~~CONFIDENTIAL//REL TO USA, FVEY~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

10 January 2014

IV-13-0069

Misuse of Government Resources

This is a PRIVILEGED DOCUMENT. Further dissemination of this report outside of the Office of Inspector General, NSA, is PROHIBITED without the approval of the Assistant Inspector General for Investigations.

~~CONFIDENTIAL//REL TO USA, FVEY~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

I. (U) SUMMARY

(b)(3) - P.L. 86-36
(b)(6)

(U//~~FOUO~~) On 22 May 2013, the NSA/CSS Office of Inspector General (OIG) received a referral from [redacted] identifying a potential data transfer violation and misuse of privileged access (PRIVAC) by [redacted] a [redacted] contractor.

(U//~~FOUO~~) The preponderance of the evidence collected during the investigation substantiated that [redacted] misused his NSA/CSS Information System (IS) on 7 May 2013 by performing an unauthorized data transfer in violation of ICS 500-18 and DNI Memorandum 2010-0610. The preponderance of the evidence also supports the conclusion that [redacted] misused his PRIVAC status [redacted] to reinstate his non-PRIVAC account, in violation of NIST Special Publication 800-53A and NSA/CSS Policy Manual 6-3, Chapter 2.

(U//~~FOUO~~) A summary memorandum will be provided to the Maryland Procurement Office and the Office of General Counsel for review and any action deemed appropriate with information copies to the NSA/CSS Senior Acquisition Executive; Contractor Clearances, ADS&CI; and Special Actions, ADS&CI.

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

(b)(6)

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

II. (U) BACKGROUND

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

(U) Introduction

(U//~~FOUO~~) [redacted] is a contractor affiliate with [redacted] assigned to [redacted] working under the [redacted] contract [redacted]. [redacted] is assigned to [redacted] and supports [redacted] as an internal system administrator.

(U//~~FOUO~~) As part of his job duties supporting [redacted] is required to act as a Data Transfer Agent (DTA) and maintain privileged access (PRIVAC). An approved DTA is an NSA/CSS trained user designated by their organization and approved by the NSA/CSS Authorizing Official (AO) or AO designee to safely transfer data and software between NSA/CSS ISs using removable media. PRIVAC is that access which is above that required for normal data acquisition or operation of U.S. government ISs, such as is required for system maintenance and operations. Individuals possessing root passwords, "super user" privileges, or similar capability to manipulate or modify data to a degree greater than that of an individual system user are considered to have privileged access.

(U//~~FOUO~~) Although his job required him to be a DTA, [redacted] was never officially approved to perform data transfers. From 2 May 2012 until 22 April 2013, [redacted] performed [redacted] data transfers without authorization. He recorded these transfers in the [redacted] data transfer tracking database [redacted]

(U//~~FOUO~~) In early 2013, in an effort to maintain greater oversight of data transfers, [redacted] began notifying users who were previously observed transferring data that they would no longer be allowed to act as a DTA unless they were officially trained and approved. As part of the authorization process, [redacted] allowed users a [redacted] grace period to obtain DTA approval following the initial notification. If a user did not complete the steps required to become a DTA by the end of the [redacted] grace period, and was subsequently detected performing a data transfer, the user's account would be disabled. Although the data transfers [redacted] accomplished from May 2012 through March 2013 were not authorized, this investigation focused on [redacted] actions after the increased oversight efforts initiated by [redacted] in early 2013.

(U//~~FOUO~~) [redacted] was observed transferring data between January and March 2013. He was notified on 27 March 2013 that he had been detected performing unauthorized data transfer activity. He was informed, via email, of the process to become an authorized DTA and was given [redacted] to complete the approval process. On 7 May 2013, [redacted] was

(b) (3) - P.L. 86-36
(b) (6)

detected performing a data transfer. Since he and his management had not completed the necessary requirements for [redacted] to become a DTA, this transfer was unauthorized. On 15 May 2013, [redacted] access to the classified network was disabled by [redacted] at the direction of [redacted] On 20 May 2013, [redacted] used his PRIVAC access (admin account) to re-enable his non-PRIVAC (personal) account.

(U) Applicable Authorities

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

(U) Intelligence Community Standard Number 500-18 (ICS 500-18), "REMOVABLE MEDIA MANAGEMENT," dated 16 February 2011.

(U) Office of the Director of National Intelligence, Assistant Director of National Intelligence and Chief Information Officer, Memorandum 2010-0610 (DNI Memorandum 2010-0610), "PROTECTION OF CLASSIFIED INFORMATION ON IC SYSTEMS," Revised Effective Date for ICS 500-18 (*Removable Media Management*) and Reinforcement of Cross-Domain Security Safeguards, dated 13 Dec 2010.

(U) National Institute of Standards and Technology (NIST) Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, dated June 2010.

(U//~~FOUO~~) NSA/CSS Policy Manual 6-3, Chapter 2, "Information System User and Supervisor Responsibilities," Annex "Separation of Duties," dated: 23 November 2009.

(U) See Appendix A for a full text of the applicable authorities.

III. (U) FINDINGS

(U//~~FOUO~~) *ALLEGATION 1: Did [redacted] perform an unauthorized data transfer on 7 May 2013, in violation of ICS 500-18 and DNI Memorandum 2010-0610?*

*(U//~~FOUO~~) **CONCLUSION**: **Substantiated.** The preponderance of the evidence supports the conclusion that [redacted] performed an unauthorized data transfer on 7 May 2013 in violation of ICS 500-18 and DNI Memorandum 2010-0610.*

(b)(3) - P.L. 86-36
(b)(6)

(U) Documentary Evidence

(U//~~FOUO~~) Despite not being designated as an approved DTA, [redacted] methodically recorded the data transfers he had performed from 2 May 2012 until 22 April 2013 in the [redacted] data transfer tracking database called the [redacted] (Appendix B). The detection of these transfers precipitated the 27 March 2013 [redacted] notification discussed below.

(U//~~FOUO~~) On 27 March 2013, [redacted] was notified via email by [redacted] that he was not authorized to transfer data (Appendix C). He was given a deadline [redacted] to become an approved DTA.

(U//~~FOUO~~) In order to become an authorized DTA, the requestor must [redacted]

On 18 April 2013, [redacted] management [redacted] forwarded a DTA User Agreement to [redacted] in order to gain DTA approval for [redacted] An immediate [redacted] reply (from [redacted] informed [redacted] that he had used an incorrect form and that he must resubmit the DTA User Agreement in order for the processing to continue. [redacted] was included as "courtesy copy" on the distribution of these messages. In an email dated 27 March 2013, [redacted] acknowledged that he could not perform DTA duties after [redacted] unless the approval process was completed (Appendix D).

(U//~~FOUO~~) On 19 April 2013, [redacted] submitted a new version of the user's agreement for the DTA approval process (Appendix E).

