~~TOP SECRET//SI//NOFORN~~

INSPECTOR GENERAL

U.S. Department of Defense

December 19, 2017

Report No. DODIG-2018-043

(U) The National Security Agency Enterprise

Classified By: Carol N. Gorman
Derived from: Multiple Sources
Declassify on: 20421101

Report 28 of 35

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~TOP SECRET//SI//NOFORN~~

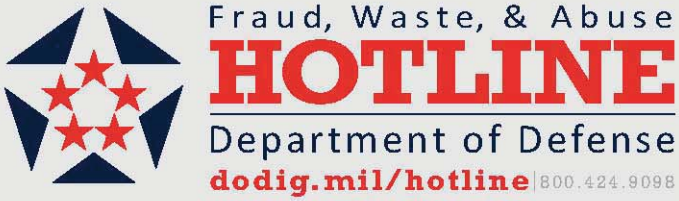
INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

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.



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

(U) Results in Brief

(U) The National Security Agency Enterprise

(U) December 19, 2017

(U) Objective

(U) We determined whether the National Security Agency (NSA) implemented effective security configuration controls and processes to protect its devices, systems, enclaves, and networks from insider and external threats. This report is the second in a series on the implementation of NSA's initiatives to improve security over its systems, networks, and data. We conducted this audit in response to a congressional requirement.

(~~S//NF~~) On August 29, 2016, we issued Report No. DODIG-2016-129, "The National Security Agency Should Take Additional Steps to Effectively Implement Its Privileged Access-Related Secure-the-Net Initiatives." The report identified NSA's progress, limitations, and effectiveness in limiting privileged access [redacted]

(U) Background

(~~S//REL~~) After the June 2013 security breach, NSA began developing and implementing [redacted] Secure-the-Net (STN) initiatives and [redacted] Secure-the-Enterprise (STE) initiatives. The STN initiatives focused on improving controls over NSA's computer systems and data, and increasing oversight of its personnel activities on core NSANet, NSA's Top Secret information technology infrastructure. The STE initiatives focused on designing, managing, and defending all NSA/Central Security Service (CSS) systems, networks, communications, data, and critical infrastructure around the world as an integrated enterprise. For this audit, we nonstatistically selected four STE and four STN initiatives that we determined presented the highest risk to the NSA's ability to secure network and enclave devices against insider and external threats.

(U) Finding

(~~S//NF~~) [redacted]

(~~C//NF~~) [redacted]

- (~~C//NF~~) develop comprehensive strategies and plans to implement the STN and STE initiatives that prioritize resources and initiatives based on risk to the mission,
- (~~C//NF~~) procure tools with the capability to [redacted], or
- (~~C//NF~~) identify the physical location of [redacted]

(~~TS//NF~~) [redacted]

(U) Results in Brief

(U) The National Security Agency Enterprise

(U) Recommendations

(~~U//FOUO~~) We recommend that the Director, NSA/Chief, CSS validate whether NSA's actions to implement STN and STE initiatives that it reported as complete are sufficient to fully meet the goals of the initiatives. In addition, the Director should assess whether the strategy and allocation of resources will enable the NSA to meet its stated goals.

(~~U//FOUO~~) We recommend that the Chief Information Officer, NSA/CSS implement a comprehensive plan with metrics that clearly outline the methodology to complete ongoing initiatives and apply a similar methodology to implement future campaign initiatives.

(~~U//FOUO~~) We recommend that the Director, Capabilities Directorate, NSA/CSS Chief Information Officer:

- (~~U//FOUO~~) verify NSA (b)(3) PL 86-36 Section 6 on all devices and authenticate all devices connected to the NSA enterprise;
- (~~U//FOUO~~) assess the volume of data across the NSA enterprise, implement tools with the capacity to register and baseline all NSA subnets, NSA (b)(3) PL 86-36 Section 6
- (~~U//FOUO~~) implement an automated solution to identify all devices connected to the NSA enterprise and verify compliance with its global security policies; and
- (~~U//FOUO~~) develop and implement procedures to verify that all devices connected to the NSA enterprise are properly configured NSA (b)(3) PL 86-36 Section 6

(~~U//FOUO~~) In addition, we recommend that the Director, Capabilities Directorate, NSA/CSS Chief Information Officer as well as the Chief of Security and Counterintelligence:

(U) Recommendations (cont'd)

- (~~U//FOUO~~) identify and validate the number and location of all enclaves connected to the NSA enterprise; NSA (b)(3) PL 86-36 Section 6
- (~~U//FOUO~~) conduct a risk assessment to identify NSA's most sensitive enclaves and data transfer agent locations, identify annual funding needed to conduct the Random Entrance Inspection Program at all locations, and until the funding is provided conduct continuous enhanced random inspections at the locations with the highest risk to the enterprise;
- (~~U//FOUO~~) identify all desktop computers connected to the NSANet, conduct a risk assessment to determine how to monitor devices where user activity monitoring is not being conducted, and conduct periodic testing to ensure that an automated monitoring tool is deployed and actively reporting user activity; and
- (~~TS//SI//NF~~) take immediate action to secure the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 enclave to include identifying all connected devices, monitoring user activity, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Management Comments and Our Response

(~~U//FOUO~~) The Director, NSA/Chief, CSS, agreed with our finding and recommendations. The Director stated that the NSA will adopt the recommendations to further enhance its security posture. The Director stated that the NSA planned to implement all recommendations by third quarter FY 2018.

(U) Results in Brief

(U) The National Security Agency Enterprise

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

(~~U//FOUO~~) With regard to our report recommendations, the Director addressed actions to implement and NSA (b)(3) PL 86-36 Section 6 connected to the NSA enterprise, NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 , the recommendation is unresolved. We request that the NSA provide documentation showing it implemented NSA (b)(3) PL 86-36 Section 6 on all devices connected to the NSA enterprise and implemented procedures and technical solutions to authenticate all devices connected to its enterprise.

(~~S//REL TO USA, FVEY~~) The Director stated that the NSA planned to use data analytics to monitor network activity NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 the recommendation is unresolved. We request that the NSA provide documentation showing it baselined all user activity, implemented tools that NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) The Director stated that the NSA modified its approach to detect all devices on the network and verify whether the devices complied with enterprise security policies. However, it is unclear how the modified approach would ensure that each device on the network complied with enterprise security policies. Therefore, the recommendation is unresolved. We request that the NSA provide documentation showing it identified all devices connected to the enterprise and enforced global security policies.

(~~U//FOUO~~) The Director stated that the NSA was updating STE Verification Checklists and validation procedures to address the gaps identified in the DoD OIG report. In addition, the Director stated that the NSA would use a combination of tools to verify that NSA (b)(3) PL 86-36 Section 6

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

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 Therefore, the recommendation is resolved. We will close the recommendation once we verify that the NSA updated the STE Verification Checklist and implemented procedures to verify that NSA (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) The Director stated that the NSA planned to identify and validate the number and location of all enclaves connected to the NSA enterprise. In addition, the Director stated that the NSA plans to update procedures to monitor enclaves and NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Therefore, the recommendation is resolved. We will close the recommendation once the NSA provides documentation that verifies the NSA identified all enclaves, including their physical location; NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 implemented procedures to monitor all enclaves; and updated procedures for monitoring enclaves and the plan to NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) In response to our recommendation to identify annual funding needed to conduct enhanced random entrance inspections at all locations, the Director stated that the NSA planned to increase physical security and other types of inspections. However, the NSA only identified annual funding to conduct the random entrance/exit inspection program NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Therefore, the recommendation is unresolved. We request that the NSA provide documentation showing it identified the funding needed and implemented a plan to conduct and sustain enhanced random entrance/exit inspections at all locations.

(~~S//REL TO USA, FVEY~~) The Director stated that the NSA plans to implement a multi-faceted approach to

(U) Results in Brief

(U) The National Security Agency Enterprise

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

(~~S//REL TO USA, FVEY~~) identify all devices connected to the network. In addition, the Director stated that the NSA identified instances where user activity monitoring did not occur and was developing new solutions to ensure all user activity data were collected. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Therefore, the recommendation is unresolved. We request that the NSA provide documentation showing it implemented tools that accurately identify all network-connected devices and a user activity monitoring solution for all operating systems and devices.

(~~TS//REL TO USA, FVEY~~) The Director stated that the NSA established a team in October 2016 to assess risk and begin implementing mitigating security measures for NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 mission areas. However, the NSA had not effectively implemented any of the STN and STE initiatives we reviewed to harden security for the NSA (b)(1) EO 13526 Section 1.4g and (enclave. Therefore, the recommendation is unresolved. We request that the NSA provide documentation showing it identified all connected devices, established a solution to monitor user activity, and validated that NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) The Director stated that the NSA would randomly spot check the sufficiency of ongoing verification measures once the STN and STE initiatives were completely implemented. In addition, the Director stated that the NSA established a team to identify, track, and reprioritize resources to implement the initiatives. The Director also stated that the NSA developed checklists and playbooks that described technical solutions and monitoring approaches to implement the initiatives on its networks and enclaves. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

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

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Therefore, the recommendation is unresolved. We request that the NSA provide documentation that shows it identified specific resources required to implement each STN and STE initiative and validated the completion of each STN and STE initiative. The Director stated that the NSA documented actions, with specific completion timeframes, in a briefing chart and developed detailed checklists and implementation playbooks. However, none of those documents provided the NSA with the ability to fully measure the completeness of each initiative, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 . Therefore, the recommendation is unresolved. We request that the NSA provide a comprehensive plan that clearly outlines the methodology and provides quantifiable means to track the progress of all the initiatives.

