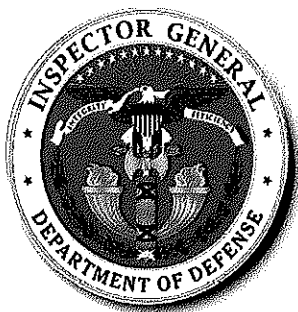


~~TOP SECRET//COMINT//NOFORN~~

Inspector General

United States Department of Defense



Report No. 11-INTEL-10
May 9, 2011

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

U.S. Cyber Command Authorities Pertaining to Use of National Security Agency Personnel (U)

Special Warning

~~This document contains information exempt from mandatory disclosure under the Freedom of Information Act. This report contains certain unclassified information relating to the organization and function of the National Security Agency that may be protected by the National Security Act of 1959, as amended (50 United States Code § 402 (note)). Reproduction or removal of pages is prohibited. Safeguards must be taken to prevent publication or improper disclosure of the information in this report.~~

Derived from: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360501

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



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

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

May 9, 2011

MEMORANDUM FOR COMMANDER, UNITED STATES STRATEGIC
COMMAND
COMMANDER, UNITED STATES CYBER COMMAND
DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF
CENTRAL SECURITY SERVICE

SUBJECT: (U) U. S. Cyber Command Authorities Pertaining to Use of National
Security Agency Personnel (Report No. 11-INTEL-10).

(U) We are providing this report for your information and use. We did not substantiate allegations of non-compliance with Title 10 and Title 50 authorities or mis-application of appropriated funds relative to the use of Title 10 and Title 50 employees.

(U//FOUO) Background: On March 10, 2010, a National Security Agency (NSA)¹ employee contacted the DoD Office of the Inspector General Hotline with a complaint about the stand-up of United States Cyber Command (USCYBERCOM). The complainant alleged that the Director, NSA (DIRNSA) was inappropriately (and likely illegally) merging organizational lines and titled legal authorities, specifically, U.S. Code Title 10, Armed Forces, and U.S. Code Title 50, War and National Defense (hereafter referred to as Title 10 and Title 50). In subsequent meetings and correspondence, the complainant clarified his concerns. The complainant enumerated the issues as follows:

1. (U) NSA personnel are conducting and directing USCYBERCOM Title 10 mission without the appropriate authority.
2. (U) The DIRNSA is inappropriately delegating signals intelligence (SIGINT) authorities to USCYBERCOM personnel.
3. (U) NSA personnel who are paid for out of NSA funding lines set aside exclusively for the cryptologic mission are not being employed for this purpose.

(U) In 2005, the DIRNSA was dual-hatted as Commander, Joint Functional Component Command for Network Warfare. In 2008, the Commander, Joint Functional Component Command for Network Warfare assumed control of Joint Task Force Global Network Operations. In 2009, the Secretary of Defense directed the creation of USCYBERCOM. USCYBERCOM is composed of the components previously created by the DoD to ensure and develop the U.S. military's ability to operate effectively in the cyberspace

¹ (U) NSA is used interchangeably with NSA/CSS (National Security Agency/ Central Security Service) throughout this document.

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360501

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

domain, including the Joint Functional Component Command for Network Warfare, subordinate to United States Strategic Command (USSTRATCOM), and the Joint Task Force Global Network Operations. On May 7, 2010, the DIRNSA was confirmed as Commander of USCYBERCOM, serving as both Director of the NSA and Commander of USCYBERCOM. USCYBERCOM subsequently assumed the responsibilities of the combined staffs of Joint Functional Component Command for Network Warfare and Joint Task Force Global Network Operations. USCYBERCOM attained initial operational capability on May 21, 2010 and full operational capability on October 31, 2010. USCYBERCOM, a sub-unified command under USSTRATCOM, operates under Title 10 authorities; to ensure and develop the U.S. Military's ability to operate effectively within cyberspace.