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

(U//~~FOUO~~) On 25 April 2013, [redacted] notified the NISIRT that the grace period deadline had passed for [redacted] to obtain DTA approval (Appendix F).

(U//~~FOUO~~) On 14 May 2013, the NISIRT notified [redacted] that [redacted] had been detected performing an unauthorized data transfer on 7 May 2013 [redacted] deadline had passed). [redacted] moved a file from a CD to NSANet (Appendix G).

(U) Testimonial Evidence

[redacted] (b) (3) - P.L. 86-36

(U//~~FOUO~~) On 4 June 2013, [redacted] was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] admitted to performing data transfers before [redacted] understood that he was given a [redacted] grace period to comply with the DTA authorization requirements. [redacted] knew that [redacted] was the grace period deadline. [redacted] initially claimed that he did not perform any data transfers after the deadline. When confronted with evidence of the 7 May 2013 transfer, [redacted] testified he did not record this transfer in the [redacted] database and claimed the transfer was completed by him under the "supervision" of the authorized DTA, [redacted] who entered the details of the data transfer in the [redacted] database. [redacted] explained that he performed the transfer as [redacted] did not have access to a folder in which the transferred material was to be placed. He was just "trying to get the job done."

(U) Analysis and Conclusions

[redacted] (b) (3) - P.L. 86-36 (b) (6)

(U//~~FOUO~~) In response to numerous incidents involving removable media on U.S. Government networks, the DNI and the DoD developed new strict controls on the usage of removable media. Recognizing that there are legitimate needs for the use of removable media, Data Transfer Agents (DTAs) are being individually authorized by the NSA/CSS Authorizing Official (AO) through the organizational Information System Security Managers (ISSM). [redacted] is responsible for managing the DTA program.

(U//~~FOUO~~) [redacted] had never been approved to perform data transfers. From 2 May 2012 until 22 April 2013, [redacted] performed [redacted] data transfers and entered the transfers in the [redacted] The [redacted] is a web-based tool available to all [redacted] employees. [redacted] database satisfies the requirement for maintaining a log of files transferred by a DTA. It also documents the approval process through the requestor's supervisor, ISSO, ISSM, CAO, and DTA. Although [redacted] was not an approved DTA when he accomplished these transfers, this inquiry is focused on unauthorized transfers [redacted] made subsequent to [redacted]

[redacted] (b) (3) - P.L. 86-36

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

(b)(3) - P.L. 86-36
(b)(6)

~~CONFIDENTIAL//REL TO USA, FVEY~~

(U//~~FOUO~~) Because he had been previously detected conducting data transfers, [redacted] was notified via a [redacted] email on 27 March 2013 that he was not authorized to transfer data until he met certain training and documentation requirements. [redacted] was given a deadline of [redacted] to complete the requirements to be designated an authorized DTA. [redacted] was informed that if after the [redacted] grace period he was not an authorized DTA and was detected performing a transfer, his account would be locked. [redacted] acknowledged his understanding of the deadline by email and during his sworn testimony.

(U//~~FOUO~~) [redacted] signed a user's agreement on 19 April 2013. Both the Chief [redacted] and ISSM had been working with [redacted] management to gain [redacted] approval as a DTA. The ISSM and Chief [redacted] were waiting for [redacted] management to complete the correct SPF to process it for approval. There is no evidence to show the correct authorization SPF was provided to the ISSM or the Chief [redacted] for approval prior to the [redacted] grace period deadline. Without the approved DTA Authorization SPF, it is unknown whether [redacted] is adhering to the constraints or restrictions as described on the DTA Authorization SPF. [redacted] never followed up with his management to see if the SPF was completed. As a result of not properly completing the required paperwork prior to the [redacted] deadline, any data transfer made by [redacted] after this date would be considered unauthorized and would result in his personal account being disabled.

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

(U//~~FOUO~~) On 14 May 2013, the NISIRT notified [redacted] that [redacted] account was detected transferring data on 7 May 2013. Because there was no record of [redacted] having been designated an authorized DTA, [redacted] personal account was disabled and a Computer Security Incident Report was generated. Despite the fact [redacted] had entered previous data transfers in [redacted] there is no record of [redacted] entering the 7 May transfer in [redacted]

(U//~~FOUO~~) In his testimony, [redacted] stated he was "just trying to get the job done" and he admitted to being well aware of the [redacted] deadline to become an approved DTA. He also acknowledged in his 27 March email that he had a "… [redacted] grace period [redacted] where I can still transfer data. After that, I will have to stop until this is rectified."

(U//~~FOUO~~) From 22 May 12 – 22 April 13, [redacted] documented [redacted] data transfers in the [redacted] database. Despite entering the previous transfers, [redacted] did not enter the 7 May transfer in the [redacted] database. [redacted] testified that he marked the [redacted] deadline on his calendar and claimed that he did not perform any data transfers after that date. After [redacted] [redacted] claimed he told users to submit the request to someone else since he was not authorized to perform data transfers.

(U//~~FOUO~~) When confronted with evidence of the 7 May 2013 transfer, [redacted] testified he did not record this transfer in the DT3 database and claimed the transfer was completed under the "supervision" of the authorized DTA who recorded the transfer in the [redacted] database. [redacted] explained that the authorized DTA did not have access to a folder in which the transferred material was to be placed; therefore, [redacted] performed the transfer. However, the transfer

~~CONFIDENTIAL//REL TO USA, FVEY~~

(b)(3) - P.L. 86-36
(b)(6)

should have been completed by an authorized DTA, and once on the system, [redacted] could have moved it to the requested location. There is no evidence that this was a mission critical request for a data transfer that required an immediate reaction by [redacted]

(U//~~FOUO~~) Despite being aware of the deadline to gain approval as an authorized DTA and not having received confirmation of the approval, [redacted] performed a data transfer on 7 May 2013.

(U//~~FOUO~~) Computer log evidence combined with [redacted] own admission supports the allegation that the data transfer he performed on 7 May 2013 was not authorized.

(b)(3) - P.L. 86-36
(b)(6)

(U//~~FOUO~~) ALLEGATION 2: ***Did [redacted] misuse his PRIVAC status to reinstate his personal account after it was disabled in violation of NIST Special Publication 800-53A and NSA/CSS Policy Manual 6-3, Chapter 2?***

(b) (6)

(U//~~FOUO~~) CONCLUSION: ***Substantiated.*** *The preponderance of the evidence supports the conclusion that [redacted] misused his PRIVAC status on [redacted] to reinstate his personal account in violation of NIST Special Publication 800-53A and NSA/CSS Policy Manual 6-3, Chapter 2.*

(b) (3) - P.L. 86-36
(b) (6)

(U) Documentary Evidence

(U//~~FOUO~~) A copy of the PRIVAC briefing is provided to all individuals who are being indoctrinated for PRIVAC (Appendix H). According to the PRIVAC Briefing, the significance of protecting the confidentiality, availability, and integrity of NSA ISs cannot be overstated. The PRIVAC duties involve privileged access to NSA/CSS ISs above the normal user to perform duties such as system maintenance and operation. Individuals with privileged access play a critical role in maintain system integrity. PRIVAC may only be used to accomplish authorized duties. Any suspected or actual abuse of the IS privileges will be reported to the appropriate organization including the ISSM.

