

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

7 April 2008
IG-10919-08

TO: DISTRIBUTION

SUBJECT: (U) Report on the Assessment of Management Controls to Implement the Protect America Act of 2007 (ST-08-0001)—ACTION MEMORANDUM

1. (U) This report summarizes our Assessment of Management Controls to Implement the Protect America Act of 2007 (ST-08-0001) and incorporates management's response to the draft report.

2. (U//~~FOUO~~) As required by NSA/CSS Policy 1-60, NSA/CSS *Office of the Inspector General*, actions on OIG recommendations are subject to monitoring and follow-up until completion. Therefore, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." If you propose that a recommendation be considered closed, please provide sufficient information to show that actions have been taken to correct the deficiency. If a planned action will not be completed by the original target completion date, please state the reason for the delay and completion date. Status reports should be sent Assistant Inspector General for Follow-up, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

3. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended to the auditors the review. For additional please 963-2988 or via e-mail

(b) (3)-P.L. 86-36

George
Inspector General

roved for Release NSA on 11-10-2015. FOIA Case #80120

DISTRIBUTION:

DIR

D/DIR

GC

D/GC(O)

Signals Intelligence Director

Chief, SID/PPAS

Chief, SV

SID/POC IG Liaison SV

Chief, S2

Chief, S3

Chief, S33

Chief, S332

cc:

IG

D12

D13

D14

(U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(S//SI)~~ NSA has implemented procedures to comply with the provisions of the Protect America Act of 2007 (PAA), which modified the Foreign Intelligence Surveillance Act (FISA) and was signed into law on 5 August 2007. To protect the privacy rights of U.S. persons, the new legislation required NSA to implement and follow procedures established by the Director, NSA (DIRNSA) to ensure its adherence to three requirements: that targets are located overseas, that the foreign intelligence purpose is significant, and that personnel follow applicable minimization procedures. In general, management controls to comply with PAA requirements are adequate. Specific controls to determine that targets are located overseas are especially strong.

~~(S//SI)~~ Made necessary by the technology changes that have occurred since the FISA was drafted in 1978, "FISA modernization" was intended to restore the effectiveness of the Act by eliminating the requirement for NSA to obtain court orders for monitoring the communications of persons physically located outside of the United States. Although the PAA expired in February 2008, NSA collection permitted under its provisions will continue for up to another year.

(U) HIGHLIGHTS

(U) The Office of the Inspector General assessed procedures established by DIRNSA to ensure compliance with the three PAA requirements. Management concurred with the recommendations.

- (U) NSA immediately implemented DIRNSA-directed procedures on compliance with the PAA. Management controls to determine that targets are located overseas are particularly strong.
- ~~(S//SI//REL TO USA//FVEY)~~ PAA tasking needs additional controls. Though current controls provide reasonable assurance of compliance with the PAA, additional controls are needed to verify that only authorized selectors are on collection and that information acquired through the use of selectors is related to the expected foreign intelligence targets.
- (U) More rigorous controls will increase the reliability of [] for PAA compliance. While existing [] are excellent preventive and detective controls, current methodologies are not rigorous enough to draw valid conclusions about the entire population.

(U) This page intentionally left blank.

(U) TABLE OF CONTENTS

(U) EXECUTIVE SUMMARY I

(U) TABLE OF CONTENTS III

I. (U) BACKGROUND..... 1

II. (U) FINDING 3

III. (U) SUMMARY OF RECOMMENDATIONS 11

(U) ACRONYMS AND ABBREVIATIONS..... 13

APPENDIX A - (U) About the Review

APPENDIX B - (U) Assessment of Management Controls

APPENDIX C - (U) Full Text of Management Comments

(U) This page intentionally left blank.

I. (U) BACKGROUND

(U) The Protect America Act of 2007

~~(S//SI//REL TO USA, FVEY)~~ On 5 August 2007, the President signed into law the Protect America Act (PAA) of 2007. The PAA, which expired on 16 February 2008, amended the Foreign Intelligence Surveillance Act (FISA) of 1978. Specifically, the PAA authorized the Attorney General (AG) and Director of National Intelligence (DNI) to approve, without a court order, the collection of foreign intelligence information from facilities located inside the United States concerning persons reasonably believed to be located outside the United States, subject to certain criteria. As of 31 March 2008, NSA had approximately [] Internet selectors and [] telephony selectors on PAA-authorized collection. From the passage of the PAA through 31 March 2008, NSA had issued [] reports that included PAA-derived intelligence.

(U) Requirements of the PAA

(U) The objective of our review was to assess the adequacy of management controls to implement and ensure compliance with three requirements of the PAA related to NSA operations:

(b) (1)
(b) (3) - P.L. 86-36

- ~~(S//SI//Foreignness)~~¹ Selectors on PAA collection must concern "persons reasonably believed to be located outside of the United States."
- ~~(S//SI//Foreign Intelligence Purpose)~~ A significant purpose of the collection is to obtain foreign intelligence information.
- (U) Minimization Procedures. NSA personnel must follow appropriate minimization procedures.

~~(S//SI//REL TO USA, FVEY)~~ At the time of our review, the AG and DNI issued [] separate certifications that authorize NSA to acquire foreign intelligence information of certain targets:

¹ (U) NSA's reasonable belief that a target is located outside of the United States based on one or more pre-determined factors.

