113TH CONGRESS
2nd Session

SENATE

REPORT

INQUIRY INTO CYBER INTRUSIONS AFFECTING U.S. TRANSPORTATION COMMAND CONTRACTORS

REPORT

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

**** GPO – USE THIS LINE FOR BACK STRIP ****

INQUIRY INTO CYBER INTRUSIONS AFFECTING U.S. TRANSPORTATION COMMAND CONTRACTORS

COMMITTEE ON ARMED SERVICES

CARL LEVIN, Michigan, *Chairman*

JACK REED, Rhode Island	JAMES M. INHOFE, Oklahoma
BILL NELSON, Florida	JOHN McCAIN, Arizona
CLAIRE McCASKILL, Missouri	JEFF SESSIONS, Alabama
MARK UDALL, Colorado	SAXBY CHAMBLISS, Georgia
KAY R. HAGAN, North Carolina	ROGER F. WICKER, Mississippi
JOE MANCHIN III, West Virginia	KELLY AYOTTE, New Hampshire
JEANNE SHAHEEN, New Hampshire	DEB FISCHER, Nebraska
KIRSTEN E. GILLIBRAND, New York	LINDSEY GRAHAM, South Carolina
RICHARD BLUMENTHAL, Connecticut	DAVID VITTER, Louisiana
JOE DONNELLY, Indiana	ROY BLUNT, Missouri
MAZIE K. HIRONO, Hawaii	MIKE LEE, Utah
TIM KAINE, Virginia	TED CRUZ, Texas
ANGUS S. KING, JR., Maine	

PETER K. LEVINE, *Staff Director*
JOHN A. BONSELL, *Minority Staff Director*

INVESTIGATION TEAM

JOSEPH M. BRYAN, *Professional Staff Member*
OZGE GUZELSU, *Majority Counsel*

WILLIAM S. CASTLE, *Minority General Counsel*
SAMANTHA L. CLARK, *Minority Counsel*

ALEXANDRA M. HATHAWAY, *Staff Assistant*

Table of Contents

List of Acronyms

AFOSI	Air Force Office of Special Investigations
APT	Advanced Persistent Threat
CRAF	Civil Reserve Air Fleet
CYBERCOM	U.S. Cyber Command
DC3	Defense Cyber Crime Center
DCHC	Defense Counterintelligence and Human Intelligence Center
DCISE	Defense Industrial Base Collaborative Information Sharing Environment
DIA	Defense Intelligence Agency
DIB CS/IA	Defense Industrial Base Cyber Security and Information Assurance
DOD	Department of Defense
DSB	Defense Science Board
DSS	Defense Security Service
FBI	Federal Bureau of Investigation
[redacted]	[redacted]
[redacted]	[redacted]
ISL	Industrial Security Letter
JPT	Joint Planning Team
LHM	Letterhead Memorandum
MDCO	Military Department Counterintelligence Investigative Organization
MOU	Memorandum of Understanding
MSP	Maritime Security Program
MVP	Mobility Value Points
NCIJTF	National Cyber Investigative Joint Task Force
NCIS	Naval Criminal Investigative Service
NDAA	National Defense Authorization Act
PLA	Chinese People's Liberation Army
SCR	Suspicious Contact Report
TRANSCOM	U.S. Transportation Command
VISA	Voluntary Intermodal Sealift Agreement

Executive Summary

"We can't stop an attack unless we can see it."

General Martin E. Dempsey
Chairman Joint Chiefs of Staff
June 27, 2013

(U) In April 2013, the Senate Armed Services Committee initiated an inquiry into how much information was known to the U.S. Transportation Command (TRANSCOM) about successful cyber intrusions affecting command contractors. The committee focused on TRANSCOM because of the central role that the command plays in mobilization, deployment, and sustainment operations and the critical capabilities that private companies contribute to TRANSCOM's ability to meet military requirements in contingencies.