(U//~~FOUO~~) On 20 November 2012, [redacted] renewed his PRIVAC status by reviewing the PRIVAC briefing (Appendix I).

(U//~~FOUO~~) On 15 May 2013, the [redacted] disabled [redacted] (non-PRIVAC account) access to the classified network due to detection of an unauthorized data transfer performed on 7 May 2013 (Appendix J).

(U//~~FOUO~~) On 21 May 2013, both [redacted] personal (non-PRIVAC) and system administrator (PRIVAC) accounts were disabled by the [redacted] (Appendix K).

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

(b) (3) - P.L. 86-36
(b) (6)

(U) Testimonial Evidence

(U//~~FOUO~~) On 4 June 2013, [redacted] was interviewed and provided the following sworn testimony.

(U//~~FOUO~~) [redacted] claimed that while attempting to log in to his non-PRIVAC account on 20 May 2013, he received a message that his account was "disabled" and to "contact a system administrator for assistance." Using his PRIVAC account, [redacted] logged into the authentication server and used an interface tool called [redacted] to re-enable his non-PRIVAC account. [redacted] claimed the message he received at log in was "something that he had never seen before." Being a system administrator, he logged in and

"fixed" the problem. [redacted] claimed he had no idea why his account was disabled and did not read the reason noted in the authentication server which read "Member account is disabled to due to violation of Data Transfer ..."He claimed he was "just trying to do his job." [redacted] stated that he was "tired" having just returned from vacation. He admitted that he did not pay attention as to why the account was disabled. [redacted] told the other system administrator what had happened but did not notify his management after reinstating his account. He continued to work as if nothing had happened.

(b) (3) - P.L. 86-36
(b) (6)

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

(U) Analysis and Conclusions

(U//~~FOUO~~) NIST Special Publication 800-53A states the organization separates duties of individuals as necessary, and implements separation of duties through assigned information system access authorizations. The requirement to maintain separation of duties does not allow an individual to manage their own account.

(U//~~FOUO~~) When [redacted] attempted to log on to his non-PRIVAC account on 20 May, his account was disabled. [redacted] then logged on to his PRIVAC account to log into the [redacted] to re-enable his non-PRIVAC account. Once he logged in, the description column in [redacted] noted that "*member account is disabled due to violation of the Data Transfer Authorization Policy. Member is not authorized to perform any data transfers until he/she is approved.*" [redacted] claimed that he did not see or read the reason for the account being disabled. [redacted] claimed his account had never been disabled before and he did not know why his account was disabled. He failed to recognize his actions (unauthorized data transfer) as the cause of the account being disabled. [redacted] did not inform his management of his account being disabled.

(U//~~FOUO~~) [redacted] use of his PRIVAC account to unlock his non-PRIVAC account demonstrated a lack of understanding his own responsibilities under PRIVAC. [redacted] action violated the required separation of duties by his acting as both a user and a System Administrator to manage his own accounts.

(U//~~FOUO~~) Annex to NSA/CSS Policy Manual 6-3, Chapter 2 states that segregation of duties is essential to reduce the likelihood of errors and/or wrongful acts being undetected by deliberately designing the activities of one individual to serve as a check on the activities of another. In a computerized operational environment it is necessary to enable key positions with privileged access with the recognition that this has the potential to result in mistaken or harmful actions that may quickly and seriously impact the organization. Controls consist mainly of the documentation, communication, and enforcement of procedures on group and individual responsibilities. However, the ultimate accountability rests with each system user who should know his/her responsibilities within the context of the total group responsibilities and the given controls in place.

(U//~~FOUO~~) [redacted] actions violated the NSA/CSS policy manual 6-3 when he used his PRIVAC account to unlock his non-PRIVAC account thus managing his own account. [redacted] also failed to recognize that his actions had serious impact potential when he failed to notify his management. When confronted with the evidence of the 7 May 2013 transfer, his claim that he was "trying to do his job" and "did not pay attention" demonstrated a disregard for rules in place to protect system integrity.

(U//~~FOUO~~) Forensic evidence combined with [redacted] own admission supports the allegation that he misused his PRIVAC status by failing to maintain a segregation of duties, thus compromising the integrity of the NSA/CSS IS in violation of NIST Special Publication 800-53A and NSA/CSS Policy Manual 6-3, Chapter 2.

(b)(3) - P.L. 86-36
(b)(6)

IV. (U) RESPONSE TO TENTATIVE CONCLUSION

(U//~~FOUO~~) [redacted] was provided the tentative conclusions on 2 July 2013. [redacted] responded to the tentative conclusion stating:

> I agree with the statement. I would like to say that the actions were done due to inattention to detail, and not done with the intention to disregard policy.

(U//~~FOUO~~) The conclusion of this investigation remains unchanged.

(b)(3) - P.L. 86-36
(b)(6)

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

V. (U) CONCLUSION

(b)(3) - P.L. 86-36
(b)(6)

(U//~~FOUO~~) The preponderance of the evidence supports the conclusion that [redacted] performed an unauthorized data transfer on 7 May 2013 in violation of ICS 500-18 and DNI Memorandum 2010-0610. In addition, the preponderance of the evidence supports the conclusion that [redacted] misused his PRIVAC status [redacted] to reinstate his non-PRIVAC account in violation of NIST Special Publication 800-53A and NSA/CSS Policy Manual 6-3, Chapter 2.

(b)(6)

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) A summary memorandum will be provided to the Maryland Procurement Office and the Office of General Counsel for review and any action deemed appropriate with information copies to the NSA/CSS Senior Acquisition Executive; Contractor Clearances, ADS&CI; and Special Actions, ADS&CI.

[redacted]
Senior Investigator

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

Concurred by:

[redacted]
Deputy Assistant Inspector General
For Investigations

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

Appendix A

(U) Applicable Authorities

(U) Intelligence Community Standard Number 500-18, "REMOVABLE MEDIA MANAGEMENT," dated 16 February 2011:

> 1. Authorizations. Unless otherwise noted, authorizations referenced in this Standard are authorizations provided by the Authorizing Official (AOs), or these designated by the AOs to provide such authorizations.
>
> > a. All removable media, and uses thereof, must be authorized prior to use.
> >
> > ...
>
> 3. Removable Media Use:
>
> > b. Removable media may only be connected to another information resource when specifically authorized.
> >
> > ...
> >
> > e. IC element user must sign an IC element user agreement prior to using, handling, or managing removable media activities.
>
> 4. Removable Media Accountability:
>
> > a. Classified removable media must be accounted for (i.e. registered, tracked, distributed, decommissioned) by the AO or AO designee responsible for the removable media. Such accountability should be automated to the maximum extent practicable.
>
> ...
>
> 9. Training: Users must undergo initial and annual training regarding the requirements of this Standard.
>
> ....