(b) (1)
(b) (3) - P.L. 86-36



(U) These certifications were based on representations made by the Director of NSA (DIRNSA) in affidavits that detail the management controls and procedures that NSA will follow.

(U) Standards of Internal Control

(U) We assessed management controls against the General Accounting Office's *Standards for Internal Control in the Federal Government*, November 1999, which presents the five standards that define the minimum level of quality acceptable for management control in government—Control Environment, Risk Assessment, Control Activities, Information and Communications, and Monitoring.

(U) Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations. NSA/CSS Policy 7-3, *Internal Control Program*, advises that evaluations of internal control should consider the requirements outlined by the Standards. The Office of the Inspector General (OIG) uses the Standards as the basis against which management control is evaluated.

II. (U) FINDING

~~(S//SI)~~ Since the PAA was passed in August 2007, Agency management has made progress in implementing the PAA and establishing management controls that are crucial to ensuring compliance with the PAA. NSA implemented all the procedures delineated by DIRNSA in the affidavits to the certifications. The controls implemented to verify that selectors tasked under the PAA for targets located outside of the United States are particularly strong. Nevertheless work remains to implement additional controls to:

- ~~(S//SI)~~ Verify [] that authorized selectors, and only those selectors, are on collection.
- ~~(S//SI)~~ Verify that analysts routinely review intercepted data and confirm that information acquired is related to the expected foreign intelligence targets.
- (U) Improve the validity and reliability of various [] of PAA compliance by Agency management. (b)(3)-P.L. 86-36
- (U) Improve target analysts' understanding of the PAA.

(b) (1)
 (b) (3) - P.L. 86-36
 (b) (3) - 50 USC 3024 (i)

(U) Assessment details are included in Appendix B.

(U) NSA Immediately Implemented DIRNSA-directed procedures on compliance with the PAA

(U) Within weeks of the PAA enactment, NSA implemented the procedures that DIRNSA delineated in the affidavits and built on those procedures to establish rigorous processes to ensure compliance with the three requirements of the PAA. Management controls to determine and document foreignness were particularly strong. Controls covering foreign intelligence purpose and compliance with minimization procedures were also adequate.

(U) Some examples of NSA's accomplishments to date are:

- (U//FOUO) The PAA Implementation Team was established to coordinate all aspects of PAA implementation. Components of the team include internal and external communications, collection and data flows, mission operations, and policy and oversight.

- ~~(S//SI//REL TO USA, FVEY)~~ Telephony and Internet selector tasking systems were updated to allow analysts to document the foreignness determination. Also, controls were programmed into tasking systems to ensure that required information is documented and tasking is appropriate to AG/DNI certification targets.
- (U//FOUO) Within weeks of PAA passage, Signals Intelligence Directorate (SID) Oversight & Compliance (O&C) office, with the Office of General Counsel (OGC) and the Associate Directorate for Education and Training, had developed interim training that included a briefing by an OGC attorney and a competency test. On January 9, 2008, O&C deployed new and improved training.
- (U//FOUO) Agency management developed and published standard operating procedures, including procedures for training and raw traffic access, tasking, and incident reporting that will ensure consistent application of the PAA.
- (U//FOUO) A PAA web site was established to provide the NSA workforce with consistent, reliable, and timely information. From a single location, target analysts can read communications from NSA leadership, access certification-related documents, and view PAA-related standard operating procedures (SOPs).
- (U//FOUO) The PAA Procedures and Analytic Support (PPAS) team runs various processes to ensure compliance with the PAA. Specifically, PPAS personnel conduct foreignness checks of current targeting and notify target analysts of potential changes to a target's status. They also perform various of taskings for compliance with other PAA requirements and guide target analysts through the ta cting and tasking processes.

(b) (3) - P.L. 86-36

(U) PAA tasking needs additional controls

~~(S//SI)~~ Although NSA implemented a series of controls to provide reasonable assurance that target analysts task only authorized selectors—selectors that meet the foreignness and foreign intelligence purpose requirements—additional controls are needed to verify that only authorized selectors are on collection and that tasked selectors are producing foreign intelligence of the expected targets.

~~(S//SI)~~ Controls are needed to verify [redacted] that authorized selectors, and only those selectors, are on collection.

~~(S//SI//REL TO USA, FVEY)~~ With the telephony tasking system, and to some extent the Internet selector tasking system, [redacted] a risk of discrepancies

[redacted] Ultimately, discrepancies might result in violations of over-collection—selectors that are on collection that should not be—and incidents of under-collection—selectors that are not on collection but should be. Periodic reconciliation of NSA and provider records is critical to identify and resolve discrepancies and minimize violations and incidents.

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)

~~(S//SI)~~ At the time of our review, NSA had not fully reconciled Agency [redacted] tasked selectors. Although Collection Managers prepared draft reconciliation procedures, the procedures were manual. [redacted]

[redacted]

[redacted]

~~(S//SI)~~ Implement [redacted] process that routinely reconciles PAA-tasked selectors with the providers.
(ACTION: S3/Chief, 8332)

(b) (1)
(b) (3) - P.L. 86-36

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

(U) Management Response

CONCUR. ~~(S//SI//NF)~~ [redacted]

Status: OPEN
Target Completion Date: 18 May 2008

(U) OIG Comment

(U) Planned and ongoing actions meet the intent of the recommendation.