(U) Please see the Recommendations Table on the next page.

(U) Recommendations Table

~~U//FOUO~~ Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, National Security Agency/Chief, Central Security Service	4	None	None
Chief Information Officer, National Security Agency/Central Security Service	1.a, 1.b, 3.b, 3.c, 3.d, 5	3.a	None
Director, Capabilities Directorate, National Security Agency/Central Security Service	1.a, 1.b, 2.a, 3.b, 3.c, 3.d	2.b, 3.a	None
Chief, Security and Counterintelligence	3.b, 3.c, 3.d	3.a	None ~~U//FOUO~~

(U) Please provide Management Comments by January 19, 2018.

(U) The following categories are used to describe agency management's comments to individual recommendations:

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

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

December 19, 2017

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

(U) SUBJECT: The National Security Agency Enterprise (Report No. DODIG-2018-043)

(~~TS//SI//NF~~) We are providing this report for review and comment. We conducted this audit in response to a congressional requirement. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted] network and security configuration-related Secure-the-Enterprise initiatives. Additionally, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted] We conducted this audit in accordance with generally accepted government auditing standards.

(~~U//FOUO~~) We considered management comments on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Director, National Security Agency/Chief, Central Security Service NSA (b)(3) PL 86-36 [redacted] Therefore, we request the Director, National Security Agency/Chief, Central Security Service provide additional comments on the recommendations by January 19, 2018.

(U) Please send a PDF file containing your comments to DoD OIG (b)(6) and DoD OIG (b)(6). Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at DoD OIG (b)(6) (DSN DoD OIG (b)(6)).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) Contents

(U) Introduction

(U) Objective

(U) We determined whether the National Security Agency (NSA) implemented effective security configuration controls and processes to protect its devices, systems, enclaves, and networks from insider and external threats.[1] This report is the second in a series on the implementation of NSA's initiatives to improve security over its systems, networks, and data.

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 On August 29, 2016, we issued Report No. DODIG-2016-129, "The National Security Agency Should Take Additional Steps to Effectively Implement Its Privileged Access-Related Secure-the-Net Initiatives." The report identified NSA's progress and effectiveness in limiting privileged access NSA (b)(1) EO . See Appendix A for the scope and methodology of this report.

(U) Background

(~~TS//SI//NF~~) The NSA/Central Security Service (CSS) leads U.S. Government cryptology operations focused on signals intelligence and information assurance products and services, and enables Computer Network Operations to gain a decision making advantage for the U.S. and its allies. The NSA/CSS Global Cryptologic Enterprise consists of NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 The NSA Top Secret (TS) information technology infrastructure, also known as "NSANet," enables signals intelligence, information assurance, and supports cyberspace operations across the NSA global cryptologic enterprise.

(~~U//FOUO~~) For this audit, we visited three regions—NSA, Washington (NSAW) in Washington DC; NSA, Hawaii (NSAH) in Hawaii; and (b)(3) PL 86-36 Section 6 —where equipment was connected to NSANet. Specifically, we visited (b)(3) PL NSAW sites, (b)(3) PL 86-36 NSAH sites, and (b)(3) PL 86-36 Section sites in the three regions.

[1] (~~U//FOUO~~) NSA defines an enclave as a collection of computing, noncomputing, or network devices that do not have external connectivity, are protected from other networks by a security device such as a boundary or a firewall, or are standalone. NSA (b)(3) PL 86-36 Section 6

[2] (~~U//FOUO~~) Global Cryptologic Enterprise includes worldwide NSA/CSS personnel, systems, and facilities.

(U) NSA Defensive Measures

(~~C//REL TO USA, FVEY~~) The unauthorized disclosures of classified data in June 2013 by Edward Snowden, a NSA contractor in Hawaii, prompted the NSA to begin implementing a Secure-the-Net (STN) campaign to improve controls over NSA's computer systems and data, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [3,4] As of August 2017, the NSA reported it had completed NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 STN initiatives. See Appendix C for the list of STN initiatives, their description, and NSA's reported status of each initiative.

(~~TS//NF~~) Further, while implementing the STN initiatives, the NSA learned SA (b)(1) EO 526 Section 4g and (b)(3) PL 86-36 Section 6 In September 2015, the NSA began implementing a second campaign, Secure-the-Enterprise (STE), to design, manage, and defend all NSA/CSS systems, networks, communications, data, and critical infrastructure around the world as an integrated enterprise. As of August 2017, the NSA reported it had completed NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 STE initiatives and planned to complete the remaining NSA (b)(1) EO initiatives by NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6. See Appendix B for the list of STE initiatives, their description, and NSA's reported status of each initiative. In October 2016, the NSA began implementing a third campaign, NSA (b)(3) PL 86-36 Section 6, to address special circumstances (such as operational, development, and test environments) within the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 mission to protect operational, development, and test environments.[6] In May 2017, since implementing these initiatives, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~U//FOUO~~) For this audit, we examined the progress of four STE and four STN initiatives that we determined presented the highest risk to the NSA's ability to secure network and enclave devices against insider and external threats. The eight initiatives were:

- (~~U//FOUO~~) enhance physical security at enclave NSA (b)(3) PL 86-36 Section 6 locations (STE initiative 21);
- (~~C//REL TO USA, FVEY~~) b)(3) PL 86-36 Section 6 (STE initiative 3);

[3] (~~U//FOUO~~) NSA investigations determined that Edward Snowden exfiltrated NSA (b)(3) PL 86-36 Section 6

[4] (~~U//FOUO~~) NSA defines core NSANet as the NSANet enterprise, excluding its enclaves.

[5] (~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 is one of the premier tools development, testing, and integration networks at NSA.

[6] (~~U//FOUO~~) We did not include NSA (b)(3) PL 86-36 Section 6 initiatives in the audit scope.

- (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 (STE initiative 4);
- (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 (STE initiative 7);
- (~~U//FOUO~~) baseline network utilization of all NSA (b)(3) PL 86-36 Section 6 (STN initiative 5);[7]
- (~~U//FOUO~~) deploy NSA (b)(3) PL 86-36 Section 6 on all desktops (STN initiative 27);
- (~~U//FOUO~~) connect all devices to NSA (b)(3) PL 86-36 Section 6 to enforce global security policies for core NSANet (STN initiative 3);[8] and
- (~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 (STN initiative 15).[9]

(U) NSA Responsibilities for Implementing STE and STN Initiatives

(~~U//FOUO~~) The Capabilities Directorate has the primary responsibility for implementing STE and STN initiatives. The Chief of Capabilities also serves as the NSA CIO. The NSA CIO reports to the Director, NSA/CSS, and is responsible for governing, managing, and providing the NSA's information technology mission and business systems. According to the Capabilities Directorate mission and functions statement, the NSA CIO is responsible for ensuring that NSA/CSS missions can be accomplished with secure, cost efficient, and responsive information technology, while complying with national, DoD, and intelligence community policies by establishing plans, strategies, policies, and standards.

(~~U//FOUO~~) Although the NSA CIO has the primary responsibility for STE and STN initiatives, other directorates provide support. For example, within the Workforce and Support Activities Directorate, the NSA/CSS Security and Counterintelligence Group (S&CI) is responsible for NSA (b)(3) PL 86-36 Section 6

[7] (U) Subnets are the logical grouping of connected network devices on an internet protocol, which is the standard protocol for communicating across networks.
[8] (U) NSA (b)(3) PL 86-36 Section 6 is a Microsoft solution used to manage, store, and enforce user computer security policies.
[9] (U) NSA (b)(3) PL 86-36 Section 6

(U) Review of Internal Controls

~~(C//NF)~~ 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.[10]

NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

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

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

(U) Finding

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Efforts to Implement STE and STN Initiatives

(~~C//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

- (~~C//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
- (~~C//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
- (~~C//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6.

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(U//FOUO)~~ NSA NSA (b)(3) PL 86-36 Section 6 Must Take Additional Actions to Meet the Goals of Four STE Initiatives

~~(C//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~*(C//NF)*~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(C//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(C//NF)~~ To assess NSA's actions for completing the initiatives, we met with NSA officials responsible for implementing the initiatives and NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~*(C//NF)*~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(C//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(TS//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[11] ~~(U//FOUO)~~ The Defensive Measures Enterprise Functional Team, led by the Capabilities Directorate, was established to develop an enterprise-wide campaign to NSA (b)(3) PL 86-36 Section 6 .

(C//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

- (U//FOUO) NSA (b)(3) PL 86-36 Section 6
- (U//FOUO) NSA (b)(3) PL 86-36 Section 6
- (U//FOUO) NSA (b)(3) PL 86-36 Section 6
- (U//FOUO) NSA (b)(3) PL 86-36 Section 6

(S//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[12] (U//FOUO) NSA (b)(3) PL 86-36 Section 6

[1] (U//FOUO) NSA (b)(3) PL 86-36 Section 6

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Table 1. NSA (b)(3) PL 86-36 Section 6

~~S//REL TO USA,FVEY~~			
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6			
			~~S//REL TO USA,FVEY~~

(U) Source: The DoD OIG.

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[14] (~~U//FOUO~~ NSA (b)(3) PL 86-36 Section 6

~~(TS//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(TS//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(C//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

- ~~(U//FOUO)~~ **Phase 1.** NSA (b)(3) PL 86-36 Section 6
- ~~(U//FOUO)~~ **Phase 2.** NSA (b)(3) PL 86-36 Section 6

- (~~U//FOUO~~) **Phase 3**. NSA (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[15] (U NSA (b)(3) PL 86-36 Section 6

[1] (~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 .