(U//~~FOUO~~) Office of the Director of National Intelligence, Assistant Director of National Intelligence and Chief Information Officer, Memorandum 2010-0610, "PROTECTION OF CLASSIFIED INFORMATION ON IC SYSTEMS," Revised Effective Date for ICS 500-18 (*Removable Media Management*) and Reinforcement of Cross-Domain Security Safeguards, dated 13 Dec 2010:

> Only when the use of Cross Domain Solutions is impractical and data transfer is critical to mission success will IC element Authorizing Officials (AOs), or their designees,

approve the use of removable media in accordance with Intelligence Community Standard 500-18. In those very limited circumstances, manual data transfers will be performed only by trained users specifically authorized by AOs and employing properly scanned, protected media.

(U) National Institute of Standards and Technology (NIST) Special Publication 800-53A Revision, "GUIDE FOR ASSESSING THE SECURITY CONTROLS IN FEDERAL INFORMATION SYSTEMS AND ORGANIZATION," dated June 2010:

AC-5. Separation of Duties.

AC-5.1 Assessment objective: Determine if:

(i) the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;

(ii) the organization documents separation of duties; and

(iii) the organization implements separation of duties through assigned information system access authorizations.

(U//~~FOUO~~) NSA/CSS Policy Manual 6-3, Chapter 2, "NFORMATION SYSTEM USER AND SUPERVISOR RESPONSIBILITIES," Annex "Segregation of Duties," dated: 23 November 2009

(U) Federal internal control standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated. In other words, no one individual should control all critical stages of an organizational process. This concept is labeled segregation of duties and is essential to reducing the likelihood of errors and/or wrongful acts being undetected by deliberately designing the activities of one group or individual to serve as a check on the activities of another. It is especially important in computerized operational environments where it is indeed necessary to enable key positions with privileged access but also to recognize this has the potential to result in mistaken/harmful actions that may quickly and seriously impact the organization.

(b)(3) - P.L. 86-36
(b)(6)

Appendix B

(U) [redacted] record of transfers performed by [redacted]

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

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

(b)(3) - P.L. 86-36
(b)(6)

IV-13-0069

Official transfers by [redacted] entered in the [redacted]

Request # **Create Date**

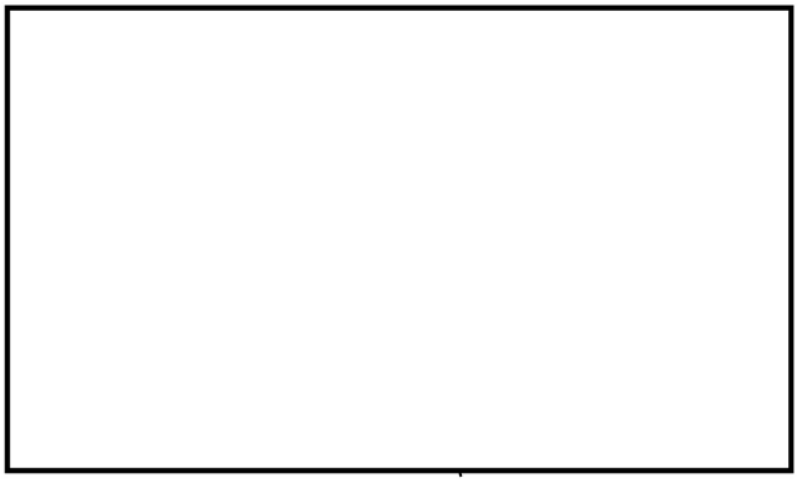
(b)(3) - P.L. 86-36

[redacted]

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

~~CONFIDENTIAL//REL TO USA, FVEY~~



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

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

Appendix C

(U) Email notification to [redacted] regarding unauthorized data transfers

[redacted]
(b)(3) - P.L. 86-36
(b)(6)

~~CONFIDENTIAL//REL TO USA, FVEY~~

IV-13-0069

(b)(3) - P.L. 86-36
(b)(6)

From: [redacted]
Sent: Wednesday, March 27, 2013 9:38 AM
To: [redacted]
Cc: [redacted]
Subject: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity
Importance: High

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

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U//~~FOUO~~) You have been identified as having performed an Unauthorized Data Transfer within the last three months.

(U//~~FOUO~~) In response to numerous incidents involving removable media on U.S. Government networks, DNI and DoD are requiring more restrictive controls on all usage of removable media. Recognizing that there are legitimate needs for the use of removable media, Data Transfer Agents (DTA) are being individually authorized by the NSA/CSS Authorizing Official (AO) through the organizational Information System Security Managers (ISSM).

(U//~~FOUO~~) The Associate Director of Technology for Information Security (TS) recognizes that mission could be impacted by an immediate denial of this capability. Therefore, we will be providing a [redacted] grace period beginning 27 Mar 2013 and ending [redacted] During this time, those not authorized to perform data transfers will need to submit a request to receive designation as an authorized DTA (via the DTA website by typing 'go DTA' in your NSANet browser). After [redacted] any unauthorized transfers by personnel that have not at least submitted a DTA request via the DTA website (with a status of PENDING in the ticket queue) will result in the immediate suspension of the user account, and a Computer Security Incident Report will be generated.

(U//~~FOUO~~) If your organization has the need for using removable media or a mission essential file transfer between networks that cannot be facilitated by an existing cross-domain solution, you can begin the process of becoming a DTA by visiting DTA Website at 'go DTA' or [redacted]

(U//~~FOUO~~) For any questions or concerns, please feel free to contact [redacted] Thank you.

Your message
To: [redacted]
Cc: [redacted]
Subject: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity
Sent: 3/27/2013 9:38 AM

was read on 3/27/2013 10:41 AM.

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

Appendix D

(U) Email communication between [redacted] and [redacted] management

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

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

From:
Sent: Thursday, April 18, 2013 2:04 PM
To:
Cc:
Subject: RE: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Anytime

(U//~~FOUO~~)

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

To find your

Subject to Privacy Information

Policy 6/33- **USER IDENTIFICATION ON THE NSA/CSS CLASSIFIED NETWORK is required. ALL users must have a signature block on ALL e-mails including replies.**
Policy 6-33 can be found at

(b) (3) - P.L. 86-36
(b) (6)

Reminder
Make sure you complete the OIAC1180 course via VUPORT. It is your responsibility!!