(U) Title 10, Armed Forces, provides the legal basis for the roles, missions and organizations of each of the three services and organizations and components within the U.S. Department of Defense. Title 50, War and National Defense, provides for a comprehensive program for the future security of the U.S.; and the establishment of integrated policies and procedures for the departments, agencies, and functions of the U.S. Government relating to national security. NSA signals intelligence activities are authorized under Executive Order 12333, as amended, commonly referred to as "Title 50" foreign intelligence authorities. NSA does not have Title 10 authorities for the conduct of military operations, specifically NSA: (b)(3) (Public Law 86-36). However, NSA does have Information Assurance Title 10 authorities (10 USC 2224) that apply to its monitoring of DoD network traffic.

~~(U//FOUO)~~ **Objective:** To determine if it was lawful and in accordance with policy for NSA personnel to conduct Title 10 activities in support of USCYBERCOM, for the DIRNSA to delegate SIGINT authority to USCYBERCOM, and for NSA personnel funded by cryptologic appropriations to support USCYBERCOM activities.

~~(U//FOUO)~~ **Scope/Methodology:** We waited to commence our review until USCYBERCOM was at full operational capacity on October 31, 2010. We reviewed information related to USCYBERCOM (and Joint Functional Component Command for Network Warfare) operations dated from May 2007 to November 2010. After interviewing the complainant, we took a macro-level approach and explored the overarching issues of the allegations. We requested information from the DIRNSA and Commander, USCYBERCOM that related to the complaint. We then considered that information in concert with our own analysis of federal statutes and national and DoD policies. We did not conduct an in-depth audit or evaluation of the implementation of the related policies or controls. We did, however, identify management controls that may warrant future review in Appendix A.

(U) RESULTS:

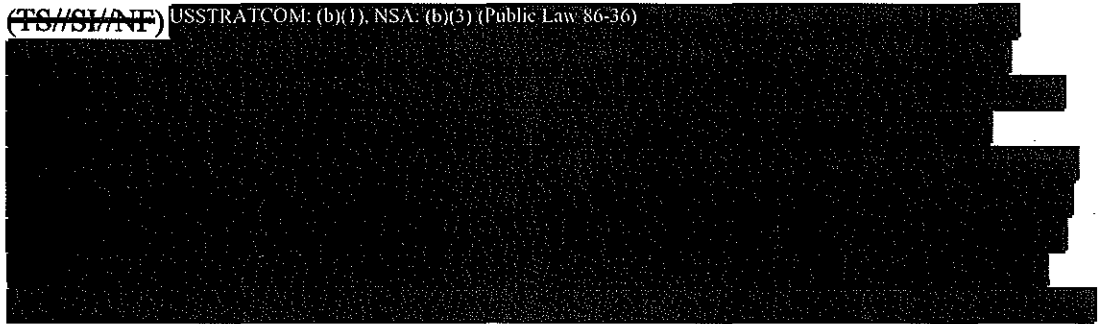
~~(TS//SI//NF)~~ Conduct of Title 10 NSA: (b)(3) (Public Law 86-36) We did not substantiate the allegation that NSA personnel are conducting and directing USCYBERCOM Title 10 mission without the appropriate authority. NSA personnel did conduct U.S. Code Title 10 operations NSA: (b)(3) (Public Law 86-36) However, those individuals were operating under the legitimate authority of USCYBERCOM (and predecessor organizations) at the time of those operations.

(U//~~FOUO~~) While NSA does not have Title 10 authority for the conduct of military operations, NSA: (b)(3) (Public Law authorities, USCYBERCOM does have that authority and was authorized to use NSA personnel to execute its mission. When NSA personnel are integrated into USCYBERCOM, they operate under the direction, supervision, and authorities of USCYBERCOM, subject to any special restrictions or agreement negotiated between NSA and USCYBERCOM.

(U//~~FOUO~~) Those special restrictions are spelled out in the "Memorandum of Understanding Between NSA and USSTRATCOM Regarding Support to USCYBERCOM," August 9, 2010 (hereafter referred to as the MOU). The MOU provides for NSA employees to be "integrated" into USCYBERCOM and perform USCYBERCOM tasks and mission. In accordance with the MOU, operational control for the NSA intees will be transferred to Commander, USCYBERCOM while assigned to USCYBERCOM.