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

- (~~U//FOUO~~) enhance the Random Entrance Inspection Program (REIP) NSA (b)(3) PL
- (~~U//FOUO~~) respond to security events NSA (b)(3) PL 86-36 Section 6 , and
- (~~U//FOUO~~) support NSA (b)(3) PL 86-36 Section 6 as an ongoing initiative.

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) In March 2014, the NSA expanded its inspection program to include the REIP because of the shooting at the Washington Navy Yard in 2013. The REIP involves S&CI officials conducting random inspections and metal detection screenings of TS/SCI cleared affiliates and visitors entering or leaving NSA/CSS facilities. Specifically, the goal is to prevent prohibited items that present a physical threat to personnel from entering NSA facilities and detect restricted items detrimental to NSA's mission that compromise its information technology infrastructure NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [17] To assess NSA's actions taken to complete the initiative, we met with NSA officials responsible for implementing the initiative. We reviewed standard operating procedures for conducting physical inspections and analyzed the results and trends of REIPs performed from June 2014 through May 2017.

[17] (~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6

(U) NSA Performed Fewer REIPs After Implementing the STE Initiative

~~(C//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Table 2. NSAW REIP Results From June 2014 Through May 2017

~~C//REL TO USA, FVEY~~				
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6				
				~~C//REL TO USA, FVEY~~

(U) Source: NSA REIP Monthly Reports.

~~(C//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(U//FOUO)~~ NSA NSA (b)(3) PL 86-36 Section 6 *REIPs*

~~(C//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[18] ~~(U//FOUO)~~ NSA (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[19] (U) The four NSA cryptologic centers are located in Texas, Georgia, Hawaii, and Colorado.
[20] (U) According to S&CI officials, a portal is an ingress or egress point in a facility where REIPs occur.
[21] (~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6

[2] (~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 .

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~U//FOUO~~) NSA NSA (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[23] (U) NSA (b)(3) PL 86-36 Section 6.

[24] (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[25] (~~TS//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[2] (~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[2] (~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(TS//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~***(U//FOUO)***~~ NSA (b)(3) PL 86-36 Section 6

~~(C//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[28] ~~(C//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[2] (U) National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Systems and Organizations," April 2013.

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[30] (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 .

[31] (U) NSA (b)(3) PL 86-36 Section 6 .

(U) Table 3. NSA (b)(3) PL 86-36 Section 6

~~S//NF~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6				
				~~S//NF~~

[1](U) NSA (b)(3) PL 86-36 Section 6

[2] ~~(S//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Source: The DoD OIG.

~~(TS//NF)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U//FOUO) NSA (b)(3) PL 86-36 Section 6

(C//REL TO USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U//FOUO) To assess NSA's actions taken to complete the initiative, we met with NSA officials responsible for implementing the initiative. We also:

- (U//FOUO) identified the tools used to detect devices NSA (b)(3) PL 86-36 Section 6;
- (U//FOUO) observed officials from the Capabilities Directorate using NSA (b)(3) PL 86-36 Section 6 to identify devices NSA (b)(3) PL 86-36 Section 6;
- (U//FOUO) developed a nonstatistical sample NSA (b)(3) PL 86-36 Section 6
- (U//FOUO) collected configuration data such as IP addresses, MAC address, and hostname for the sampled devices, and compared the configuration data to NSA (b)(3) PL 86-36 Section 6 screen prints of the same devices.

(S//REL TO USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[32] (S//SI//REL TO USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(U) Table 4. NSA (b)(3) PL 86-36 Section 6

~~S//NF~~				
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]				
				~~S//NF~~

(U) Source: The DoD OIG.

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

~~(U//FOUO)~~ NSA (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[33] (U) Committee on National Security Systems Directive No. 504, "Directive on Protecting National Security Systems from Insider Threat," February 4, 2014.

(S//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(TS//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(C//REL TO USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA's Actions to Secure its Enterprise

(TS//NF) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

[34] (U//FOUO) NSA (b)(3) PL 86-36 Section 6

[3] (U) NSA (b)(3) PL 86-36 Section 6

(~~TS//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//SI//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//SI//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//SI//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//SI//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~TS//SI//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(U) Management Comments on the Finding and Our Response

(U) NSA Comments

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 . The Director stated that he, NSA leadership, and the Board of Directors were fully engaged and committed to completely, comprehensively, and quickly achieving the defensive measure goals; and therefore have reprioritized significant resources in support of those goals.

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 As a result, the Director stated that he directed a major reorganization in August 2016, NSA 21, which consolidated the responsibilities to develop, deploy, manage, secure, and defend the entire NSA enterprise into the Capabilities Directorate, led by the CIO, dual hatted as the Chief Technology Officer.

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

- (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
- (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 ;
- (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
- (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
- (~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~U//FOUO~~) Finally, the Director requested that we conduct a follow-up to this audit after third quarter FY 2018 to assess whether the NSA implemented the initiatives and achieved its desired outcome.

(U) Our Response

(~~TS//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(~~U//FOUO~~) We recommend that the Director, Capabilities Directorate, National Security Agency/Central Security Service Chief Information Officer:

a. (~~U//FOUO~~) Verify NSA (b)(3) PL 86-36 Section 6 **on all devices and authenticate all devices connected to the NSA enterprise.**

(U) NSA Comments

(~~S//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendation, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Our Response

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 the recommendation is unresolved. NSA (b)(3) PL 86-36 Section 6 Therefore, we request that the NSA provide documentation showing it NSA (b)(3) PL 86-36 Section 6 implemented procedures and technical solutions to authenticate all devices connected to its enterprise.

b. (~~U//FOUO~~) Assess the volume of data across the National Security Agency enterprise, implement tools with the capacity to register and baseline all National Security Agency subnets NSA (b)(3) PL 86-36 Section 6 **.**

(U) NSA Comments

(~~S//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendation, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Our Response

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Recommendation 2

(U) We recommend that the Director, Capabilities Directorate, National Security Agency/Central Security Service:

a. **(~~U//FOUO~~) Implement an automated solution to identify all devices connected to the National Security Agency enterprise and verify compliance with its global security policies.**

(U) NSA Comments

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(U) Our Response

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 [redacted] the recommendation is unresolved. NSA (b)(3) PL 86-36 Section 6 [redacted] Therefore, we request that the NSA provide documentation showing it identified all devices connected to the enterprise and enforced global security policies.

b. (~~U//FOUO~~) Develop and implement procedures to verify that all devices connected to the National Security Agency enterprise are properly configured NSA (b)(3) PL 86-36 Section 6 **.**

(U) NSA Comments

(~~C//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendation, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(U) Our Response

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 [redacted] the recommendation is resolved. We will close the recommendation once we verify that the NSA updated the STE Verification Checklist and implemented procedures NSA (b)(3) PL 86-36 Section 6 [redacted]

(U) Recommendation 3

(~~U//FOUO~~) We recommend that the Director, Capabilities Directorate, National Security Agency/Central Security Service Chief Information Officer and the Chief, Security and Counterintelligence:

a. **(~~U//FOUO~~) Identify and validate the number and location of all enclaves connected to the National Security Agency enterprise;** NSA (b)(3) PL 86-36 Section 6 [redacted]

(U) NSA Comments

(~~S//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendation, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~U//FOUO~~) In addition, the Director acknowledged NSA's challenges with using NSA (b)(3) PL 86-36 Section 6. The Director stated that the NSA has replaced and added new data sources to NSA (b)(3) PL 86-36 Section 6 to close the gap on missing or inaccurate data and was evaluating other sources to fully understand its network. The Director stated that the NSA plans to update NSA (b)(3) PL 86-36 Section 6 to add enclave-level alerting and develop a process to alert physically isolated enclave owners when new devices were connected to the enclave. The Director stated that the NSA plans to update procedures to monitor enclaves NSA (b)(3) PL 86-36 Section 6 by third quarter FY 2018.

(U) Our Response

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6, the recommendation is resolved. We will close the recommendation once the NSA provides documentation that verifies the NSA identified all enclaves, including their physical location; validated the accuracy of NSA (b)(3) PL 86-36 Section 6 data; implemented procedures to monitor all enclaves; and updated procedures for monitoring enclaves and NSA (b)(3) PL 86-36 Section 6

b. (~~U//FOUO~~) Conduct a risk assessment to identify the National Security Agency's most sensitive enclaves and data transfer agent locations, identify annual funding needed to conduct enhanced random entrance inspection at all locations, and, until the funding is provided, conduct

(~~U//FOUO~~) continuous enhanced random inspections at the locations with the highest risk to the enterprise.

(U) NSA Comments

(~~S//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendations, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(U) Our Response

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 the recommendation is unresolved. [redacted] Therefore, we request that the NSA provide documentation showing it identified the funding and implemented a plan to conduct and sustain enhanced random entry/exit inspections at all locations.

c. ~~(U//FOUO)~~ Identify all desktop computers connected to the National Security Agency network, conduct a risk assessment to determine how to monitor devices where user activity monitoring is not being conducted, and conduct periodic testing to ensure that an automated monitoring tool is deployed and actively reporting user activity.

(U) NSA Comments

(~~S//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendation, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

~~(S//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(U) Our Response

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6 [redacted], the recommendation is unresolved. As noted in our response to the Director's comments to Recommendation 2.A, NSA (b)(3) PL 86-36 Section 6 [redacted]. While the NSA took actions to identify noncompliant devices, those actions were limited to in-scope devices rather than all devices within the NSA enterprise. Therefore, we request that the NSA provide policies it uses to determine whether a device is in scope and requires monitoring and documentation showing it verified user activity monitoring solutions are in place across the entire enterprise.