~~(S//SI)~~ Controls are needed to validate that target analysts routinely confirm that information acquired through the use of selectors is related to the expected foreign intelligence targets.

~~(S//SI)~~ PAA Standard Operating Procedures #2-07, Analyst Checklist, obligates target analysts to periodically "review intercepted data and confirm that the tasked selector is producing foreign intelligence from the expected target (which is authorized under the Certification)." A supplementary SOP on the analysts' obligation to review was in draft. Additional controls are needed to monitor compliance with this requirement to ensure that unintended persons are not mistakenly targeted.

~~(S//SI)~~ Implement controls to verify that target analysts routinely review intercepted data and confirm that information acquired through the use of selectors is related to the expected foreign intelligence targets.

(ACTION: Chief, S2 with O&C)

(U//FOUO) In December 2007, Analysis and Production personnel said they are considering an automated report that will determine whether target analysts query, and therefore review, communications in the collection databases. Although such a report is technically feasible, its usefulness as a management control remains uncertain.

(U) Management Response

CONCUR. ~~(S//SI)~~ The Deputy Director for Analysis and Production (DDAP) is working with O&C to establish formal controls to verify that target analysts routinely review both telephony and internet-based collection. The system currently being devised will

Status: OPEN

(b) (1)

Target Completion Date: 30 June 2008 P.L. 86-36

(b) (3)-50 USC 3024(i)

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

(U) More rigorous methodologies will improve the reliability of NSA spot checks

(U//~~FOUO~~) As shown in Appendix B, NSA is conducting, or plans to conduct, [] that are important to ensure compliance with the requirements of the PAA. Specifically,

- ~~(S//SI)~~ The PPAS team is conducting [] of foreignness determinations (with limited checks of foreign intelligence purpose) of selectors tasked under the PAA.
- ~~(S//SI)~~ The SID O&C reviews selectors pulled for AG/DNI reviews and is working on plans to conduct [] of targeting decisions that will complement AG/DNI reviews without being redundant.
- (U//~~FOUO~~) O&C conducts [] superaudit reviews of queries in raw traffic databases to ensure compliance with the appropriate certification and minimization procedures.
- (U//~~FOUO~~) O&C conducts [] reviews of all reports generated by PAA collection to ensure adherence to NSA policy and standard minimization procedures.

(U) While such checks are excellent preventive and detective controls, neither organization had documented its [] procedures or considered using quality assurance and statistical sampling techniques that would strengthen the reliability of the results. In particular, neither organization had documented formal methodologies that specified the universe, population, sample size, and means of selecting items for review. The bases for sample sizes were unstructured and sample item selections were judgmental rather than truly random.² Sampling results were therefore not rigorous enough to draw valid conclusions about the entire population.

(b)(3)-P.L. 86-36

(U) Integration of statistical sampling or quality assurance techniques into existing and planned methodologies will not only increase the validity and usefulness of the [] but will likely decrease the frequency, time, and effort needed to conduct them. In short, well-planned methodologies will improve the reliability and efficiency of these important controls.

²(U) For a sample to represent a population, all items should have an equal probability of selection. Only samples that are truly random (e.g., by using a random number table to select items) are representative of the population. Samples based on haphazard or judgmental methods may be biased and are unlikely to be representative of the population.

~~(U//FOUO)~~ Develop and document rigorous methodologies for conducting [] of PAA compliance.

(ACTION: Chief, O&C and Chief, PPAS)

~~(U//FOUO)~~ In January 2008, the Chief, O&C stated that both O&C and PPAS are working on more rigorous methodologies.

(b) (3) -P.L. 86-36

(U) Management Response

CONCUR. ~~(S//SI//REL)~~ Management stated that O&C is documenting methodologies and procedures for conducting [] [] The management response did not include planned corrective actions for PPAS []

Status: OPEN

Target Completion Date: 2 May 2008

(U) OIG Comment

(U) Planned action meets the intent of the recommendation for O&C. Planned action for PPAS remains unresolved.

(U) Target analysts need greater understanding of the PAA

~~(U//FOUO)~~ As shown in Appendix B, NSA has made significant progress in implementing a critical management control - training and awareness. Agency-wide e-mails, workforce presentations, a PAA-dedicated web site, and interim training are used to communicate with the NSA workforce. Improved training will further highlight aspects of the PAA authority most relevant to target analysts. However, two additional improvements are needed to provide target analysts the tools and guidance they need to implement the PAA.

(U) Working Aid or Quick Reference on NSA Authorities

~~(U//FOUO)~~ Given the increasingly complex and dynamic web of authorities under which NSA operates, target analysts are at risk of misunderstanding the PAA authorities. Although existing training and awareness provides details on the PAA, analysts might still be confused about how it differs from other NSA authorities. A working aid or quick reference that compares the basic elements and requirements of NSA's various authorities, with links to the authorities themselves, will help analysts navigate through the many documents and legalese and reduce the risk of violations.

Such guidelines and working aids should be available to employees at all times.