(U//~~FOUO~~) The MOU complies with DoD Instruction 4000.19 "Interservice and Intra-governmental Support," August 9, 1995. According to DoDI 4000.19, DoD can provide requested support to other DoD activities when the head of the requesting activity determines it would be in the best interest of the U.S. Government and the head of the supplying activity determines capabilities exist to provide the support without jeopardizing assigned missions. These determinations are signified by signing a support agreement(s). No further written determinations are required for agreements between DoD activities. On August 1, 2010, an Interservice Support Agreement (ISA) between the NSA and USSTRATCOM was signed.

~~(TS//SI//NF)~~ USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)



USSTRATCOM: (b)(1)

~~(S//REL TO USA, ACGU)~~ USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)
USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)

~~(TS//SI//NF)~~ USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)
USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)

~~(S)~~ USSTRATCOM: (b)(1)

~~(U//FOUO)~~ **Delegation of SIGINT Authority.** We did not substantiate the allegation that the DIRNSA inappropriately delegated SIGINT authorities to USCYBERCOM personnel. General Alexander did delegate SIGINT authority to designated USCYBERCOM positions; however, that delegation was appropriate and lawful.

(U) Pursuant to Section 1.7(c)(2) of Executive Order 12333, as amended, no other department or agency, other than NSA, may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director of National Intelligence. On August 8, 2002, the Secretary of Defense updated a March 23, 1978 memorandum to delegate his signals intelligence *delegation* authority to the DIRNSA subject only to the following limitations: (1) the authority may not be delegated further; and (2) actions taken pursuant to this authority shall be summarized

² ~~(S//REL TO USA, ACGU)~~ USSTRATCOM: (b)(1)

periodically and reported to the Secretary of Defense. DoD Directive 5100.20, January 26, 2010 "National Security Agency/Central Security Service" codifies the authority of the DIRNSA to delegate the authority to conduct SIGINT activities.

(S//REL TO USA, ACCU) USSTRATCOM: (b)(1)
USSTRATCOM: (b)(1)



(U//~~FOUO~~) In a January 27, 2010 memorandum, the DIRNSA coordinated his intent to delegate SIGINT authority to certain members of Joint Functional Component Command for Network Warfare (now USCYBERCOM) with the Director of National Intelligence. The Director of National Intelligence agreed with this plan on March 5, 2010.

(U//~~FOUO~~) **NSA Funding in Support of USCYBERCOM.** We did not substantiate the allegation that NSA personnel who are paid out of NSA funding lines set aside exclusively for the cryptologic mission are not being employed for this purpose. While NSA: (b)(3) (Public Law 86-36) NSA and USCYBERCOM have developed policies and procedures to account for the costs associated with that support. Those policies delineate the circumstances in which the support supplier will be reimbursed. We did not independently verify the accuracy of those accounting mechanisms.

(U) DoD Instruction 4000.19 allows DoD activities to request support from other DoD activities when in-house capabilities do not exist or when support can be obtained more efficiently or effectively from other existing DoD capabilities. Policy further states that broad areas of recurring interservice support and cooperation that do not require reimbursement should be documented with a MOU.

(U) Recurring support that requires reimbursement shall be documented in a support agreement. Support is reimbursable to the extent that provision of the specified support to a receiver increases the support supplier's direct costs and that cost is measurable and attributable to the support receiver. Support services that are operated for the supplier's benefit and that also benefit other activities without increasing the cost to the supplier is not reimbursable. Civilian Personnel Services to include recruitment, classification, staffing, pay administration, personnel management, employee relations, awards, equal opportunity programs, and career development is customarily a reimbursable expense.

(U//~~FOUO~~) On August 1, 2010, the Interservice Support Agreement (ISA) between the NSA and USSTRATCOM was signed detailing the reimbursable support requirements, procedures, and costs associated with the establishment and operation of

USCYBERCOM. The ISA covers some, but not all ad-hoc or non-recurring reimbursable requirements.

(U//~~FOUO~~) The ISA shows reimbursable support services in seven primary categories:

- Deployment and Temporary Duty Support
- Business Management Integration Services (e.g. contracting support)
- Facilities and Logistics Support
- Information Systems Support
- Manpower/Personnel Support
- Personnel Security/Physical Security/Counterintelligence Support
- Strategic Communication Support (e.g. web, speech writing, multimedia, and public outreach assistance)

(U//~~FOUO~~) According to the response to our inquiry, NSA's Resources Management Organization monitors these support services and submits monthly reports to USCYBERCOM on expenses incurred by NSA. In addition, on May 21, 2010, NSA issued standard operating procedures for implementation of the ISA between USSTRATCOM and NSA. Those procedures provide further delineation of activities under the general provisions of the ISA.

