA concurs with the DoD IG's recommendation.

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

b.

~~(S//REL)~~ NSA Response: NSA concurs with the DoD IG's recommendation. NSA

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~SECRET//REL TO USA, FVEY~~

(U) National Security Agency (cont'd)

~~SECRET//REL TO USA, FVEY~~

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Recommendation 2

~~(S//REL)~~ We recommend that the Director, Technology Directorate, National Security Agency / Central Security Service Chief Information Technology Officer develop a strategy that includes milestones and metrics to:

a. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

~~(S//REL)~~ NSA Response: NSA concurs with the DoD IG's recommendation. The

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

b. NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

~~(S//REL)~~ NSA Response: NSA concurs with the DoD IG's recommendation and believes it has satisfied this recommendation.

NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

~~SECRET//REL TO USA, FVEY~~

(U) National Security Agency (cont'd)

SECRET//REL TO USA, FVEY

(U) Recommendation 3

(U//FOUO) We recommend that the Director, Technology Directorate, National Security Agency/Central Security Service Chief Information Officer, in coordination with system owners:

a. NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[Redacted]

(U//FOUO) NSA Response: NSA concurs with the DoD IG's recommendation.

b. NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[Redacted]

(U//FOUO) NSA Response: NSA concurs with the DoD IG's recommendation and

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

c. NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6), (b) (5)

[Redacted]

(U//FOUO) NSA Response: NSA concurs with the DoD IG's recommendation and

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) Thank you for the opportunity to review and comment on the draft audit report.

NSA/CSS: (b) (6)

[Redacted]

GREGORY L. SMITHBERGER
NSA/CSS Chief Information Officer

Encl:

(U//FOUO) DoD IG Discussion Draft – Project No. D2016-D000RC-0072.000
Comment Matrix

SECRET//REL TO USA, FVEY

(U) National Security Agency (cont'd)

Document Title: DoD IG Draft - Project No. D2016-D000RC-0072.000		Date Date: 5 Aug 2016					
Comment #	Page #	Line #	Paragraph #	POC Info: Organization, Name, Title, Phone, Email	Comment Type: Administrative (A), Critical (C)	Comments (Use classification portion markings)	Response (Use classification portion markings)
1	28	24	1			NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)	Accept
2	28	25	2			NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)	Reflect
3	28	26	3			NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)	Accept
4	28	27	4			NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)	Rational

Classified By: (b) (6)
 Declassify on: 20410001
 Derived From: NSA/CSS
 Date: 2/18/2008
 Declassify on: 20410001

(U) Glossary

(U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) **Data Center and Machine Room.** Facilities that host computing systems, servers, data storage, and machine rooms.

(U) **Data Center Manager.** Personnel with responsibility for overseeing and managing DCM activities and operations.

(U//~~FOUO~~) **Data Transfer Agent (DTA).** Designated personnel approved to use removable media to transfer data to or from an information system.

(U) **Data Transfer Agent (DTA) General.** Personnel who have a primary responsibility to move data within the enterprise using removable media.

(U) **Data Transfer Agent (DTA) Privileged.** Personnel who use removable media to perform PRIVAC functions.

(U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) **Limited Administrator.** Users who perform PRIVAC functions on standalone systems.

(C//REL TO USA, FVEY) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U) **Network Administrators.** Administrative users who maintain computer infrastructure with emphasis on networks.

(U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

(U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6); (b) (3)
[Redacted]
[Redacted]
[Redacted]

(U) **Privileged Access.** A level of access that is significantly greater than that of users performing normal operations.

(U) **Public Key Infrastructure.** An enterprise-wide service supporting digital signatures and other public key-based security mechanisms for DoD functional enterprise programs.

(U//~~FOUO~~) NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
[Redacted]

(U) **Tier 3 System Administrators (SYS3).** NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
[Redacted]

(U) **Tier 2 System Administrators (SYS2).** NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
[Redacted]

(U//~~FOUO~~) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
[Redacted]

(U//~~FOUO~~) NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]
[Redacted]
[Redacted]

(U) **System Administrator (SA).** Administrative users who have privileged access to maintain, configure, and operate computer systems.

(U) **System Security Plans.** Provide an overview of system security requirements for a specific system and describe implemented security controls to meet the requirements.

~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]

~~(U//FOUO)~~ **Two Person Access (TPA)**. Requires two authorized personnel NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]

~~(U//FOUO)~~ **Two Stage Authentication (TSA)**. Requires administrators to use at least two separate sources of authentication NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]

~~(C//REL TO USA, FVEY)~~ NSA/CSS: (b) (1), EO 13526, sec. 1.4(c), 1.4(g), (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)
[Redacted]