(U//FOUO) Publish and maintain a working aid that compares key requirements for SIGINT collection, processing, retention, and dissemination authorized by E.O. 12333 with requirements of other significant additional authorities, for example the PAA and FISA. In the working aid, provide links to the authorizing documents.

(ACTION: O&C with OGC)

(U//FOUO) The Chief, O&C, stated that planning has begun to develop a course that will include an overview and explanation of NSA's authorities, when to use them, what needs to be done to acquire them, and what the handling and minimization procedures are for each. If a working aid becomes an element of such training, we recommend that it be made available to the workforce as soon as possible rather than be tied exclusively to the training course.

(U) Management Response

CONCUR. **(U//FOUO)** Management stated that O&C levied a requirement for the Associate Directorate for Education and Training to develop an overview course of NSA's surveillance authorities. Course development is well underway and includes a requirement for a job aid.

Status: OPEN

Target Completion Date: 25 April 2008

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

(U) Communicating PAA-related Guidance (b)(1)

(b)(3)-P.L. 86-36

(S//SI) Not surprisingly, certain overarching questions on how to apply and comply with the PAA surfaced during our review. For example, target analysts expressed their uncertainty on quering and purging communications of targets [redacted] the United States. However, no mechanism was in place to keep the analysts informed of what to do while O&C consulted with OGC and developed the needed guidance. For example, by the end of our review, OGC had issued guidance in an e-mail to O&C, who subsequently decided that PPAS, rather than the target analysts, would purge collection for PAA incidents; but, existing procedures

were not updated to reflect this change. As NSA personnel continue to apply the PAA, more questions and uncertainties will inevitably emerge. To minimize confusion, a process is needed to vet, communicate, and post PAA guidance as a reference until it can be incorporated into more formal policy or SOPs, if needed.

(U//FOUO) Implement a process to vet, communicate, and post PAA guidance until it can be incorporated into policy or SOPs.

(ACTION: O&C)

(U) Management Response

CONCUR. (U//FOUO) Management stated that O&C would work with the OIG, OGC, SID Policy and the PAA Legal/Policy/Oversight Team to document the process for vetting, communicating, and posting PAA guidance.

Status: **OPEN**

Target Completion Date: **2 May 2008**

(U) OIG Comment

(U) Planned action meets the intent of the recommendation.

(U) Conclusion

(U) Within a short time, NSA has made considerable progress in setting up the needed training, policies, processes, procedures, systems, and oversight to ensure compliance with the PAA. Our recommendations strengthen the planned or implemented management controls, and NSA has already taken steps to address many of our concerns. As Congress continues to debate a long-term solution to the collection gaps that exist in FISA, the controls that NSA has in place set a solid foundation that will accommodate any law that supersedes the PAA.

(U) For this review, we did not conduct a full range of compliance and substantive testing needed to draw conclusions on the efficacy of management controls. We plan to complete such testing in a follow-on review.

III. (U) SUMMARY OF RECOMMENDATIONS

(b) (3) - P.L. 86-36

(U) Recommendation 1~~(S//SI)~~ Implement [redacted] process that routinely reconciles PAA-tasked selectors [redacted]

(U) Action: SID/S332

(b) (1)

(U) Status: OPEN

(b) (3) - P.L. 86-36

(b) (3) - 50 USC 3024(i)

(U) Target Completion Date: 15 May 2008

(U) Recommendation 2~~(S//SI)~~ Implement controls to verify that target analysts routinely review intercepted data and confirm that information acquired through the use of selectors is related to the expected foreign intelligence targets.

(U) Action: SID/S2

(U) Status: OPEN

(U) Target Completion Date: 30 June 2008

(U) Recommendation 3~~(U//FOUO)~~ Develop and document rigorous methodologies for conducting [redacted] of PAA compliance.

(U) Action: SID/O&C and PPAS

(b) (3) - P.L. 86-36

(U) Status: OPEN

(U) Target Completion Date: 2 May 2008

(U) Recommendation 4~~(U//FOUO)~~ Publish and maintain a working aid that compares key requirements for SIGINT collection, processing, retention, and dissemination authorized by E.O. 12333 with requirements of other significant additional authorities, for example the PAA and FISA. In the working aid, provide links to the authorizing documents.

(U) Action: SID/O&C with D/OGC

(U) Status: OPEN

(U) Target Completion Date: 25 April 2008

(U) Recommendation 5

(U//FOUO) Implement a process to vet, communicate, and post PAA guidance until it can be incorporated into policy or SOPs.

(U) Action: SID/O&C

(U) Status: OPEN

(U) Target Completion Date: 2 May 2008

(U) ACRONYMS AND ABBREVIATIONS

AG	(U) Attorney General
DIRNSA	(U) Director, National Security Agency
DNI	(U) Director of National Intelligence
FISA	(U) Foreign Intelligence Surveillance Act
O&C	(U) Oversight & Compliance
OIG	(U) Office of the Inspector General
PAA	(U) Protect America Act
PPAS	(U) PAA Procedures and Analytic Support
OGC	(U) Office of General Counsel
SID	(U) Signals Intelligence Directorate

(U) This page intentionally left blank.