(~~U//FOUO~~) We acknowledge the NSA developed alternate solutions to conduct user activity monitoring on devices that did not support existing user activity monitoring solutions. We also acknowledge that the NSA was testing alternative solutions; however, those solutions were not implemented across the enterprise. Although the NSA took steps to conduct periodic testing through the implementation of an analytic capability, the tool is reliant on the NSA's ability to accurately identify all devices connected to its network. Therefore, we request that the NSA provide documentation showing it implemented tools that accurately identify all network-connected devices and a user activity monitoring solution for all operating systems and devices.

d. (~~TS//NF~~) Take immediate action to secure the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 **enclave to include identifying all connected devices, monitoring user activity** NSA (b)(1) EO 13526 Section 1.4g [redacted]**.**

(U) NSA Comments

(~~TS//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendation, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

~~(TS//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Our Response

~~(TS//REL TO USA, FVEY)~~ NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 , the recommendation is unresolved. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 . Therefore, we request that the NSA provide additional comments on the final report to clarify how and when the NSA will fully implement all STN, STE, and enhanced security measures. In addition, we request that the NSA provide documentation NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Recommendation 4

~~(U//FOUO~~) We recommend that the Director, National Security Agency/Chief, Central Security Service validate whether the National Security Agency's actions to implement Secure-the-Net and Secure-the-Enterprise initiatives that it reported as complete are sufficient to fully meet the goals of the initiatives, and assess whether the strategy and allocation of resources to effectively complete

(~~U//FOUO~~) the initiatives for ongoing campaigns will enable the National Security Agency to meet its stated goals.

(U) NSA Comments

(~~S//REL TO USA, FVEY~~) The Director, NSA/Chief, CSS, agreed with the recommendation, stating that he and the NSA Board of Directors were directly involved in implementing the STN, STE, and enhanced defensive measures campaigns since November 2016 and have identified the expected costs associated with achieving and maintaining the desired end state. For example, the Director stated that the NSA NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~S//REL TO USA, FVEY~~) In addition, the Director stated that the NSA developed checklists and playbooks that described approved technical solutions and monitoring approaches, for STN and STE technical measures implemented on its networks and enclaves. The Director also stated that the Capabilities Director, NSA/CSS, CIO, assigned a group to ensure enclaves, including core NSANet, complied with all STN and STE initiatives. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted] The Director stated the NSA planned to implement all STN and STE initiatives across all NSA networks and enclaves by third quarter FY 2018.

(U) Our Response

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted], the recommendation is unresolved. While the NSA established teams to review whether enclaves were compliant with the STN and STE initiatives, the teams were not established until 2017, more than 3 years after the NSA implemented its first STN initiative. In addition, their efforts focused on enclaves and not on the entire NSA enterprise. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted] For example, one of the STN initiatives required the NSA to generate alerts when normal subnet activity exceeded a threshold. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//REL TO USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

Therefore, we request that the NSA provide documentation showing it identified specific resources required to implement each STN and STE initiative and validated the completion of each STN and STE initiative.

(U) Recommendation 5

(U//FOUO) We recommend that the Chief Information Officer, National Security Agency/Central Security Service develop and implement a comprehensive plan with metrics that clearly outline the methodology to complete the Secure-the-Enterprise initiatives and apply a similar methodology to implement the NSA (b)(3) PL 86-36 Section 6 initiatives.

(U) NSA Comments

(S//REL TO USA, FVEY) The Director, NSA/Chief, CSS, agreed with the recommendations, stating that the NSA CIO was executing a comprehensive plan, with metrics, to complete the STN and STE initiatives while simultaneously executing a separate plan to complete NSA (b)(3) PL 86-36 Section 6 initiatives. The Director stated that the NSA completed a formal risk assessment that considered NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Specifically, the Director stated that the NSA documented actions, with specific completion timeframes, in a briefing chart and developed detailed checklists and implementation playbooks. The Director also stated that the NSA CIO maintained a dashboard that tracked NSA's progress in near real-time in implementing the STE initiatives and noted that NSA leadership received regular briefings to ensure continued progress was made in meeting one of the NSA Director's top priorities.

(S//REL TO USA, FVEY) The Director also stated that the NSA established a team in October 2016 to oversee the implementation of a risk mitigation strategy for the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 enclave. The Director stated that the team used a layered security approach and built upon the STE initiatives to develop a methodology to harden security for the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 enclave. The Director stated that defensive measures for securing the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 enclave were documented in a briefing chart, on a checklist, and in playbook. The Director further stated that NSA's progress in securing

(~~S//REL TO USA, FVEY~~) the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 enclave was tracked by the NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 scorecard, which was briefed regularly to NSA leadership. The Director stated that the NSA plans to complete these actions by third quarter FY 2018.

(U) Our Response

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 , the recommendation is unresolved. We disagree that the placemat, checklists, and playbooks provide a comprehensive plan, with metrics, for completing the STN and STE initiatives. Those documents did not provide the NSA with the ability to fully measure the completeness of each initiative. In addition, the checklist and playbooks did not address all STN and STE initiatives; NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 For example, the briefing chart, checklist, and playbooks did not describe specific actions to NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Moreover, the placemat, checklists, and playbooks did not outline the outcomes needed to consider an initiative complete. Although those documents provide specific actions to implement some of the initiatives, they did not constitute a comprehensive plan that outlines the overarching methodology to complete the initiatives. Furthermore, the dashboard did not track NSA's progress in completing all initiatives; it only tracked the implementation status NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Therefore, we request that the NSA provide a comprehensive plan with detailed steps to implement and specific quantifiable means to track the progress of all the initiatives.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from November 2016 through November 2017 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.

(~~S//NF~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~C//REL TO USA, FVEY~~) We met with officials at NSA headquarters from the Capabilities Directorate, Workforce and Support Activities Directorate, Security and Counterintelligence Group, and other directorates responsible for developing, implementing, and monitoring the completion of the STE and STN initiatives. We also met with NSA officials responsible for monitoring user activity and observed how the NSA used specific tools to monitor user activities and devices connected to the NSANet. Additionally, we reviewed briefing charts, NSA/CSS policy instructions and procedures, and applicable security classification guides to determine whether the NSA implemented controls for securing and configuring its network infrastructure. We collected NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6, selected device configuration reports, STE and STN activity updates and plans to determine whether the NSA completed the STE and STN initiatives based on its stated goals.

(~~U//FOUO~~) We nonstatistically selected and visited three regions—NSAW in Washington DC, NSAH in Hawaii, and NSA (b)(3) PL 86-36 Section 6 —where equipment was connected to NSANet. We visited NSA (b) NSAW sites, NSA (b)(3) PL NSAH sites, and NSA (b)(3) PL 86-36 Section 6 sites in the three regions. We selected these three regions because NSAW is the NSA's Headquarters

(~~U//FOUO~~) location, and NSAH NSA (b)(3) PL 86-36 Section 6 worked. We conducted walkthroughs of the facilities to observe where the equipment was located and operated. We met with officials responsible for conducting physical inspections and overseeing security at the sites.

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Table 5. Sampled Devices at NSAW, NSAH, NSA (b)(3) PL 86-36 Section 6

~~S//NF~~				
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6				
				~~S//NF~~

(U) Source: The DoD OIG.

(U) Scope Limitation

(~~U//FOUO~~) The NSA did not provide sufficient information to test whether it NSA (b)(3) PL 86-36 Section 6 . Before conducting site visits, we discussed configuration data needed by the NSA to identify whether NSA (b)(3) PL 86-36 Section 6 . In February 2017, NSA officials informed us that NSA (b)(3) PL 86-36 Section 6

(~~U//FOUO~~) NSA (b)(3) PL 86-36 Section 6

(U) Use of Computer-Processed Data

(~~C//REL TO USA, FVEY~~) We used computer-processed data to perform this audit. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 In addition, the DoD OIG information technology specialists validated our methods used to analyze the computer-processed data.

(~~C//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) Use of Technical Assistance

(U) We worked with the DoD OIG Quantitative Methods Division to develop a method for selecting sites, enclaves, and a nonstatistical sample of devices. We also used the technical assistance of two information technology specialists from the DoD OIG Office of the Chief Information Officer. The information technology specialists provided expert knowledge on selecting devices in the sample, developing command scripts to obtain device configuration data, and validating the methods used to analyze audit results to complete testing at sites associated with NSAW, NSAH, NSA (b)(3) PL 86-36 Section 6.

(U) Prior Coverage

(U) During the last 5 years, the DoD OIG and the NSA Inspector General issued three reports discussing the NSA's ability to implement initiatives to secure its network and enterprise. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

(U) DoD OIG

(U) Report No. DODIG-2016-129, "The National Security Agency Should Take Additional Steps to Effectively Implement Its Privileged Access-Related Secure-the-Net Initiatives," August 29, 2016 (Document classified SECRET//NOFORN)

(U) NSA Inspector General

(U) Report No. AU-15-0014, "Audit of Removable Media," February 16, 2017 (Document classified SECRET//NOFORN)

(U) Report No. AU-14-0005, "Audit of NSANet Server Security," June 19, 2015 (Document classified CONFIDENTIAL//REL TO USA, FVEY)

(U) Appendix B

(U) STE Initiatives

(~~U//FOUO~~) The NSA is implementing NSA (b)(3) PL STE initiatives to design, manage, and defend all NSA/CSS systems, networks, communications, data, and critical infrastructure around the world as an integrated enterprise. The NSA categorized the initiatives in three major areas: maintain a secure enterprise, actively defend the enterprise, and integrate enterprise expertise. Table 6 identifies the STE initiatives, a description of the initiative, and the status of each initiative according to NSA officials.