(U) Over the course of the inquiry, the committee reviewed information provided by TRANSCOM, 11 command contractors, the Federal Bureau of Investigation (FBI), the Defense Security Service (DSS), the Defense Cyber Crime Center (DC3), and the U.S. Air Force Office of Special Investigations (AFOSI). The committee also reviewed TRANSCOM's cyber incident reporting requirement, cyber intrusion reporting provisions included in the Fiscal Year 2013 National Defense Authorization Act (NDAA), and a number of executive branch guidelines, directives, and agreements to assess their effectiveness in promoting information sharing.

(U) The committee's inquiry identified approximately 50 successful intrusions or other cyber events[1] targeting TRANSCOM contractors between June 1, 2012 and May 30, 2013. Of those 50, at least 20 were successful intrusions into contractor networks attributed to an "advanced persistent threat" (APT), a term used to distinguish sophisticated cyber threats that are frequently associated with foreign governments. Of those APT-linked intrusions, TRANSCOM was made aware of only two, a troubling finding given the potential impact of cyber intrusions on defense information and operations.

(U) ~~(S//NF)~~ Of the at least 20 successful cyber intrusions attributed to an APT, all were attributed to China.

[1] Cyber events include incidents that may not be confirmed successful intrusions but which the FBI determined that a victim notification was warranted.

(U) As to the reasons for TRANSCOM's lack of knowledge regarding these intrusions, the committee found gaps in requirements that result in many cyber intrusions not being reported to the command and a lack of common understanding between TRANSCOM and its contractors as to the scope of cyber intrusions that must be reported. The committee also found that FBI and Department of Defense (DOD) components were frequently unaware that companies they had identified as victims of cyber intrusions were TRANSCOM contractors. In addition, the inquiry revealed misperceptions about the rules governing how cyber intrusion-related information identifying a particular victim may be shared and a lack of communication between TRANSCOM and other DOD components regarding TRANSCOM's need to know about cyber intrusions. In the end, these shortcomings left TRANSCOM uninformed about the overwhelming majority of cyber intrusions affecting contractor networks by APT actors.

I. The Cyber Threat to Defense Operations

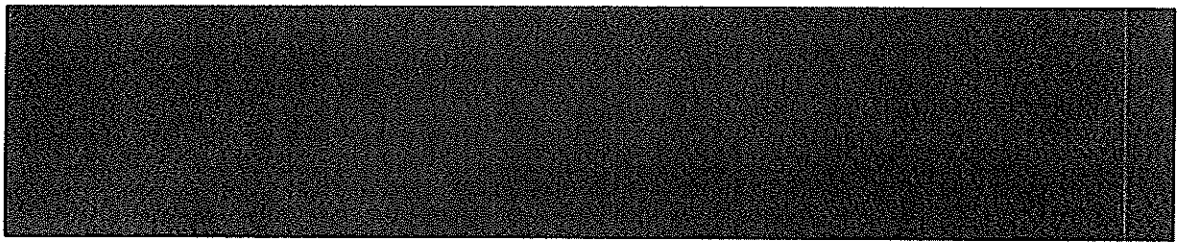
(U) Foreign governments regularly probe DOD and private contractor computer networks to identify vulnerabilities that could allow them to compromise systems in order to steal intellectual property, collect intelligence, or establish a foothold for future exploitation. The theft through cyberspace of U.S. companies' intellectual property risks long-term damage to U.S. economic security. The damage inflicted by compromises of the defense industry goes well beyond economic impacts. As the Director of National Intelligence has said, cyber theft "is almost certainly allowing our adversaries to close the technological gap between our respective militaries, slowly neutralizing one of our key advantages in the international arena."

(U) Cyber intrusions into private sector networks also have the potential to impact military operations. The private sector plays a crucial role in force mobilization, deployment, and sustainment operations. For example, private airlines provide more than 90 percent of DOD's passenger movement capability and more than one-third of its bulk cargo capability. In addition, the overwhelming majority of DOD deployment and distribution transactions occur over unclassified networks, many of which are owned by private companies. In fact, TRANSCOM's Commander has estimated that "over 90 percent of DOD deployment and distribution transactions are handled on unclassified systems."