(U) APPENDIX A

(U) About the Review

(U) This page intentionally left blank

(U) ABOUT THE REVIEW

(U) Objectives

(U) The objective of this review was to assess whether management controls are adequate to provide reasonable assurance that NSA complies with the terms of the PAA. In particular, our review assessed the adequacy of controls on the three PAA requirements:

- ~~(S//SI)~~ **Foreignness.** Selectors on PAA collection must concern "persons reasonably believed to be located outside of the United States."
- ~~(S//SI)~~ **Foreign Intelligence Purpose.** A significant purpose of the collection is to obtain foreign intelligence information.
- (U) **Minimization Procedures.** NSA personnel must follow appropriate minimization procedures.

(U) Scope and Methodology

(U) The review was conducted from September 14, 2007 to November 30, 2007.

(U) We interviewed Agency personnel and reviewed documentation to satisfy the review objectives.

(U) We did not conduct a full range of compliance or substantive testing that would allow us to draw conclusions on the efficacy of management controls. Our assessment was limited to the overall adequacy of management controls.

(U) This review was conducted in accordance with generally accepted government auditing standards, as set forth by the Comptroller General of the United States and implemented by the audit manuals of the DoD and NSA/CSS Inspectors General.

(U) Prior Coverage

(U) The OIG has conducted no prior coverage of NSA's implementation of the PAA.

(U) This page intentionally left blank

(U) APPENDIX B

(U) Assessment of Management Controls

(U) This page intentionally left blank

(U) ASSESSMENT OF MANAGEMENT CONTROLS

(U) Many of the internal control requirements were established by the Affidavit of DIRNSA submitted for each Certification, Exhibit A to the Affidavit, and Exhibit B to the Affidavit. Exhibit A is common to each of the three AC/DNI certifications issued at the time of the review and establishes the procedures used to determine the foreignness of a target. Exhibit B for each affidavit contains the minimization procedures to be used for information collected under the related Certification. These procedures are unique to each Certification. In addition to the control requirements established by the affidavits and exhibits, the Standards for Internal Control in the Federal Government provides a general framework of controls that should be incorporated into daily operations.

	Control Objective	Source	Description	Assessment		
				Good	Needs Improvement	Needs Improvement
Foreignness	(U//FOUO) [redacted]	(U) Exhibit A	(U//FOUO) According to the Analyst Checklist, a tasking analyst must review tasking submitted by a target analyst for a second-level review of foreignness. If the target analyst and tasking analyst are the same person, a tasking auditor will perform the second level review.		•	
	(b) (1) (b) (3) - P.L. 86-36		(S//SI) The [redacted] reviews tasking to ensure the required information has been entered. [redacted]		•	
			(U//FOUO) The Oversight & Compliance (O&C), in coordination with the OGC, has developed mandatory training for analysts tasking under the FAA and analysts accessing information collected under the FAA.	•		
	(U//FOUO) [redacted]	(U) Exhibit A	(U//FOUO) The FAA Procedures and Analytic Support (PPAS) Team was established [redacted] to detect incidents of targets entering the United States. [redacted] has been particularly successful. [redacted] The PPAS team also [redacted] to follow up with analysts on potential violations, detain, and purge data as needed.	•		

(U) ASSESSMENT OF MANAGEMENT CONTROLS

Control Objective	Source	Description	Assessment		
			Good	Adequate	Needs Improvement
Foreignness (U//FOUO) [redacted] (b) (2) (b) (3) - P. L. 86-36	(U) Exhibit A	(U//FOUO) To meet the requirements for documenting "foreignness determinations" in Exhibit A of the DIRNSA Affidavit, [redacted] to ensure that analysts fully document "foreignness" determinations when targeting under the PAA.	•		
	(U) Exhibit A	(U//FOUO) The Analyst Checklist states that "the target analyst is required to create a permanent record of the citations associated with each target and associated selectors." [redacted] The Checklist further describes [redacted] to retain "foreignness" documentation. Procedures to retain source documents are nearing completion.		•	
	(U) Exhibit A	(U//FOUO) NSA personnel support mandated AG/DNI reviews of PAA targeting decisions. So far, AG/DNI have not formally reported any violations to NSA.		•	
	(U) Exhibit A	(U//FOUO) The AG and DNI conducted 12 independent reviews of "foreignness" determinations as mandated in Exhibit A. Initial reviews were conducted 14 days after the certification was signed, and subsequent reviews are conducted every 30 days thereafter. [redacted] the AG and DNI decided to conduct reviews every 30 days. Agency personnel track resolution of feedback and recommendations provided by the AG/DNI review teams during the reviews.	(b) (3) - P. L. 86-36	•	
(U//FOUO) [redacted]	(U) Exhibit A	(U//FOUO) O&C was checking selectors pulled for AG/DNI reviews but had no formal standard operating procedures or rigorous methodology for conducting [redacted] independent of the reviews. O&C was working to develop procedures that will complement AG/DNI reviews without being redundant. See Recommendation #3.			•
(U//FOUO) [redacted]	(U) Exhibit A	(U//FOUO) The PPAS team does limited checks for foreignness. However, the PPAS team does not have a documented methodology for conducting the [redacted]. See Recommendation #3.			•