(U//~~FOUO~~) In accordance with DoDI 4000.19, the August 9, 2010 MOU between the NSA and USSTRATCOM outlined mutual responsibilities and non-reimbursable support with respect to enabling activities associated with the establishment and operation of USCYBERCOM elements located at NSA- Washington. The MOU shows that:

- NSA: (b)(3) (Public Law 86-36) [REDACTED]
- NSA: (b)(3) (Public Law 86-36) [REDACTED]

(S//REL TO USA, FVEY) NSA: (b)(3) (Public Law 86-36) [REDACTED]
NSA: (b)(3) (Public Law 86-36) [REDACTED]

(U) CONCLUSION:

(U) We did not substantiate the hotline allegations.

~~(S//REL TO USA, ACOU)~~ USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)

An August 9, 2010 MOU between NSA and USSTRATCOM provided for the integration of NSA employees into USCYBERCOM to perform USCYBERCOM mission and tasks under the direction and control of USCYBERCOM.


~~(S//REL TO USA, FVEY)~~ In August 2002, the Secretary of Defense delegated his SIGINT *delegation authority* to the DIRNSA. On January 27, 2010, the DIRNSA coordinated with the Director of National Intelligence the delegation of SIGINT authority to personnel filling designated USCYBERCOM positions. The Director of National Intelligence acknowledged and agreed with this plan on March 5, 2010.

(U//~~FOUO~~) NSA and USCYBERCOM developed policies and procedures to account for the costs associated with support provided from one organization to the other. On August 1, 2010, the Inter-service Support Agreement between the NSA and USSTRATCOM detailed the reimbursable support requirements, procedures, and costs associated with the establishment and operation of USCYBERCOM. NSA's Resources Management Organization is required to monitor support services and submit monthly reports to USCYBERCOM on expenses incurred by NSA.

(U) We did not verify the efficacy of the accounting mechanisms as that was outside the scope of this review. We found some documentation deficiencies that we reported to management. As NSA and USCYBERCOM implement the management controls for the NSA/USCYBERCOM relationship, the required internal reviews of the management controls should address these areas. Appendix A provides more details.

(U//~~FOUO~~) Appendix B discusses the lack of the U.S. Government definition for "use of force" as it pertains to operations in cyberspace, potentially leading to inconsistencies in interpretation of what constitutes force in cyberspace.

(U//~~FOUO~~) Thank you for your support of our efforts in responding to this Hotline request. Although not required, if you have comments to this report, please provide them to NSA (b)(3)-PL 86-36 by May 31, 2011. If you have any questions, please contact me at 703-604-8800 or Sean Mitchell at 703-604-8815.


Patricia A. Brannin
Deputy Inspector General
for Intelligence

(U) Appendix A. Other Matters of Interest

(U) OMB Circular A-123, "Manager's Responsibility for Internal Control" December 21, 2004, states that agencies should establish controls that reasonably ensure that obligations and costs are in compliance with applicable law; funds, property, and other assets are safeguarded against waste, loss, unauthorized use, and misappropriation; and revenues and expenditure applicable to agency operations are properly recorded and accounted for and to maintain accountability over assets. Congress notes that operations in cyber space have outpaced the development of policy, law, and standards to guide and control those operations. As a result, continuous management control reviews within USCYBERCOM are essential to the success of the command.

(U) In our review, we did not validate management controls in place for USCYBERCOM operations. However, USCYBERCOM only recently obtained full operational capability in October 2010 and is still fine tuning procedures. Nevertheless, we identified potential weaknesses that may warrant future management control reviews. Management has acknowledged and corrected some of these problems, such as document gaps.