From:
Sent: Thursday, April 18, 2013 2:02 PM
To:
Cc:
Subject: RE: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

~~CONFIDENTIAL//REL TO USA, FVEY~~

[redacted]

Roger that! [redacted] and [redacted] will fill these out and get them to you.

Thanks so much for your help!

(U//~~FOUO~~)

[redacted]

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

*** Where's [redacted] now??? ***

From: [redacted]
Sent: Thursday, April 18, 2013 1:47 PM
To: [redacted]
Cc: [redacted]
Subject: RE: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

[redacted]

I recalled the previous message.

(b)(3) - P.L. 86-36
(b)(6)

Attached is the DTA UAF that must be used.

I am forwarding the SPF's to the ISSM for his review.

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

(U//~~FOUO~~)

[redacted]

To find your [redacted]

Subject to Privacy Information

Policy 6/33- **USER IDENTIFICATION ON THE NSA/CSS CLASSIFIED NETWORK is required. ALL users must have a signature block on ALL e-mails including replies.**
Policy 6-33 can be found at

[redacted]

****Reminder****
Make sure you complete the OIAC1180 course via VUPORT. It is your responsibility!!

From: [redacted]
Sent: Thursday, April 18, 2013 1:45 PM
To: [redacted]
Cc: [redacted]
Subject: RE: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity

Classification: UNCLASSIFIED/~~/FOR OFFICIAL USE ONLY~~

[redacted] (b)(3) - P.L. 86-36 (b)(6)

[redacted] (b)(3) - P.L. 86-36

I am sorry but the forms are not the correct ones to use. I am attaching the correct form. Additionally, an SPF needs to be completed. I have attached that form as well. I recommend you work with your ISSM, [redacted] to get these forms completed.

Thank you,

[redacted]

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

IV-13-0069

(U//~~FOUO~~)

[redacted]

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

To find your [redacted]

Subject to Privacy Information

Policy 6/33- **USER IDENTIFICATION ON THE NSA/CSS CLASSIFIED NETWORK is required. ALL users must have a signature block on ALL e-mails including replies.**
Policy 6-33 can be found at [redacted]

Reminder
Make sure you complete the OIAC1180 course via VUPORT. It is your responsibility!!

From: [redacted]
Sent: Thursday, April 18, 2013 1:43 PM
To: [redacted]
Cc: [redacted]
Subject: FW: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity
Importance: High

(b)(3) - P.L. 86-36
(b)(6)

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

To Whom It May Concern;

Good afternoon! Attached are the DTA User Agreements for both [redacted] System Administrators [redacted] in order for them to continue processing data transfer requests.

Please alert either [redacted] or myself if more information is needed in order to complete this action.

Thanks!

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

(U//~~FOUO~~)

[redacted]

(b)(3) - P.L. 86-36
(b)(6)

> Where's [redacted] now??? <

From: [redacted]
Sent: Wednesday, March 27, 2013 12:41 PM
To: [redacted]
Cc: [redacted]
Subject: FW: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity
Importance: High

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

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

All,

I spoke to [redacted] about the email he sent me saying that I had performed an Unauthorized Data Transfer. He said that neither [redacted] nor myself are authorized to perform data transfers, as they do not have Staff Processing Forms (SPFs) listing either of us. Since we belong to [redacted] but support [redacted] I'm not sure who the best person would be to submit a ticket (off of the 'go dta' site) to request authorization for [redacted] and I to transfer data. As the email points out, I've got a [redacted] grace period ending [redacted] where I can still transfer data. After that, I will have to stop until this is rectified.

Regards,

(U//~~FOUO~~) [redacted]

[redacted]

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

[redacted]

(b)(3) - P.L. 86-36
(b)(6)

From: [redacted]
Sent: Wednesday, March 27, 2013 9:38 AM
To: [redacted]
Cc: [redacted]
Subject: (U//~~FOUO~~) Notification of Unauthorized Data Transfer Activity
Importance: High

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

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U//~~FOUO~~) You have been identified as having performed an Unauthorized Data Transfer within the last three months.

(U//~~FOUO~~) In response to numerous incidents involving removable media on U.S. Government networks, DNI and DoD are requiring more restrictive controls on all usage of removable media. Recognizing that there are legitimate needs for the use of removable media, Data Transfer Agents (DTA) are being individually authorized by the NSA/CSS Authorizing Official (AO) through the organizational Information System Security Managers (ISSM).

(U//~~FOUO~~) The Associate Director of Technology for Information Security (TS) recognizes that mission could be impacted by an immediate denial of this capability. Therefore, we will be providing a [redacted] grace period beginning 27 Mar 2013 and ending [redacted] During this time, those not authorized to perform data transfers will need to submit a request to receive designation as an authorized DTA (via the DTA website by typing 'go DTA' in your NSANet browser). After [redacted] any unauthorized transfers by personnel that have not at least submitted a DTA request via the DTA website (with a status of PENDING in the ticket queue) will result in the immediate suspension of the user account, and a Computer Security Incident Report will be generated.

(U//~~FOUO~~) If your organization has the need for using removable media or a mission essential file transfer between networks that cannot be facilitated by an existing cross-domain solution, you can begin the process of becoming a DTA by visiting DTA Website at 'go DTA' or [redacted]

(U//~~FOUO~~) For any questions or concerns, please feel free to contact [redacted] Thank you.

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

(U//~~FOUO~~)

[redacted] ------ (b)(3) - P.L. 86-36

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

Appendix E

(U) Email containing [redacted] signed user's agreement dated 19 April 2013

(b)(3) - P.L. 86-36
(b)(6)

~~CONFIDENTIAL//REL TO USA, FVEY~~

~~CONFIDENTIAL//REL TO USA, FVEY~~

IV-13-0069

(b)(3) - P.L. 86-36
(b)(6)

From:
Sent: Friday, April 19, 2013 7:36 AM
To:
Cc:

Subject: (U) DTA User Agreement for

Classification: UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Here is the signed User Agreement.