(U) Table 6. List and Description of STE Initiatives

~~S//NF~~ STE Initiative	Initiative Description	NSA Reported Completion Status (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

~~S//NF~~ STE Initiative	Initiative Description	NSA Reported Completion Status (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

~~S//NF~~ STE Initiative	Initiative Description	NSA Reported Completion Status (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

~~S//NF~~ STE Initiative	Initiative Description	NSA Reported Completion Status (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

~~S//NF~~ STE Initiative	Initiative Description	NSA Reported Completion Status (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

(U) Source: The NSA.

(U) Appendix C

(U) STN Initiatives

(~~U//FOUO~~) The NSA is implementing NSA (b)(3) PL STN initiatives in response to the June 2013 security breach. The NSA categorized the initiatives in three major areas: tighten controls on computer systems, tighten controls on data, and increase oversight of its personnel. Table 7 identifies the STN initiatives, a description of the initiative, and the status of each initiative according to NSA officials.

(U) Table 7. List and Description of STN Initiatives

~~S//NF~~ STN Initiative	Initiative Description	NSA Reported Status of Completion (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

~~S//NF~~ STN Initiative	Initiative Description	NSA Reported Status of Completion (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

~~S//NF~~ STN Initiative	Initiative Description	NSA Reported Status of Completion (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

~~S//NF~~ STN Initiative	Initiative Description	NSA Reported Status of Completion (as of August 2017)
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6		
		~~S//NF~~

*(U) NSA (b)(3) PL 86-36 Section 6

(U) Source: The NSA.

(U) Management Comments

(U) National Security Agency

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

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

22 November 2017

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: (~~U//FOUO~~) Response to Request for Comment

REFERENCE: (U) Department of Defense Inspector General Draft Report, "The National Security Agency Enterprise" (Project No. D2017-D000RC-0001.000)

(U) The National Security Agency appreciates the work of the DOD Inspector General and welcomes this opportunity to provide comment to its draft report on the Agency's efforts to achieve effective network, personnel, and physical security configuration controls and processes.

(~~U//FOUO~~) We acknowledge and accept the DoD IG's observations during the period of this report NSA (b)(3) PL 86-36 Section 6

- (U) A lack of a prioritized comprehensive strategy;
- (U) Our inability to fully implement our plans;
- (U) Insufficient internal controls; and
- (U) A failure to adequately establish a physical inspections regime.

(~~S//REL TO USA, FVEY~~) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 We have maintained the commitment and focus of an incredibly talented and dedicated workforce, and through their work have achieved encouraging progress to address the DoD IG's findings. Specifically:

- (~~U//FOUO~~) The NSA Director set unified accountability and management controls conditions across all NSA mission and enterprise IT NSA (b)(3) PL 86-36 Section 6 for tracking implementation of, and ongoing compliance with, STN/STE requirements;

- (~~U//FOUO~~) The NSA Director approved a governance and implementation construct that has proven effective NSA (b)(3) PL 86-36 Section 6
NSA (b)(3) PL 86-36 Section 6

Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: ~~20421101~~

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

(U) National Security Agency (cont'd)

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

- ~~(U//FOUO)~~ NSA has dynamically adapted our implementation plans in pace with dynamic baseline changes, new discoveries, and emerging security technology & tradecraft;
- ~~(U//FOUO)~~ NSA has recalibrated personnel, physical, and industrial security processes and procedures and created a joint organization NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6
- ~~(U//FOUO)~~ NSA has established an integrated team, NSA (b)(3) PL 86-36 Section 6 combining the talent, technology, and techniques spanning our Operations, Research, Security & Counterintelligence, and Capabilities organizations NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 and
- (U) NSA has a comprehensive communications and action plan focused on affirming a culture of security consistent with stewardship of the classified national security information and systems with which we are entrusted.

(~~U//FOUO~~) We fully acknowledge the urgency of this effort NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 In our detailed comments we have outlined substantive progress since the date of this review, as well as our steps and timelines moving forward. Moreover, we have confidence in our course forward to achieve a secure baseline, and are enacting accompanying procedures to sustain that secure state in a manner consistent with our obligation to the American people. We can only be credible in our defensive mission if our own networks are the standard bearer for these best practices.

(~~U//FOUO~~) We welcome the insights and views of our DOD IG counterparts and we ask that you return to NSA later in FY18, following the projected 3rd quarter FY18 completion of our comprehensive security improvements, to assess whether we have achieved our desired outcome and to provide us any further recommendations or insights – even as we acknowledge improved security is an effort that never stops and must constantly evolve.

NSA (b)(3) PL 86-36 Section 6

MICHAEL S. ROGERS
Admiral, U.S. Navy
Director, NSA/Chief, CSS

Encl: ~~(U//FOUO)~~ NSA Response to Draft DoD IG Report "The National Security Agency Enterprise: Project No. D2017-D000RC-0001.000," dated 31 October 2017

Copy furnished:
Secretary of Defense
Vice Chairman, Joint Chiefs of Staff

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

(U) National Security Agency (cont'd)

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

22 November 2017

SUBJECT: ~~(U//FOUO)~~ NSA Response to Draft DoD IG Report "The National Security Agency Enterprise: Project No. D2017-D000RC-0001.000", dated 31 October 2017

~~(U//FOUO)~~ NSA appreciates the opportunity to review and respond to the DoD IG Report concerning "The National Security Agency Enterprise." NSA agrees with the findings of the DoD IG and welcomes their independent assessment. NSA fully acknowledges that the comprehensive work we have undertaken to protect all networks and systems associated with NSA's mission from insider and external threats NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 Given the complexity of deploying these defensive measures comprehensively across the NSA enterprise, we acknowledge that the Director of NSA (DIRNSA) set a challenging goal for completion NSA (b)(3) PL 86-36 Section 6 but he did so consciously to drive both completion and cultural change at NSA. Because of focused senior leadership attention at the highest levels, significant reallocation of resources (people and dollars), and the tireless work of the highly skilled NSA workforce, we continue to make significant progress and estimate that NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 we are on course to complete the designated tasks in 3QFY18. Protecting core national security secrets is a responsibility we take very seriously; it is also a task that will never be complete as we need to continuously adapt to new technologies and new threats. Accordingly, we value the DoD IG's feedback on the progress we had made through early 2017 in our endeavor to harden our networks and processes against insider and external threats, as well as your recommendations and insights to help us manage these efforts more effectively.

(U) The Complexity of NSA's Mission and Networks

~~(S//REL)~~ Given NSA's signals intelligence and information assurance missions, we know there are no silver bullets in information or network security. Throughout our existence, we have continuously evolved our security practices to incorporate new technologies and compensate for the ever-changing threat environment. Recent unauthorized disclosures by affiliated insiders caused the Agency to adopt and aggressively implement a comprehensive set of enterprise defensive measures designed around a defense in depth model. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

~~(S//REL USA, FVEY)~~ NSA has a very complex, diverse, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) technology environment composed of mission and enterprise (desktops, networks, office automation, business, collection, processing, and high performance computing) systems, operating at all classification levels, NSA (b)(1) EO 13526 Section 1.4g and (b) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section NSA's mission requires that we understand all of the constantly changing information, communication, and security technology used by our foreign intelligence targets (for our Signals Intelligence mission), as well as by the US Government and our allies (for our Information Assurance mission). We need to bring all of this diverse technology into NSA's networks, and then develop and globally deploy additional technology to exploit and/or defend it. To protect sensitive NSA missions and capabilities, as well as to enable NSA to safely study foreign malware, NSA's

Classified By: NSA (b)(3) PL 86-36 Section 6
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: ~~20421101~~

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

(U) National Security Agency (cont'd)

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

information technology. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36

(~~U//FOUO~~) Prior to August 2016, NSA had a federated approach to managing, securing, and defending its networks. While the NSA CIO had a policy and standards role that covered all NSA IT, the NSA CIO (dual hatted as the Technology Director) only had direct management control over enterprise IT and large-scale mission systems. Management controls over mission IT, and IT for some other specialized purposes, was federated to other NSA directorates. As NSA launched the Secure the Enterprise (STE) initiative in summer 2015, with DIRNSA's stated objective to deploy these defensive measures comprehensively and completely by NSA (b)(3) PL 86-36 Section 6 it became apparent to NSA leadership that this federated approach to IT NSA (b)(3) PL 86-36 Section 6 to uniformly achieving and maintaining the enhanced network security posture that is foundational to NSA's continued success.

(~~U//FOUO~~) These challenges, in fact, were a key driver in the restructuring of NSA (NSA21) that took place effective 31 August 2016, consolidating responsibility for developing, deploying, managing, securing, and defending all NSA IT networks and systems, at all classification levels and for all purposes across the NSA enterprise, into one directorate (Capabilities) headed by the Chief Information Officer (dual hatted as Capabilities Director). Another stated objective of NSA21 was to combine technology experts in the Capabilities Directorate (and operational experts in the Operations Directorate) from both the Signals Intelligence and Information Assurance missions in order to ensure that all NSA solutions and activities leveraged the full knowledge of NSA. In other words, the Director of NSA reorganized the Agency to create a Chief Technology Officer role (i.e. the Capabilities Director), to unify that role with the Chief Information Officer, and to set the conditions for unified management controls across all NSA mission, business, and enterprise IT.