(U) ASSESSMENT OF MANAGEMENT CONTROLS

Control Objective	Source	Description	Assessment		
			Good	Adequate	Needs Improvement
Foreign Intelligence Purpose (U//PPAS) In determining whether each of the persons targeted for collection pertained to this request purposes and is likely to communicate information of a foreign intelligence value, NSA considers certain information.	(U) INX/ISA Affidavit	(U//PPAS) The Analyst Checklist includes steps that analysts must follow to establish under which certification the target can be tasked.		•	
		(U//PPAS) Tracking tools were modified [redacted] to ensure consistency and accuracy in targeting information entered by analysts. [redacted]	•		
		(U//PPAS) Analysts must also document, in the tracking tools, the information used that a target is certified to study.			
		(U//PPAS) The Analyst Checklist requires analysts to routinely review intercepted data and confirm that tasked selectors are producing foreign intelligence from the expected targets. A SoP is planned that will provide full instructions on an analyst's review obligations. In addition to the SoP, management should develop controls to ensure analysts are conducting required reviews. See Recommendation #2.			•
		(U//PPAS) In conjunction with [redacted] of foreignness, the PPAS team does limited checks of foreign intelligence purpose. However, the PPAS team does not have a documented methodology for conducting the [redacted]. See Recommendation #3.			•
(U) Routine audits of queries of raw traffic databases are performed to validate that the queries will likely produce foreign intelligence information.			•		

(b) (3) - P.L. 86-36

(U) ASSESSMENT OF MANAGEMENT CONTROLS

Control Objective	Source	Description	Assessment			
			Good	Needs Improvement	Needs Improvement	
Minimization Procedures	(S) NSA will follow: (a) the Standard Minimization Procedures for Electronic Surveillance Conducted by the NSA (also known as Annex A to United States Signals Intelligence Directive 18), which have been adopted by the Attorney General and are on file with the Foreign Intelligence Surveillance Court (except as modified by Exhibit B to each Certification);	(U) Exhibit B	<p>(U//FOUO) Standard minimization procedures have been promulgated as (USSD SP0)8—Legal Compliance and Minimization Procedures (USSD 18), since 1993. The current version of USSD 18 supercedes a prior version issued in 1980. The policies and procedures prescribed by USSD 18 are well-established and well-known to analysts. Also, USSD CR1610 requires analysts be briefed by OOC and SID O&C on USSD 18 before obtaining access to raw SIGINT databases. CR1610 also requires USSD 18 briefings every two years in order to maintain database access.</p> <p>(U//FOUO) Although FAA training has been implemented, improvements could be made when discussing the differences between USSD 18 and the minimization procedures for each certification. A working aid for analysts would help analysts distinguish between authorities and their related minimization procedures. See Recommendation #4.</p>	•		
	(U//FOUO)	(U) Exhibit A	<p>(S//SI) The PFAS team [redacted] to detect incidents of targets entering the United States. [redacted] has been particularly successful. [redacted] The PFAS team also [redacted] to follow up with analysts on potential violations, detain, and purge data as needed.</p> <p>(b) (1) (b) (3) - P. L. 86-36</p>	•		
	(U//FOUO)	(U) Exhibit A	<p>(U//FOUO) The PFAS team and SID O&C verify compliance with reporting minimization procedures [redacted] for compliance with Certification minimization procedures performed for published reports. However, O&C has not documented procedures or a methodology for such reviews. See Recommendation #3.</p>			•

(b) (3) - P. L. 86-36

(U) ASSESSMENT OF MANAGEMENT CONTROLS

Control Objective	Source	Description	Assessment		
			Good	Adequate	Needs Improvement
(U) "Information should be recorded and communicated to management and others within the entity who need it and in a form and within a timeframe that enables them to carry out their internal control and other responsibilities."	(U) Standards for Internal Control in the Federal Government	(U//FOUO) An internal web site has been established to provide dissemination of PAA-related information to the NSA workforce. The website serves as a single point of contact for PAA-related information. From one location, analysts can access PAA SOPs, DODISA affidavits and related exhibits for each registration, archived PAA communications from NSA leadership, and PAA Help Team contact information.	•		
	(b) (3) - P.L. 86-36	(U//FOUO) NSA leadership has emphasized the importance of the PAA through various Agency-wide e-mails and presentations.	•		
	(b) (1)	(U//SI//REL TO USGAT/VER) A system to post PAA Standard Operating Procedures is in place. Sets of Standard operating procedures have been posted so far: Analyst Checklist, Incident Reporting, Training.	•		
	(b) (3) - P.L. 86-36	[redacted] In addition, a number of procedures were still in draft and various local procedures had either been formalized or were in draft.			
	(b) (3) - 50 USC 3024 (i)	(U//FOUO) Although a process is in place to promulgate SOPs, a similar process does not exist for communicating and posting interim guidance until OIG and OIG can publish more formal policy, as needed. Given the response of the PAA, more questions on applying and complying with the PAA will inevitably emerge. Answers to such questions have been communicated by e-mail to OIG; however, existing procedures had not been updated to reflect any changes. A process to post such questions and answers for future reference with electronic evaluation on the part of the analysts until SOPs are updated. See Recommendation #5.			•
		(U//FOUO) PAA SOP has been developed for incident reporting and published on the PAA website. Published SOPs enable analysts to quickly recognize reportable incidents and take appropriate action.	•		
		(U//FOUO) The PPAAS Team enables SI product lines by guiding analysts through the targeting and tracking process.	•		