(U) Chinese military analysts, for example, have identified logistics and mobilization as potential U.S. vulnerabilities "given the requirements for precision in coordinating transportation, communications, and logistics networks." In fact, Chinese military doctrine "advocate[s] targeting adversary command and control and logistics networks to impact their ability to operate during the early stages of conflict." U.S. experts on Chinese military planning have raised the prospect of China using cyber capabilities to impede U.S. force deployment in the event of a contingency.

(U) In discussing China's cyber capabilities, DOD has pointed out "the accesses and skills required for [stealing information] are similar to those necessary to conduct computer network *attacks*." As the Defense Science Board (DSB) said in its 2013 report:

Should the United States find itself in a full-scale conflict with a peer adversary, attacks would be expected to include denial of service, data corruption, supply chain corruption, traitorous insiders, kinetic and related non-kinetic attacks at all altitudes from underwater to space. U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed.



(U) Peacetime cyber compromises of operationally critical contractors could prove valuable to foreign countries, such as China, as a source of intelligence about network operations or to establish a foothold in the computer networks of companies that supply crucial support to DOD operations, either of which could be exploited in a contingency.

[redacted]

(U) • ~~(S//NF)~~ Between 2008 and 2010, a TRANSCOM contractor [redacted] was compromised by the Chinese military who stole emails, documents, user accounts, passwords and even source code [redacted]

(U) • ~~(S//NF)~~ In 2009, the Chinese military compromised a TRANSCOM contractor, [redacted]

(U) • ~~(S//NF)~~ In 2010, the Chinese military compromised the computer network of a Civil Reserve Air Fleet (CRAF) contractor, stealing documents, flight details, credentials and pins and passwords for encrypted email. That same year, the Chinese military compromised another TRANSCOM contractor, [redacted]

(U) • ~~(S//NF)~~ In 2012, the Chinese military compromised "multiple systems" onboard a commercial ship contracted by TRANSCOM for logistics routes.

(U) • ~~(S//NF)~~ In 2013, [redacted] on China's military spear-phishing campaigns targeting commercial logistics companies that support command operations. Also in 2013, a CRAF airline was the victim of a phishing email, attributed to the Chinese government, which is suspected to have led to a malware download on the airline's network.

II. Cyber Threat Information-Sharing

(U) Information sharing is one key to combating cyber threats. As Chairman of the Joint Chiefs of Staff Martin Dempsey has said, "every day, adversaries are injecting malware into our networks, the worst of this malware is equivalent to cyber bullets and bombs. We must share what it looks like so that we can stop it before it detonates."

(U) While TRANSCOM can monitor its own network for possible cyber intrusions, the command's knowledge of intrusions into contractor computer networks depends on reporting from the contractors themselves, other DOD components, the FBI, and other government agencies. The committee's inquiry found, however, that TRANSCOM is only aware of a small fraction of APT intrusions into its contractors. In fact, TRANSCOM was aware of only one of 11 APT intrusions detected by a subset of TRANSCOM contractors from whom the committee requested information. In addition, TRANSCOM was only aware of one of at least nine successful APT intrusions and none of six other cyber events targeting TRANSCOM contractor networks that were known to the U.S. government.