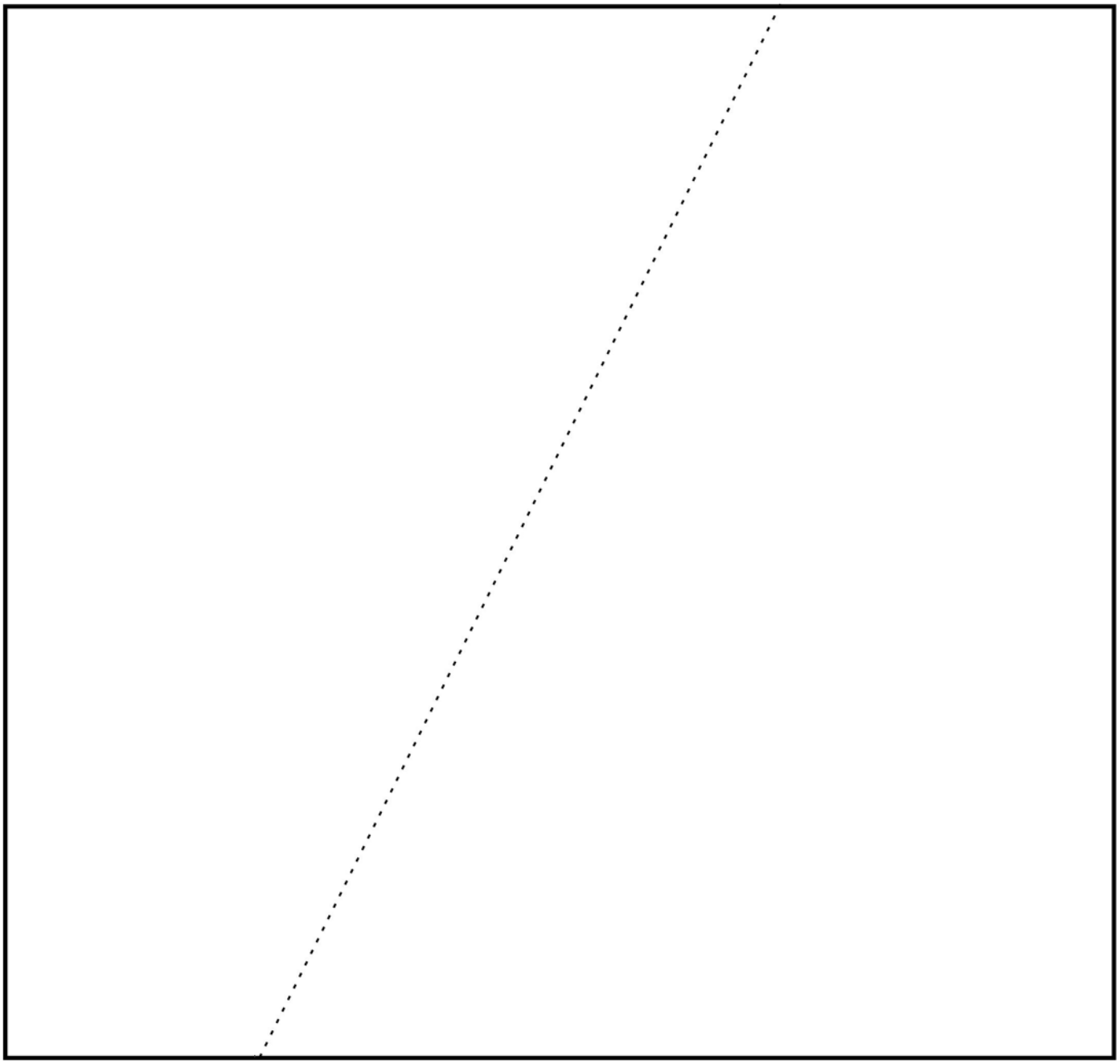
(b)(3) - P.L. 86-36

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

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

IV-13-0069



Full Name:

Organization:

Signature:

(b)(3) - P.L. 86-36
(b)(6)

Appendix F

(U) [redacted] notifying NISIRT of deadline passed

[redacted] (b)(3) - P.L. 86-36

~~CONFIDENTIAL//REL TO USA, FVEY~~

IV-13-0069

From:
Sent:
To:
Cc:

Subject: (U//~~FOUO~~) Unauthorized Data Transfer Notification Deadline Passed
Importance: High

Classification: ~~CONFIDENTIAL//REL TO USA, FVEY~~

All - (b) (3) - P.L. 86-36
(b) (6)

~~(C//REL)~~ The following SIDs have passed the deadline set of for obtaining approval for Data Transfer Agent:

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

Other SIDs removed

~~(C//REL)~~ If SIDs are observer transferring any data from now until they are officially authorized, please submit a CSIR and disable their account on the network the removable media was connected to.

~~(C//REL)~~ Please advise the following: Member account is disabled due to violation of the Data Transfer Authorization Policy. Member is not authorized to perform any Data Transfer until he/she is approved by the AO / AO Representative. To Re-Enable members account, members supervisor must contact either the during normal working hours or the SHO. Supervisor will be informed of the Member's violation and be instructed that the member is not authorized to perform Data Transfer until approved. Supervisor will also be informed that a secondary violation will be submitted to the IG with an account disable and only the IG will authorize re-enablement of the account. Supervisor must send an email with information regarding the members understanding of the policy to the ISSM and/or SHO for account re-enable.

(U//~~FOUO~~) Any questions or concerns please feel free to ask.

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

Appendix G

(U) Notification from NISIRT to [redacted]

[redacted] (b)(3) - P.L. 86-36

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

IV-13-0069

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

From:
Sent: Tuesday, May 14, 2013 10:49 AM
To:
Subject: RE: (U//~~FOUO~~) Unauthorized Data Transfer Notification Deadline Passed

Classification: ~~CONFIDENTIAL//REL TO USA, FVEY~~

Just wanted to let you know that moved 1 file off a CD on 5/7/2013, the file was This move took place on the TS network.

(b) (3) - P.L. 86-36
(b) (6)