(~~U//FOUO~~) Despite the disruptive nature of such a major reorganization, the newly established Capabilities Directorate has steadily gained momentum in executing the defensive measures reviewed by the DoD IG. Early in 2017, we established a governance and implementation construct that has been very effective. NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 alternate approaches have been needed to secure some of the more specialized networks to the STN/STE standards. As the orchestration and implementation teams have identified networks and enclaves NSA (b)(3) PL 86-36 Section NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 NSA has reprioritized significant resources (personnel, money and time) in support of this goal. Senior leadership across the Agency (including DIRNSA and the NSA Board of Directors) is fully engaged and there is unambiguous emphasis from DIRNSA on completing the work completely, comprehensively, and quickly. Thus, the insights provided by the DoD IG are valued and accepted and will be adopted to further enhance our security posture.

(~~S//REL USA, FVEY~~) Many of our missions present particularly complex situations which add challenges to reaching the desired defensive measures goals. For example, NSA employs a subset of our workforce NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 These particular circumstances resulted in the establishment of an additional set of security initiatives, NSA (b)(3) PL 86-36 Section 6 Defensive Measures (DM), developed by a cross-organizational DM Enterprise Functional Team (DMEFT).

2

(U) National Security Agency (cont'd)

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

~~(S//REL USA, FVEY)~~ In every phase of our increased security efforts (Secure the Network (STN), Secure the Enterprise (STE), and NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 It has always been recognized that a compilation of measures, or a defense in depth approach, is necessary to achieve the desired security posture. In addition to the layered defense approach, NSA quickly determined that reaching our objectives in our complex networks required a combination of NSA-developed Information technology and commercially available technology, with lots of adaptation along the way. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL USA, FVEY~~) Since summer 2015, NSA has also had a series of in depth discussions NSA (b)(1) EO 13526 Section 1.4g and (b)(3) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U) NSA's Defensive Measures

~~(S//REL USA, FVEY)~~ NSA's STN and STE defensive measures reviewed by the DoD IG extend the fundamental protections mandated by the DoD Cybersecurity Scorecard and add advanced security measures across all NSA networks NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 regardless of purpose or sensitivity. STN/STE applies the general principles recommended by NSA for all national security systems to our own complex, multi-domain enterprise, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 STN/STE will achieve the following outcomes:

- Privileged User Accountability: Ensure that no system administrator can take actions without being observed and that no system administrator can cover his/her tracks.
- Full Visibility: Ensure that we have an automated way to NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 (This is a cumulative outcome from several individual technical efforts.)
- Analytic Rigor: Ensure that all security-relevant events on NSA's hosts and networks are captured and fed into big data analytics. These analytics automatically detect anomalous activity on the network NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
- Secure Development: Initiate programs to ensure that new NSA capabilities are secure at deployment and remain so throughout their lifetime, leveraging automation to detect deviation from established security standards.
- Robust & Reliable Systems: Identify key mission systems and dependencies; invest in reliability and survivability for end-to-end threads for mission essential functions. Extend security to physical and industrial infrastructure supporting NSA facilities NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

3

(U) National Security Agency (cont'd)

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

- Security Beyond Technology: Complementary physical and personnel measures, including NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(~~S//REL USA, FVEY~~) NSA has re-prioritized significant resources to meet these objectives. Between FY14 and FY17, NSA expended NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 on efforts specific to implementation of STN, STE, and NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 To sustain these efforts going forward, NSA has internally budgeted NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 across the FYDP. In addition, NSA continues to utilize large numbers of highly skilled government personnel to manage implementation of currently approved security measures, NSA (b)(1) EO 13526 Section NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 and to continuously assess the effectiveness of our comprehensive approach against known and anticipated insider and external threats.

(~~U//FOUO~~) NSA recognizes that once these measures are in place, operating them for enterprise-wide defense and assurance will require long-term investment of personnel, analytic resources, and continuous innovation. This investment is essential to provide appropriate protection of NSA's operational capabilities and extraordinarily sensitive information. A particularly important part of this investment will need to be in fostering and maintaining a more aware/resolute/sophisticated culture of security across the entire workforce.

(~~U//FOUO~~) As NSA gains experience with these advanced techniques, we are committed to incorporating what we have learned into guidance issued by our information assurance mission, into defensive cybersecurity operations we conduct across the National Security community, and into engagements with partners on how to best protect our National Security assets.

(~~U//FOUO~~) Recommendation 1 – We recommend that the Director, Capabilities Directorate, and Chief Information Officer of the National Security Agency/Central Security Service:

a. **(~~U//FOUO~~) Verify** NSA (b)(3) PL 86-36 Section 6 **on all devices and authenticate all devices connected to the NSA enterprise.**

NSA Response: (~~S//REL USA, FVEY~~) **Agree.** We acknowledge the importance of this measure. At the time the DOD IG performed the audit of NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 still adapting its approach to properly implement this activity. We have since made significant progress NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

Target Completion Date: (U) 3QFY18

4

(U) National Security Agency (cont'd)

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

b. **(U//FOUO) Assess the volume of data across the National Security Agency enterprise, implement tools with the capacity to register and baseline all National Security Agency subnets** NSA (b)(3) PL 86-36 Section 6

NSA Response: (S//REL USA, FVEY) **Agree.** NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 is a key component of our overall initiative. We continue to make progress toward this goal; the rate of progress has increased. Our initial effort to baseline network utilization of NSANet subnets under STN NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 That work was completed in October 2014, but as previously noted, additional disclosures identified the need to extend this measure into all network enclaves. Achieving the necessary level of insight into all enclaves and the core NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//REL USA, FVEY) NSA agrees that registering all NSA subnets is a critical security measure and continues to expand the layered management process across all networked planes to include new and/or newly reported enclaves. A re-evaluation of alternative data analytics and network instrumentation has been conducted and as a result, NSA has concluded that a combination of data analytics and network instrumentation will scale to meet growing network monitoring needs, and leverage modern analytic platforms to support STE/STN initiatives. Efforts that support increased network monitoring are focused on analytics combining data from a variety of sources. As mentioned previously, a layered approach is best suited to implement this recommendation. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(U//FOUO) NSA is deploying an initial comprehensive capability (combining many solutions) as part of the STE deployment, which NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 However, the big data analytics and alerting mechanisms will continue to evolve over time as NSA develops progressively more sophisticated tactics to identify what is anomalous on our networks.

Target Completion Date: (U) 3QFY18

(U) Recommendation 2 – We recommend that the Director, Capabilities Directorate, National Security Agency/Central Security Service:

a. **(U//FOUO) Implement an automated solution to identify all devices connected to the National Security Agency enterprise and verify compliance with its global security policies.**

NSA Response: (S//REL USA, FVEY) **Agree.** Initially NSA's approach was to use a single capability NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 However, we made the same observation that NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 As a consequence, we have adjusted our STE implementation approach. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

5

(U) National Security Agency (cont'd)

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//REL USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

Target Completion Date: (U) 3QFY18

b. **(U//FOUO) Develop and implement procedures to verify that all devices that connect to the National Security Agency enterprise are properly configured** NSA (b)(3) PL 86-36 Section 6
NSA (b)(3) PL 86-36

NSA Response: (C//REL USA, FVEY) **Agree.** NSA's current efforts as part of STN/STE for NSA (b)(1) EO 13526 Section
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA is currently updating the STE Verification Checklists and validation procedures accordingly.

(C//REL USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

Target Completion Date: (U) 3QFY18

6

(U) National Security Agency (cont'd)

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

(U//FOUO) Recommendation 3 – We recommend that the Director, Capabilities Directorate, Chief Information Officer, and the Chief, Security and Counterintelligence, of National Security Agency/Central Security Service Chief Information Officer:

a. **(U//FOUO) Identify and validate the number and location of all enclaves connected to the National Security Agency enterprise;** NSA (b)(3) PL 86-36 Section 6
NSA (b)(3) PL 86-36 Section 6

NSA Response: (S//REL USA, FVEY) Agree. NSA requires that the STE measures be implemented in all networks, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 associated with the NSA mission, regardless of classification or purpose. STE coverage has been directed by DIRNSA to be complete and comprehensive; the various definitions of enclaves were intended to convey that point to the entire NSA enterprise. Since the primary networks and subnetworks associated with NSA's mission have been under direct management control of the NSA CIO since STE began, the emphasis has been on cataloging the enclaves that had been under federated control. Although different documents at NSA used slightly different language to describe an enclave, there was no practical significance because the requirement to implement STE is comprehensive across NSA. NSA has now established a single authoritative definition of "enclave", which is inclusive of all networks, NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g associated with NSA's missions and functions (regardless of purpose, classification level, or compartmentation). For completeness, we have now recorded even the core NSA Top Secret network, NSANet, as an enclave.

(S//REL USA, FVEY) Since NSA21, the Capabilities Directorate has established a single, authoritative list of all enclaves associated with the NSA mission (referred to as NSA (b)(1) EO 13526 Section 1.4g and (b)(3)). Although the first draft of NSA (b)(1) EO 13526 Section 1.4g and (b)(3) was created through the data calls indicated in the DoD IG report, the STE Advanced Verification teams (described in more detail in response to Recommendation 4 below) have been systematically working with all mission elements and all system administrators throughout the NSA enterprise to identify all enclaves associated with the NSA mission. When a new enclave is identified, both a senior manager within the appropriate mission element and the NSA CIO must approve its continued existence in writing; once approved the enclave/system is added to NSA (b)(1) EO 13526 Section 1.4g and (b)(3).

(S//REL USA, FVEY) NSA continues to identify new enclaves through ongoing data calls, mission owner engagements, and network inspections. All new enclaves must be approved by the NSA CIO and added to the online NSA (b)(1) EO 13526 Section system, which is part of the CIO Dashboard and the Source System of Record for enclave data. Additionally, NSA agrees that having the location data for the enclaves is important information to inform NSA's physical security activities. NSA has begun collecting that information for all enclaves and is entering the data in the online NSA (b)(1) EO 13526 Section system. This effort will be complete by 31 December 2017.