Communication

(U) ASSESSMENT OF MANAGEMENT CONTROLS

Control Objective	Source	Description	Assessment		
			Good	Adquate	Needs Improvement
(U//FOUO) [redacted] (b) (1) (b) (3) - P. L.	(U) Exhibit A 86-36	(U//FOUO) O&C and OIC developed training that requires watching a video briefing from OIC, reading the certifications and related documents, and taking and passing a competency test with a score of 80% or better. (U//FOUO) O&C has made improvements to the training based on feedback from the initial course. The updated training clarifies key points for analysts and draws distinctions between PAA and other NSA authorities.	•		
		(U//FOUO) A Training SOP has been developed and published on the internal PAA website. The SOP outlines the training requirements to obtain access to PAA derived collection, as well as the process to obtain the training.	•		
(U) In terms of control monitoring should assess the quality of performance over time and ensure findings are resolved. It includes regular management and supervisory activities, such as ongoing comparisons and reconciliations, to ensure controls are functioning properly.	(U) Standards for Internal Control in the Federal Government	(S//NF) Periodic reconciliation of selections on collection is NSA systems [redacted] should be performed to detect potential over-collection or under-collection. Although collection managers prepared draft reconciliation procedures, the procedures were designed to [redacted] See Recommendation #1.		(b) (1) (b) (3) - P. L. 86-36 (b) (3) - 50 USC 3024 (f)	
		(U//FOUO) O&C currently conducts supervisory of queries to raw traffic databases for USSID 18 compliance. O&C will conduct [redacted] supervisory of queries made to PAA data partitions to ensure compliance with appropriate certifications and USSID 18. See Recommendation #1.		•	

(b) (3) - P. L. 86-36

(U) APPENDIX C

(U) Full Text of Management Comments

(U) This page intentionally left blank

~~TOP SECRET//COMINT//NOFORN~~
SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO OIG	EXREG CONTROL NUMBER 1250-08	KCC CONTROL NUMBER
THRU	ACTION <input type="checkbox"/> APPROVAL <input type="checkbox"/> SIGNATURE <input checked="" type="checkbox"/> INFORMATION	EXREG SUSPENSE
SUBJECT (U//FOUO) SID Response to OIG Draft Report on the Assessment of Management Controls to Implement the Protect America Act (PAA) of 2007 (ST-08-0001)		KCC SUSPENSE
DISTRIBUTION SID, SV, S2, S3, PPAS, OGC		ELEMENT SUSPENSE

SUMMARY

PURPOSE: (U//FOUO) To provide the SID response on the OIG Draft Report on the Assessment of Management Controls to Implement the Protect America Act (PAA) of 2007 (ST-08-0001).

BACKGROUND: (S//SI//REL) The OIG performed an assessment of the procedures established by the Director NSA (DIRNSA) to ensure NSA's adherence to three PAA requirements: that targets are located overseas, that the foreign intelligence purpose is significant, and that personnel follow applicable minimization procedures. The OIG draft report was published on 31 January 2008 and provides a complete summary of the OIG's assessment. The SIGINT Directorate (SID) was tasked to review and comment on the OIG Draft Report.

DISCUSSION: (U//FOUO) The Office of Oversight & Compliance (SV), the SID Directorate for Analysis & Production (S2), and the SID Directorate for Data Acquisition (S3) have reviewed and concurred with the recommendations in the OIG Draft Report. These organizations have responded with detailed plans of action, to include their expected target completion dates.

(b) (3) - P.L. 86-36

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
SID	M SID 7/27/08	966-7700			
SV	26 Mar 2008	966-2479			
ADDAP	11 Mar 08	963-3335			
DDDA	21 Mar 08	963-1921			
PAA Team	1/25 Mar 08	966-2044			
ORIGINATOR	SID IG Liaison		ORG. SV	PHONE (Secure) 966-2464	DATE PREPARED 17 March 2008

FORM 857B
REV NOV 06

Derived From: NSA/CSSM 1-52
Dated 6 January 2007
Declassify on: 20080408

SECURITY CLASSIFICATION

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

~~(U//FOUO)~~ **SID RESPONSE to the OIG Draft Report on the Assessment of Management Controls to Implement the Protect America Act (PAA) (ST-08-0001)**

Recommendation 1: ~~(S//SI)~~ Implement [redacted] process to routinely reconcile PAA-tracked selectors [redacted] (ACTION: Chief, S332)

(U) SID ACTION: S3/Chief, S332

(b) (1)
(b) (3) - P.L. 86-36

SID Response (March 2008): ~~(U//FOUO)~~ [redacted] (S332) concurs with the OIG Draft Report and Recommendation 1 and provides the following description of planned corrective actions and a target completion date.

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

[Large redacted block]

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

[Redacted block]

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)

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

[Large redacted block]

Derived From: NSA/CSSM 1.52
Date: 20070108
Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN~~

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

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

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)

1. [redacted]
2. [redacted]
3. [redacted]

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

~~(U//FOUO)~~ The Target Completion Date for S3 to implement [redacted] process is 15 May 2008.