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

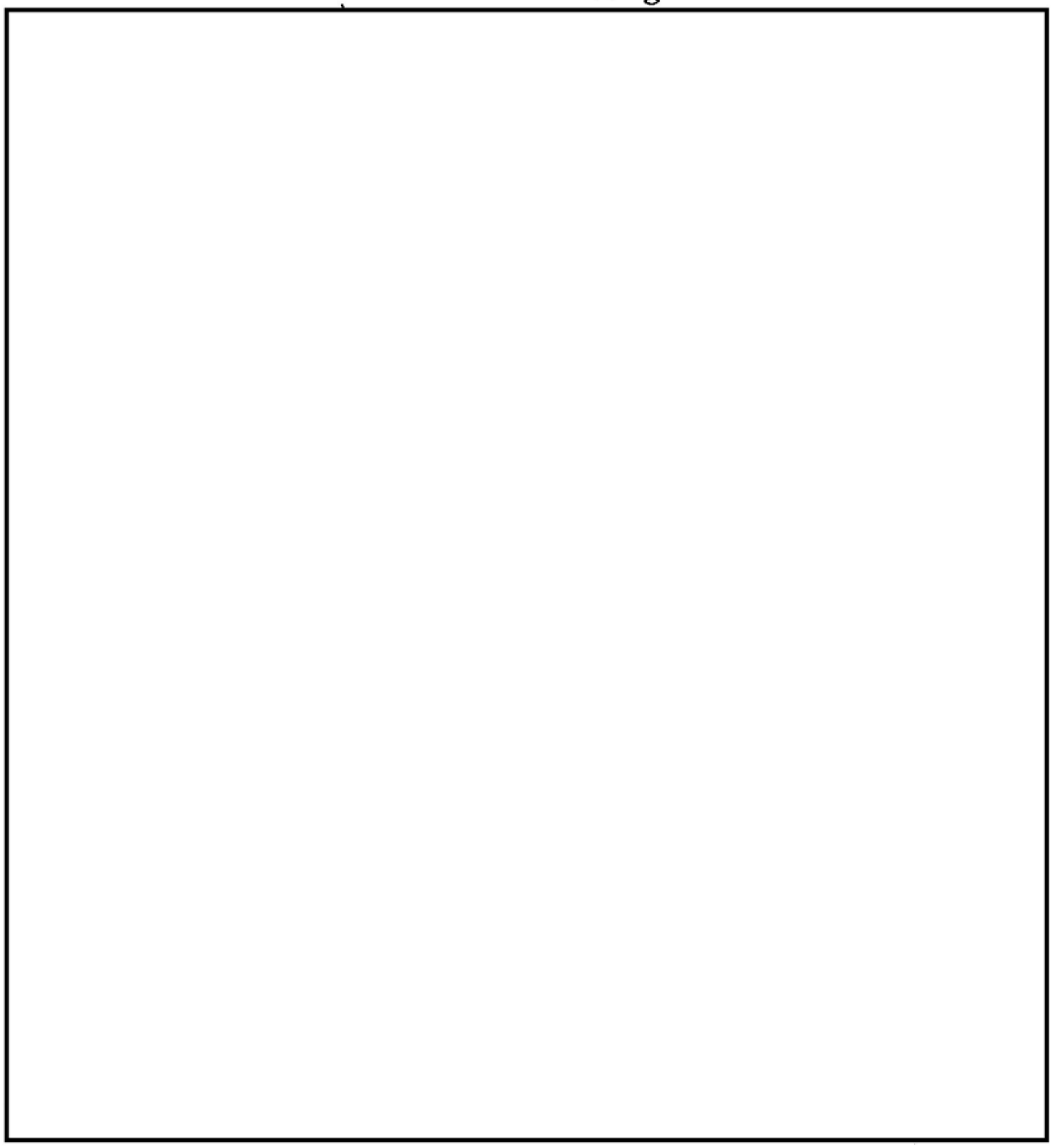
~~CONFIDENTIAL//REL TO USA, FVEY~~

Appendix H

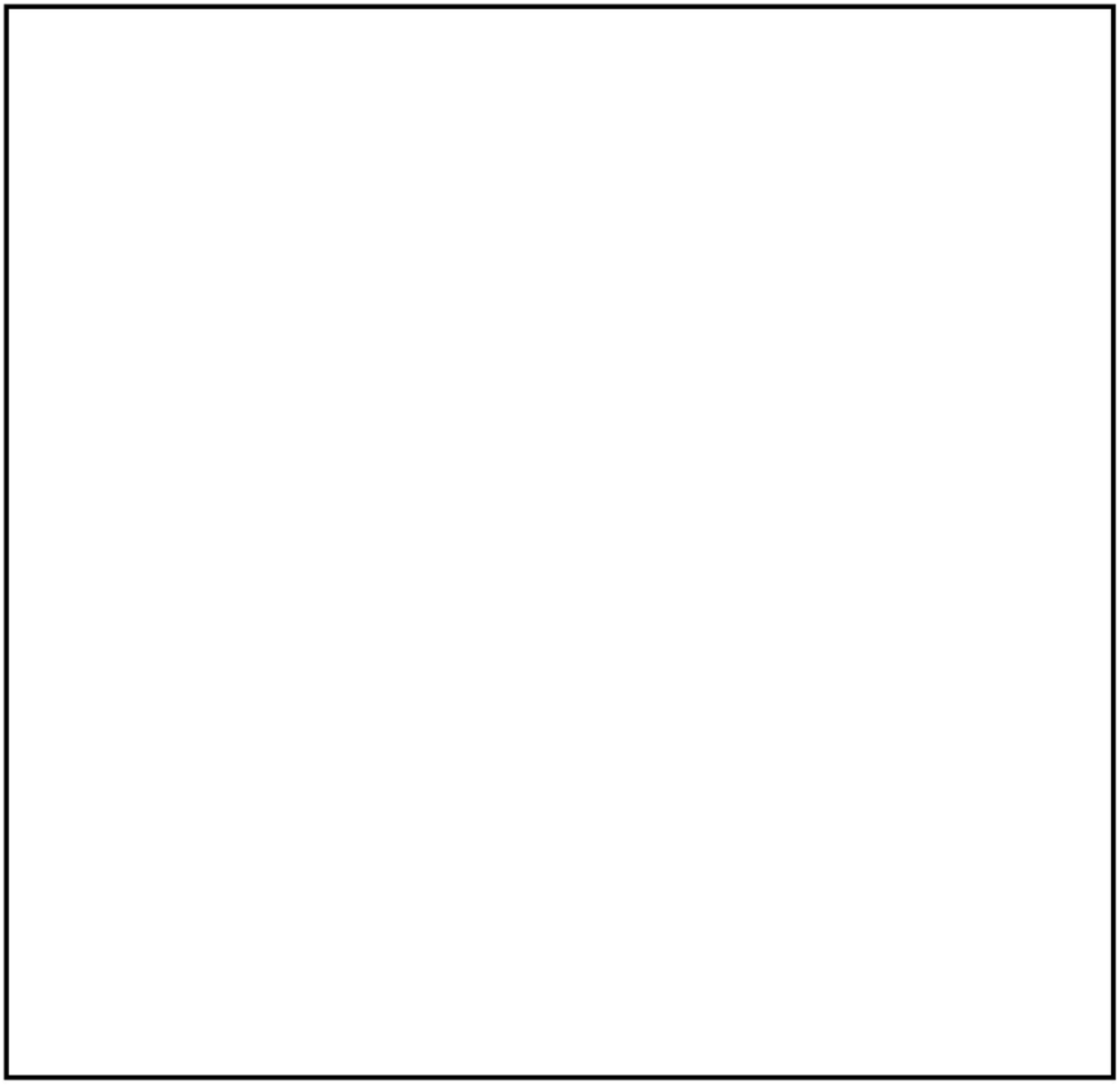
(U) PRIVAC Briefing

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

PRIVAC Briefing



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

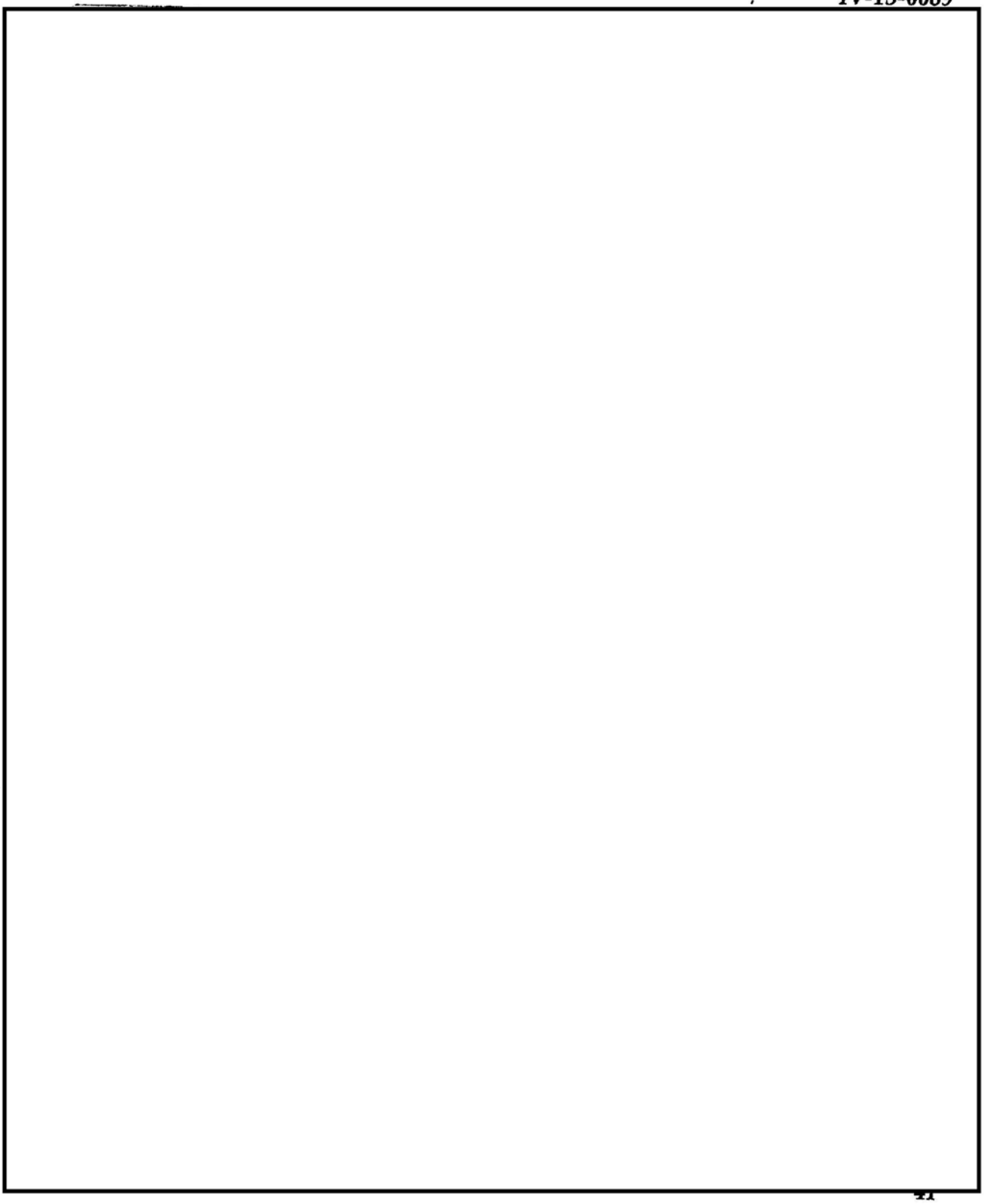


Appendix I

(U) PRIVAC renewal documentation

(b)(3) - P.L. 86-36
(b)(6)

IV-13-0069



(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

Appendix J

(U) Email request to disable [redacted] account and confirmation the account was disabled

(b)(3) - P.L. 86-36
(b)(6)

~~CONFIDENTIAL//REL TO USA, FVEY~~

From: [redacted]
Sent: Wednesday, May 15, 2013 7:25 AM
To: [redacted] IT Service Desk
Cc: SHO; [redacted]
Subject: (U//~~FOUO~~) CSIR Report [redacted] Unauthorize Data Transfer Activity Violation
Importance: High

Classification: ~~CONFIDENTIAL//REL TO USA, FVEY~~

IT Service Desk

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

Please Disable User's NSANet Account SID: [redacted]

Please ensure the following INFO is tagged to it:

Member account is disabled due to violation of the Data Transfer Authorization Policy. Member is not authorized to perform any Data Transfer until he/she is approved by the AO / AO Representative. To Re-Enable members account, members supervisor must contact either the [redacted] during normal working hours or the SHO. Supervisor will be informed of the Member's violation and be instructed that the member is not authorized to perform Data Transfer until approved. Supervisor will also be informed that a secondary violation will be submitted to the IG with an account disable and only the IG will authorize re-enablement of the account. Supervisor must send an email with information regarding the members understanding of the policy to the ISSM and/or SHO for account re-enable.

From [redacted] IT Service Desk
Sent: Wednesday, May 15, 2013 7:40 AM
To: [redacted]
Cc: SHO