~~(TS//SI//NF)~~ **Training Certification and Acknowledgements.** According to DIRNSA/Commander USCYBERCOM

USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)
NSA: (b)(3) (Public Law 86-36)

At the completion of the training, they are required to sign an acknowledgment form indicating they agree and understand the rules and regulations. However, NSA and USCYBERCOM have become aware that the acknowledgment forms were not signed prior to

NSA: (b)(3) (Public Law 86-36)
NSA and USCYBERCOM recognized that this is a management control weakness and have taken steps to remedy document gaps. Specifically, copies of the acknowledgment forms will be maintained by both NSA and USCYBERCOM.

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

USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)

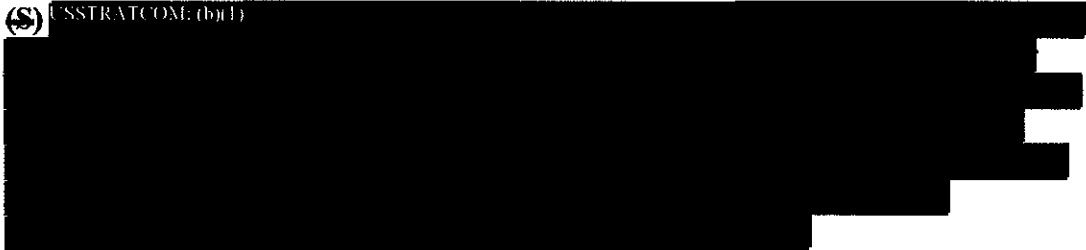
~~(TS//SI//NF)~~

USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)

(S) USSTRATCOM: (b)(1), NSA: (b)(3) (Public Law 86-36)



(S) USSTRATCOM: (b)(1)



(U//FOUO) Funding. The ISA and a MOU between NSA and USSTRATCOM documents all agreed upon reimbursable and non-reimbursable support requirements. However, during our review we did not verify if NSA and USCYBERCOM are effectively executing the requirements and procedures and managing costs associated with the agreements.

(U) Appendix B. Use of Force

(S//REL TO USA, ACGU) In the course of our review ^{USSTRATCOM (b)(1)} [REDACTED]

[REDACTED] Further inquiry revealed that there is not a precise U.S. Government definition for “use of force” in cyberspace. Consequently, USCYBERCOM used its own definition and measured its use of civilians against that definition.

(S) USCYBERCOM defines “use of force” in cyberspace as those actions that would cause physical damage similar to what is produced by traditional military operations. The determination ^{USSTRATCOM (b)(1)} [REDACTED] was made by the Legal Advisor to Commander, USCYBERCOM by analyzing the nature of the proposed capabilities ^{USSTRATCOM (b)(1)} [REDACTED]

(S) Congress questioned the DIRNSA about use of force in the *Advanced Questions Nominee for Commander, USCYBERCOM March 26, 2010*. The DIRNSA replied by stating, “Article 2(4) of the United Nations Charter provides that states shall refrain from the threat or use of force against the territorial integrity or political independence of any state. DoD operations are conducted consistent with international law principles in regard to what is a threat or use of force in terms of hostile intent and hostile act, as reflected in the Joint Chiefs of Staff’s *Standing Rules of Engagement / Standing Rules for the Use of Force for U.S. Forces, June 13, 2005 (SROE)*.”

(S) The SROE authorizes the U.S. to use force in self-defense when the requirements of necessity (i.e., when a hostile act occurs or when an opponent exhibits hostile intent) and proportionality (i.e., the principle that the amount of force used to counter a hostile act or hostile intent must be reasonable in intensity, duration, and magnitude) are met. The SROE permits the use of force when “adversary hostile acts and demonstrated hostile intent are defined to involve disruption, denial, degradation, exploitation, or destruction of U.S. computer systems or the information on them from which there is a high probability of immediate loss of life, serious injury, or loss of systems vital to national security.” However, The SROE neither mentions what constitutes a hostile act or hostile intent within cyberspace, nor does it explain what constitutes a use of force in cyberspace.

(U) Since there is no international consensus on a precise definition of use of force as it pertains to cyberspace, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force in cyberspace. Thus, there is always potential disagreement among nations concerning what may amount to a threat or

use of force. This potential inconsistency of interpretation should be considered carefully when the U.S. Government plans or reacts to activities in cyberspace.

~~SECRET//COMINT//NOFORN~~



Inspector General Department of Defense

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