(b) (1)
(b) (3) - P.L. 86-36

~~(U//FOUO)~~ SID POC(s): [redacted]
(S33243), NSTS: 963-4886.

(b) (3) - P.L. 86-36

Recommendation 2: ~~(S//SI)~~ Implement controls to verify that target analysts routinely review intercepted data and confirm that tasked selectors are producing foreign intelligence from the expected targets. (ACTION: Chief, S2)

(U) SID ACTION: DDAP (Chief, S2)

SID Response (March 2008): ~~(S//SI)~~ The Deputy Director for Analysis & Production (DDAP) will continue to work with Oversight & Compliance (SV) to formally establish the requested controls. The system currently being devised will cover both DNI and telephony. [redacted]

[redacted] The system should

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)

~~TOP SECRET//COMINT//NOFORN~~



(U) The Target Completion Date for official implementation of these procedures is 30 June 2008.

(U//FOUO) SID POC(s): [Redacted]
[Redacted] NSTS: 963-1161.

(b) (3) - P.L. 86-36

Recommendation 3: (U//FOUO) Develop and document rigorous methodologies for conducting [Redacted] of PAA compliance. (ACTION: Chief, O&C and Chief, PPAS)

SID Response (March 2008): (U//FOUO) Oversight and Compliance (SV) concurs with this recommendation .

(b) (1)

(b) (3) - P.L. 86-36

~~(S//SI//REL)~~ Oversight and Compliance (O&C) is currently documenting the methodologies and procedures for conducting [Redacted] of targeting decisions, intelligence disseminations, and queries in data repositories to ensure compliance with established procedures and in accordance with Exhibits A under the [Redacted] PAA certifications. O&C is currently conducting [Redacted] of intelligence disseminations by reviewing 100% of all reporting [Redacted]

[Redacted] In addition, O&C is conducting [Redacted] super-audits against a [Redacted] file.

(b) (3) - P.L. 86

All query terms are reviewed to ensure that there are no terms that will inherently return U.S. entity communications. These procedures will be documented. Finally, Oversight and Compliance is working with DOJ and ODNI attorneys in every review of all targeting decisions. Procedures for these reviews will also be documented. It should be noted that these procedures may change pending the passage of permanent legislation.

(U) The Target Completion Date for the documentation of the methodologies and procedures is 2 May 2008.

(U//FOUO) SID POC(s): [Redacted] Chief, [Redacted]
[Redacted] (SV2), NSTS: 963-0248; [Redacted] PPAS (S0), NSTS: 963-0363.

(b) (3) - P.L. 86-36

Recommendation 4: (U//FOUO) Issue and maintain an up-to-date working aid or quick reference that compares key elements and requirements of and links to NSA's various authorities. (ACTION: O&C with OGC)

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

(U) SID ACTION: O&C (SV)

SID Response (March 2008): SV concurs with this recommendation.

~~(TS//SI//REL)~~ Prior to receiving this recommendation, Oversight and Compliance (O&C) had already levied a requirement with ADET in October 2007 to develop an overview course of NSA's surveillance authorities. The Training Control Document for this course was completed on 1 February 2008 and includes a requirement for a job aid to fulfill this recommendation. The development of the course is well underway. Details of the course are available upon request. It should be noted that some course content may change pending the passage of permanent legislation.

(U) The Target Completion Date for the course and the job aid is 25 April 2008.

(U//FOUO) SID POC(s): [redacted] Chief [redacted]
 (SV3), NSTS: 966-887; and [redacted] FISA Technical Lead, SV09,
 NSTS: 963-8168.

(b) (3) - P.L. 86-36

Recommendation 5: (U//FOUO) Implement a process to vet, communicate, and post PAA guidance until it can be incorporated into policy or SOPs. (ACTION: O&C)

(U) SID ACTION: O&C (SV)

(b) (1)

(b) (3) - P.L. 86-36

SID Response (March 2008): SV concurs with this recommendation.

~~(S//SI//REL)~~ Immediately after the temporary PAA legislation was passed, SID established a PAA implementation team, which consisted of [redacted] sub-teams that included the following: [redacted]

[redacted] and a Legal/Policy/Oversight (LPO) team. The LPO team, led by the Chief of Oversight and Compliance (SV), has been meeting periodically since August 2007 to discuss and develop guidance related to PAA implementation. The team has promulgated [redacted] SOPs and is in the process of developing [redacted]. These SOPs are posted on both the PAA and O&C websites. In addition, members of the LPO team (which includes SID Policy, OGC, S2, and S3 members) participate in the almost daily PAA team lead sessions where additional information is discussed to include the need for further guidance. Although this recommendation is somewhat vague in terms of expected deliverables, Oversight and Compliance will work with the OIG Office, OGC, SID Policy, and the LPO team to document the process for vetting, communicating and posting PAA guidance. It should be noted that some guidance may change pending passage of permanent legislation.

(b)(3)-P.L. 86-36

(U) The Target Completion Date for documenting the process is 2 May 2008.

(U//FOUO) SID POC(s): [redacted] Chief, Oversight and Compliance (SV), NSTS: 966-2479.

(b) (3) - P.L. 86-36

~~TOP SECRET//COMINT//NOFORN~~