(U) Source of Classified Information

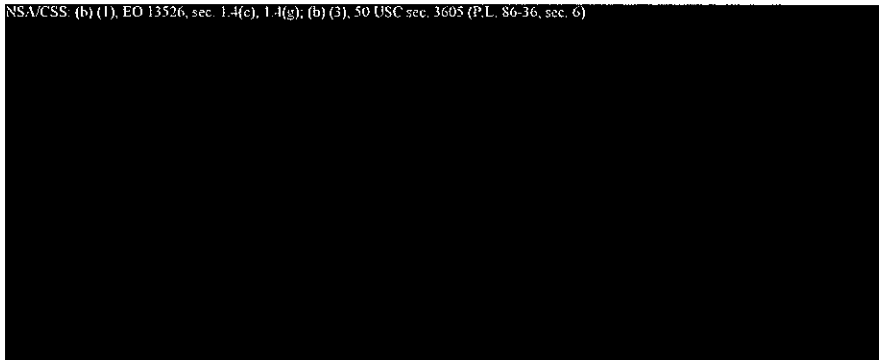
- Source 1:** (U) Permanent Select Committee on Intelligence, "Intelligence Authorization Act for Fiscal Year 2016:" (Document classified SECRET//NOFORN)
Declassification Date: January 1, 2040
Generated Date: October 5, 2015
- Source 2:** (U) NSA-provided Secure-the-Net Activity Update, November 16, 2016: (Document classified SECRET//NOFORN)
Declassification Date: September 1, 2039
Generated Date: November 16, 2015
- Source 3:** (U) NSA Associate Directorate for Security and Counterintelligence, "Snowden Investigative Overview:" (Document classified SECRET//REL TO USA, FVEY)
Declassification Date: March 1, 2041
Generated Date: February 9, 2016
- Source 4:** (U) NSA-provided Securing the Net Update, May 2015: (Document classified CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: May 1, 2040
Generated Date: May 2015
- Source 5:** (U) NSA Commander Intent for "Securing the Enterprise is the Path Forward:" (Document classified CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: September 30, 2038
Generated Date: September 8, 2015
- Source 6:** (U) NSA Town Hall Briefing, "Secure the Enterprise:" (Document classified SECRET//REL TO USA, FVEY)
Declassification Date: November 1, 2040
Generated Date: November 12, 2015
- Source 7:** (U) NSA Secure the Network Detailed Report, January 2016: (Document classified CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: January 28, 2041
Generated Date: January 28, 2016

Source 8: (U) NSA List of Privileged Users: (Document classified
CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: August 1, 2038
Generated Date: January 28, 2016

Source 9: (U) NSA-Texas List of Privileged Users (Document classified
CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: February 1, 2041
Generated Date: February 16, 2016

Source 10: (U) NSA-Washington List of Privileged Users (Document classified
CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: February 1, 2041
Generated Date: February 23, 2016

Source 11: NSA/CSS (b) (1), EO 13526, sec. 1.4(e), 1.4(g); (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)



Source 12:

(U) Acronyms and Abbreviations

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

CSS Central Security Service
DCM Data Center and Machine Room
DCIO Deputy Chief Information Officer
DTA Data Transfer Agent
NSA National Security Agency
NSANet NSA Network
PRIVAC Privileged Access
SA System Administrator
STN Secure-the-Net
TPA Two-Person Access

NSA/CSS: (b) (3), 50 USC sec. 3605 (P.L. 86-36, sec. 6)

TSA Two-Stage Authentication

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

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

Congressional Liaison

congressional@dodig.mil; 703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

Monthly Update

dodigconnect-request@listserve.com

Reports Mailing List

dodig_report@listserve.com

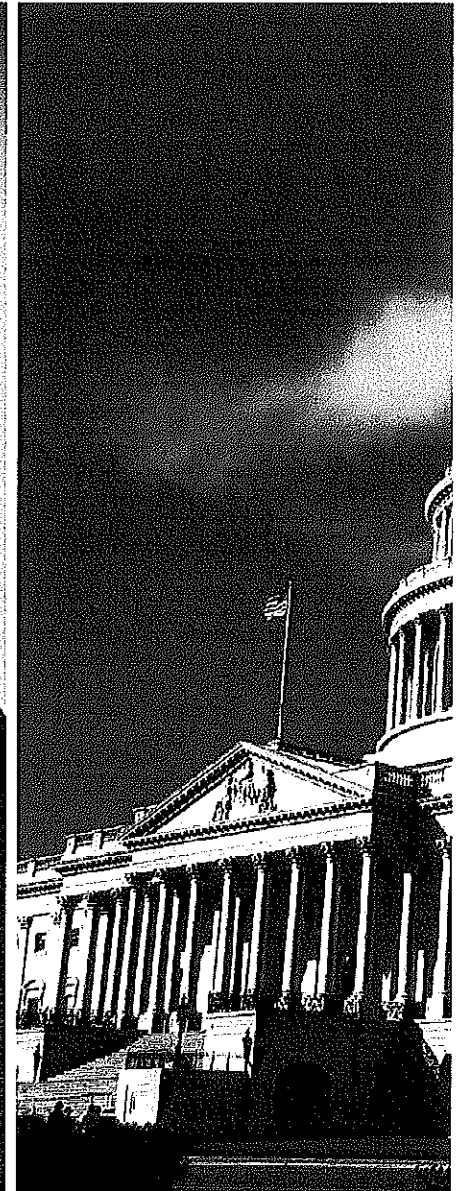
Twitter

twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline

SECRET//NOFORN



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500

www.dodig.mil

Defense Hotline 1.800.424.9098

SECRET//NOFORN