(U//FOUO) NSA (b)(3) PL 86-36 Section 6
NSA (b)(3) PL 86-36 Section 6

7

(U) National Security Agency (cont'd)

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

NSA (b)(3) PL 86-36 Section 6

(U//FOUO) NSA (b)(3) PL 86-36 Section 6
NSA (b)(3) PL 86-36 Section 6

(U//FOUO) NSA has created an authoritative and a comprehensive list of enclaves approved by the NSA CIO. We will continue to maintain an authoritative list as new enclaves are approved and previous enclaves are decommissioned. All new networks, enclaves, and systems added to NSA's enterprise will be required to be fully compliant with the STN and STE standards as part of their initial security authorization. With the dynamic nature of our networks and the connected IT devices, NSA will continuously review the validity and accuracy of NSA (b)(3) PL 86-36 Section 6 data and make adjustments as necessary. Procedures for monitoring enclaves and the plan to disconnect non-compliant devices will be updated.

Target Completion Date: (U) 3QFY18

b. **(U//FOUO) Conduct a risk assessment to identify the National Security Agency's most sensitive enclaves and data transfer agent locations, identify annual funding needed to conduct enhanced random entrance inspection at all locations, and, until the funding is provided, conduct continuous enhanced random inspections at the locations with the highest risk to the enterprise.**

NSA Response: (S//REL USA, FVEY) **Agree.** NSA appreciates the importance of physical security as a critical component to overall security of our personnel, systems, information and equipment. NSA's Security & Counterintelligence (S&CI) has taken multiple steps to increase security through various inspection initiatives. Resources have been identified and approved NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 and are pending conclusion of the continuing resolution and the hiring/clearance processing of inspection assets. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//REL USA, FVEY) Subsequent to the STN/STE efforts, NSA responded to the White House directed 30-day Security Review of High-Impact Unauthorized Disclosures with a prioritized list NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 In addition, NSA established a cross-agency functional team (Defensive Measures Enterprise Functional Team (DMEFT)) which, among other initiatives, conducted an analytical risk assessment to identify the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 The results were used to select the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 to be examined for defensive measures above the STN/STE standard and provided input to identifying the most sensitive enclaves and data transfer locations. As a result NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section were slated for enhanced personnel and physical security scrutiny to include the immediate funding and forthcoming procurement and implementation of continuous

8

(U) National Security Agency (cont'd)

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

enhanced physical security entry/exit inspections. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(C//REL USA, FVEY) Among NSA's defense in depth approach to achieving greater security are four coordinated efforts covering Mission Security (modifications in procedure, access and control), Personnel Security (increased vetting and polygraphs), User Activity Monitoring (increased coverage and focus) and Physical Security (Enhanced two person controls, REIPs and full-time Enhanced Inspections). Under the auspices of the DMEFT efforts, NSA has implemented Enhanced Inspections (EIs) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) These EIs are in addition to Aperiodic Exit Inspections (AEI) which are performed by Access Control Specialists throughout the day at all NSA-Washington (NSAW) and Cryptologic Center lobbies, and REIPs which continue across the entire NSA extended enterprise; all of which are currently being executed with existing resources NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL

(U//FOUO) Noted decreases in REIPs from June 2014 to May 2017 failed to include AEIs which should have also been taken into account in order to form a more complete picture of NSA's level of effort and prioritization against satisfying STE objectives. Coinciding with the implementation of REIPs, NSA also increased the number of AEIs conducted by Access Control Specialist (ACS) contractors (random exit inspections without metal detectors) across the NSA enterprise. When taking into account all these physical security efforts, NSA experienced an overall increase in exit inspections during this timeframe (June 2014-May 2017). NSA increased the total number of inspections each year: NSA (b)(3) PL 86-36 Section 6
NSA (b)(3) PL 86-36 Section 6

(S//REL USA, FVEY) Inspections at NSAW & Violations Discovered					
Dates	REIP Inspections	REIP Violations	Aperiodic Inspections	Aperiodic Violations	TOTAL Inspections
June 2014-May 2015	NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6				
June 2015-May 2016					
June 2016-May 2017					
June 2017-Oct. 2017					

(U//FOUO) NSA is committed to implementing additional inspections, as a complement to other security efforts, at future NSA (b)(3) PL 86-36 Section 6 locations.

Target Completion Date: (U) 3QFY18

9

(U) National Security Agency (cont'd)

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

c. **(~~U//FOUO~~) Identify all desktop computers connected to the National Security Agency network, conduct a risk assessment to determine how to monitor devices where user activity monitoring is not being conducted, and conduct periodic testing to ensure that an automated monitoring tool is deployed and actively reporting user activity.**

NSA Response: (~~S//REL USA, FVEY~~) **Agree.** As described in the response to recommendation 2a above, NSA is working an ambitious, multi-faceted approach to identify user interaction with all devices NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 that are connected to the network. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

(~~U//FOUO~~) Regarding an automated monitoring tool, NSA has developed an analytic capability to identify in-scope devices that are both covered and uncovered from a UAM standpoint. This analytic feeds automated notification to NSA (b)(3) PL 86-36 Section 6 NSA (b)(3) PL 86-36 Section 6 In addition, we provide guidance on how to correct devices that are not UAM compliant in an effort to increase consistent UAM coverage across the enterprise. This initiative was piloted in August 2017 and operationalized in September 2017 with notifications being sent on a weekly basis.

(~~S//REL USA, FVEY~~) Automated UAM coverage metrics are already in place through the CIO Dashboard. The automated notification mechanism is currently in use. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 are currently being tested and operationalized.

Target Completion Date: (U) 3QFY18

d. **(~~TS//REL USA, FVEY~~) Take immediate action to secure the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 8 enclave to include identifying all connected devices, monitoring user activity, and**

NSA Response: (~~C//REL USA, FVEY~~) **Agree.** A combination of teams across the Agency has initiated, implemented and continues to improve mitigating security measures within the NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 enclave.

(~~TS//REL TO USA, FVEY~~) The NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Defensive Measures activity was established in October 2016 to focus on particularly sensitive and critical mission areas where the unique technical, architectural, or operational characteristics of the mission and networks require advanced measures beyond STN and STE to protect them against determined insider threats. NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 [redacted]

10

(U) National Security Agency (cont'd)

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(S//REL USA, FVEY) NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6
NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

(TS//REL USA, FVEY) A team of subject matter experts from a wide range of disciplines, including NSA (b)(1) EO 13526 Section mission, capabilities development, information technology, counterintelligence, physical security, personnel security, facilities, and legal, assembled to develop a set of recommendations for securing NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 standards. To substantially reduce risks to our NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section this experienced team identified the largest NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 enclave as its primary initial focus in December 2016.

- Core mission components of NSA (b)(1) were identified, including supporting IT infrastructure, physical perimeter, associated personnel NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 and current risk mitigation measures.
- A risk awareness process was established, scoring a weighted set of NSA (b)(1) risks against the list of mitigations to quantify the expected reduction in risk.

(S//REL USA, FVEY) The output of these two efforts led to the following:

- IT equipment and applications are being modernized and standardized in compliance with the STN/STE requirements.
- NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 tighten access control and remove local and unnecessary duplicate copies of data.
- Complementary IT/infrastructure and physical security plans are underway to separate physical access from administrative control and implement user activity monitoring where technically feasible.
- Physical security measures are being implemented to increase entrance and exit inspections in areas associated with NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

Target Completion Date: (U) 3QFY18

11

(U) National Security Agency (cont'd)

TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

(U//FOUO) Recommendation 4 - We recommend that the Director, National Security Agency/Central Security Service, validate whether the National Security Agency's actions to implement Secure-the-Net and Secure-the-Enterprise initiatives that it reported as complete are sufficient to fully meet the goals of the initiatives, and assess whether the strategy and allocation of resources to effectively complete the initiatives for ongoing campaigns will enable the National Security Agency to meet its stated goals.

NSA Response: (S//REL TO USA, FVEY) **Agree.** DIRNSA and the NSA Board of Directors have been directly involved in regular reviews of the implementation of STN, STE, and enhanced defensive measures for NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 since November 2016. NSA has implemented a well-documented checks and balances approach to validating the satisfactory completion of STN/STE work (see below). Once STN and STE measures have been completely deployed, NSA will randomly but frequently spot check sufficiency of ongoing verification measures. From a resource perspective we have captured the expected costs associated with achieving and maintaining the desired end state. As the infrastructure and threats evolve, we will need to adjust our resource strategy accordingly.

(S//REL USA, FVEY) To ensure that all STN and STE measures were implemented across all NSA networks (Top Secret, Secret, and Unclassified), including all enclaves NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6

- (U//FOUO) NSA developed STN/STE specific checklists for all technical measures which must be implemented on each network and in every enclave, and documented formal verification procedures with designated entities as the official verifier for each checklist item. The requirement to implement these measures was formally signed by the NSA CIO, as well as procedures and delegations to address any proposed exceptions.
- (U//FOUO) For each checklist item, playbooks have been developed describing the approved technical solutions and associated monitoring approaches to achieve full compliance. As new solutions are approved by the NSA CIO, they are added to the playbook.
- (U//FOUO) The NSA CIO/Capabilities Director divided the entire NSA mission and function space into four bins and assigned an Orchestration Lead to each with responsibility for ensuring that every enclave associated within their bin across the NSA enterprise was brought into full STN/STE compliance. These leaders comprise the Orchestration team.
- (U//FOUO) Each Orchestration Lead established an Execution Team to oversee bringing all of their assigned enclaves into compliance. These Execution teams were then augmented by 12 Advanced Verification teams to assist individual enclave owners with implementation of all required checklist items, to monitor schedules for completion, and to determine when a specific enclave is ready for formal verification for each checklist item. NSA (b)(3) PL 86-36 Section 6
NSA (b)(3) PL 86-36 Section 6
- (U//FOUO) The NSA CIO required core NSANet to implement the standards and requirements spelled out in the Enclave Checklist, to ensure core NSANet is brought into full STN/STE compliance as well NSA (b)(3) PL 86-36 Section 6
- (U//FOUO) To ensure that enclaves remain compliant, NSA established a CIO dashboard which receives automated feeds from the centralized big data analytics that determine

12

(U) National Security Agency (cont'd)

the percentage of coverage for each checklist item for each enclave, for all checklist items capable of automated verification. For the remaining items, manual independent validation is the best that can be achieved; periodic manual validations are also included in the dashboard.