Subject: RE: (U//~~FOUO~~) CSIR Report [redacted] Unauthorize Data Transfer Activity Violation
Importance: High

Classification: ~~CONFIDENTIAL//REL TO USA, FVEY~~

(b)(3) - P.L. 86-36
(b)(6)

Hi [redacted]

Per our phone conversation and the email below, the account for [redacted] has been disabled and tagged with the following message; "Member account is disabled due to violation of the Data Transfer Authorization Policy. Member is not authorized to perform any Data Transfer until he/she is approved by the AO / AO Representative. To

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

Re-Enable members account, members supervisor must contact either the [redacted] during normal working hours or the SHO". This work was performed under Ticket [redacted]

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

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

Appendix K

(U) Email notification that [redacted] account was re-enabled

(b)(3) - P.L. 86-36
(b)(6)

~~CONFIDENTIAL//REL TO USA, FVEY~~

From: [redacted]
Sent: Tuesday, May 21, 2013 10:44 AM
To: [redacted]
Cc:
Subject: RE: (U//~~FOUO~~) CSIR [redacted]

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

Classification: ~~CONFIDENTIAL//REL TO USA, FVEY~~

Looks like he enabled his own user account via his admin account using [redacted]

[redacted]

(b)(3) - P.L. 86-36
(b)(6)

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~

Appendix L

(U) Email Confirmation that both [redacted] accounts were disabled

(b)(3) - P.L. 86-36
(b)(6)

~~CONFIDENTIAL//REL TO USA, FVEY~~

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

From: [redacted]
Sent: Tuesday, May 21, 2013 11:05 AM
To: [redacted]
Cc: [redacted]
Subject: RE: (U//~~FOUO~~) CSIR [redacted]

Classification: ~~CONFIDENTIAL//REL TO USA, FVEY~~

(b)(3) - P.L. 86-36
(b)(6)

Confirmed...

[redacted]

(U) This Report of Investigation may be declassified and marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of attachment(s)

~~CONFIDENTIAL//REL TO USA, FVEY~~