- (S//REL USA, FVEY) NSA also established a Program Management team to identify and track all resources and purchases required to implement all STN/STE measures. The team has worked with NSA leadership to reprioritize resources as required. In addition to the NSA (b)(1) EO 13526 programmed to add advanced security measures across all NSA networks (Top Secret, Secret and Unclassified), the Agency also reprioritized NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 funding, received an additional NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 supplemental funding, and reprioritized thousands of government resource hours to accelerate the implementation timeline. The Agency, as a whole, is aggressively moving forward to complete these initiatives.

Target Completion Date: (U) 3QFY18

(U//FOUO) Recommendation 5 - We recommend that the Chief Information Officer, National Security Agency/Central Security Service, develop and implement a comprehensive plan with metrics that clearly outline the methodology to complete the Secure-the-Enterprise initiatives and apply a similar methodology to implement the NSA (b)(3) PL 86-36 Section 6 initiatives.

NSA Response: (S//REL USA, FVEY) **Agree.** Under direct supervision from DIRNSA, the NSA CIO is executing a comprehensive, time-bound plan, with metrics, to complete the STN and STE initiatives. NSA is simultaneously executing a plan to complete additional initiatives tailored to NSA (b)(3) PL 86-36 Section 6 effort. All STN, STE and NSA (b)(3) PL 86-36 Section initiatives are progressing toward completion.

(S//REL USA, FVEY) Responding to the unauthorized disclosures since 2013, NSA identified a set of STN and then STE measures that would collectively reduce the risk posed by a malicious insider. The STE initiative (like the STN effort that preceded it) began with a formal risk assessment conducted by a cross-disciplinary team of experts drawn from both the foreign intelligence and defensive missions at NSA, which considered all possible insider and external risks to NSA's networks and the relative effectiveness of various prevention and mitigation techniques. Our evaluation of risks and mitigations was informed by industry leaders and other U.S. Government agencies. This risk assessment and the most effective and implementable mitigations were approved by DIRNSA in August 2015. The approved STE mitigations are documented in a placemat (with deadlines noted for each measure), as well as a more detailed checklist with implementation-level playbooks for the execution teams. Progress of each STE measure is tracked via a near real-time dashboard, and briefed to the NSA's Chief Information Officer/Director of Capabilities on a weekly basis, to DIRNSA at least monthly (with additional meetings on specific topics), and to NSA's Board of Directors biweekly, to ensure its continued emphasis as one of the DIRNSA's top priorities.

(S//REL USA, FVEY) NSA established the Defensive Measures Enterprise Functional Team (DMEFT) in October 2016 to articulate, and oversee the implementation of, a mitigation strategy to quantifiably reduce the risk posture of NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 NSA (b)(1) EO 13526 Section 1.4g and (b)(3) PL 86-36 Section 6 Building on the STE initiatives already being executed,

13

(U) National Security Agency (cont'd)

~~TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL~~

premised on the concept of a focused and layered security approach, and drawing from the cross-organizational makeup of the DMEFT as well as several senior Subject Matter Experts within the NSA (b)(1) EO community, the DMEFT constructed a methodology to harden the NSA (b)(1) environment. Like STE, the defensive measures for NSA (b)(1) EO are documented in a placemat, checklist, and detailed playbooks and the implementation progress is tracked via an NSA (b)(1) EO 13526 Section scorecard, which is also regularly briefed to NSA Senior Leaders.

Target Completion Date: (U) 3QFY18

~~(U//FOUO~~) NSA recognizes the need to maintain the momentum currently driving the implementation of STN, STE and NSA (b)(3) PL 86-36 Section initiatives, and will continue to invest human and financial capital in FY2018 and beyond to sustain the entirety of defensive measures as an NSA top priority. Additional enhancements and expansions of STE and NSA (b)(3) PL 86-36 Section measures are under discussion for implementation in 2018 as our security efforts are never "complete."

14

(U) Glossary

(U) **Active Directory.** A Microsoft solution used to store user computer security policies.

(U) **CASCADE**. A commercial product used to baseline subnets and identify unauthorized subnet behavior.

(~~U//FOUO~~) **Data Transfer Agent (DTA).** Designated personnel approved to [redacted] transfer data to or from an information system.

(~~U//FOUO~~) **Enclave.** A collection of computing, non-computing, or network devices that do not have external connectivity or are protected from other networks by a security device such as a boundary or firewall or standalone. The enclaves included in the scope of the NSA enterprise are [redacted]

(~~U//FOUO~~) **NSA Network (NSANet).** The composite of all infrastructure, connected devices, enterprise environment, and community services owned, leased, and operated by the NSA/CSS and affiliated organizations.

(~~U//FOUO~~) **Orbitcity**. A commercial product [redacted]

(U) **Port Security.** Denies network access to devices [redacted]

(U) **Portal.** Ingress or egress point in a NSA facility where REIPS occur.

(U~~//FOUO~~) **Prohibited Items.** Items that constitute threats to installation security or personal safety [redacted].

(~~U//FOUO~~) **Removable Media.** A portable electronic data medium that can be added to or removed from a computing device or network to store or transfer information.

(~~U//FOUO~~) **Restricted Items.** Items that constitute a technical threat to NSA/CSS information [redacted]

(~~U//FOUO~~) **SILENTSPARROW.** An automated tool [redacted]

(U) **Subnet.** The logical grouping of connected network devices on an internet protocol, which is the standard protocol for communicating across networks.

(U) **Thick Client.** A computing device that acts as a user interface to access data stored locally, another desktop, application, server or system.

(U) **Thin Client.** A computing device that acts as a user interface to a backend infrastructure.

(U) **Token.** A physical object used to authenticate identity.

(U~~//FOUO~~) **WATCHMAN.** A process that provides audit capability [redacted] NSA (b)(3) PL 86-36 Section 6

(U) Sources of Classified Information

Source 1: (U) Permanent Select Committee on Intelligence, "Intelligence Authorization Act for Fiscal Year 2016:" (Document classified TOP SECRET//SI//TK//NOFORN)
Generated Date: June 15, 2015

Source 2: (U) NSA-provided Secure-the-Net Activity Update, November 2016: (Document classified CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: November 1, 2041
Generated Date: November 1, 2016

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 4, 2016

Source 4: (U) NSA-provided Securing the Net Update, August 2017 (Document classified SECRET//REL TO USA, FVEY)
Declassification Date: August 1, 2042
Generated Date: August 1, 2017

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 Securing the Enterprise Detail Report," (Document classified TOP SECRET//SI//NF)
Declassification Date: October 1, 2042
Generated Date: January 12, 2017

Source 7: (~~U//FOU~~O) DoD OIG Report No. DODIG-2016-129, "The National Security Agency Should Take Additional Steps to Effectively Implement its Privileged Access-Related Secure-the-Net Initiatives" (Document classified SECRET//NOFORN)
Declassification Date: March 8, 2041
Generated Date: August 29, 2016

Source 8: (~~U//FOUO~~) Industry Update on "Secure the Net" "Secure the Enterprise (Document is classified TOP SECRET//SI//NOFORN)
Declassification Date: November 1, 2040
Generated Date: April 25, 2017

Source 9: (~~U//FOUO~~) "NSA/CSS Network Security Strategy: Secure the Enterprise Quad Charts" (Document is classified CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: October 1, 2040
Generated Date: September 10, 2015

Source 10: (~~U//FOUO~~) "NSA/CSS Network Security Strategy: Secure the Enterprise Quad Charts" (Document is classified CONFIDENTIAL//REL TO USA, FVEY)
Declassification Date: January 27, 2042
Generated Date: January 27, 2017

Source 11: (~~U//FOUO~~) "Secure the Enterprise Update, November 20, 2015" (Document is classified TOP SECRET//NOFORN)
Declassification Date: November 20, 2039
Generated Date: November 20, 2015

Source 12: (U) Enclave Master NSA (b)(3) PL 86-36 Section 6 Provided by the NSA (Document is classified TOP SECRET//SI//NOFORN)
Declassification Date: February 1, 2042
Generated Date: February 2, 2017

(U) Acronyms and Abbreviations

CSS	Central Security Service
CIO	Chief Information Officer
COA	Course of Action
NSA (b)(3) PL 86-36 Section 6	
DTA	Data Transfer Agent
IP	Internet Protocol
MAC	Media Access Control
NSA	National Security Agency
NSAH	National Security Agency Hawaii
NSANet	National Security Agency Top Secret Network
NSAW	National Security Agency Washington
REIP	Random Entrance Inspection Program
STE	Secure-the-Enterprise
STN	Secure-the-Net
S&CI	Security and Counterintelligence
TS	Top Secret

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

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

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
www.dodig.mil/pubs/email_update.cfm

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098