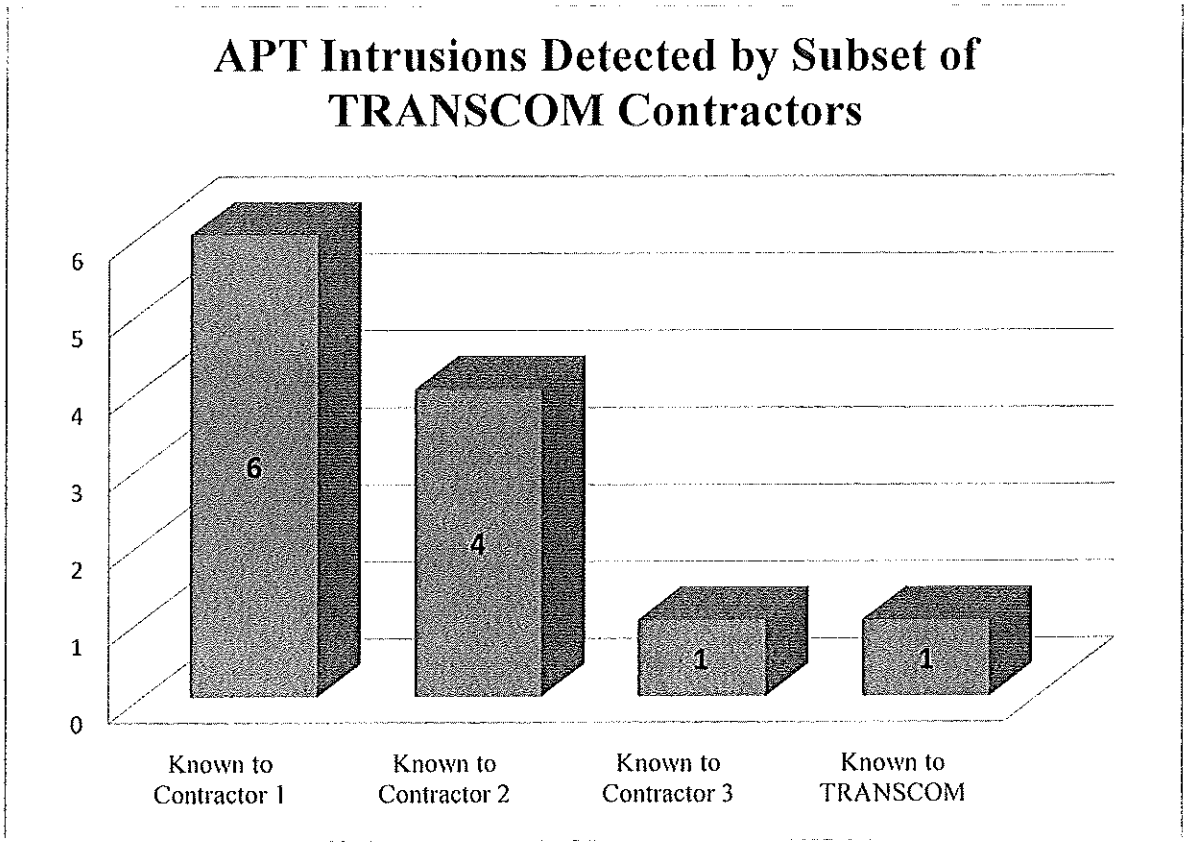
A. TRANSCOM Contractor Intrusion Reporting

(U) Beginning in 2010, in what may be the first effort by a DOD component to use contract language to improve cyber intrusion information-sharing, TRANSCOM began including a clause in its contracts requiring that certain cyber security incidents be reported to the command. While more than 80 companies are subject to the clause, up until August 2013, TRANSCOM had received only two cyber intrusion reports from those contractors. In order to assess how companies were complying with reporting requirements, the committee requested information from 11 TRANSCOM contractors about cyber intrusions they experienced between January 1, 2013 and June 30, 2013 and how they determined whether or not the intrusions were reportable. The group included six Civil Reserve Air Fleet (CRAF) airlines, three shippers who are participants in the Voluntary Intermodal Sealift Agreement (VISA) and two companies that provide the command with logistics systems support services.

(U) Of the 11 contractors, eight said that they were not aware of any cyber intrusions having occurred during the period in question. (That does not necessarily mean the eight contractors were not victims of a successful intrusion during that period, only that they were not *aware* of such an intrusion.) The remaining three companies identified a total of 32 intrusions.[2] As reflected in the chart below, of the 32 intrusions, 11 were associated with an advanced persistent threat (APT) actor. In describing APTs, the FBI has said "the sophistication, resources, and types of information sought [by APT actors] suggest governmental support."

(U) ~~(S)~~ All 11 were attributed to China.

[2] One of those intrusions occurred in August 2013, which is outside the period initially covered by the committee's inquiry.



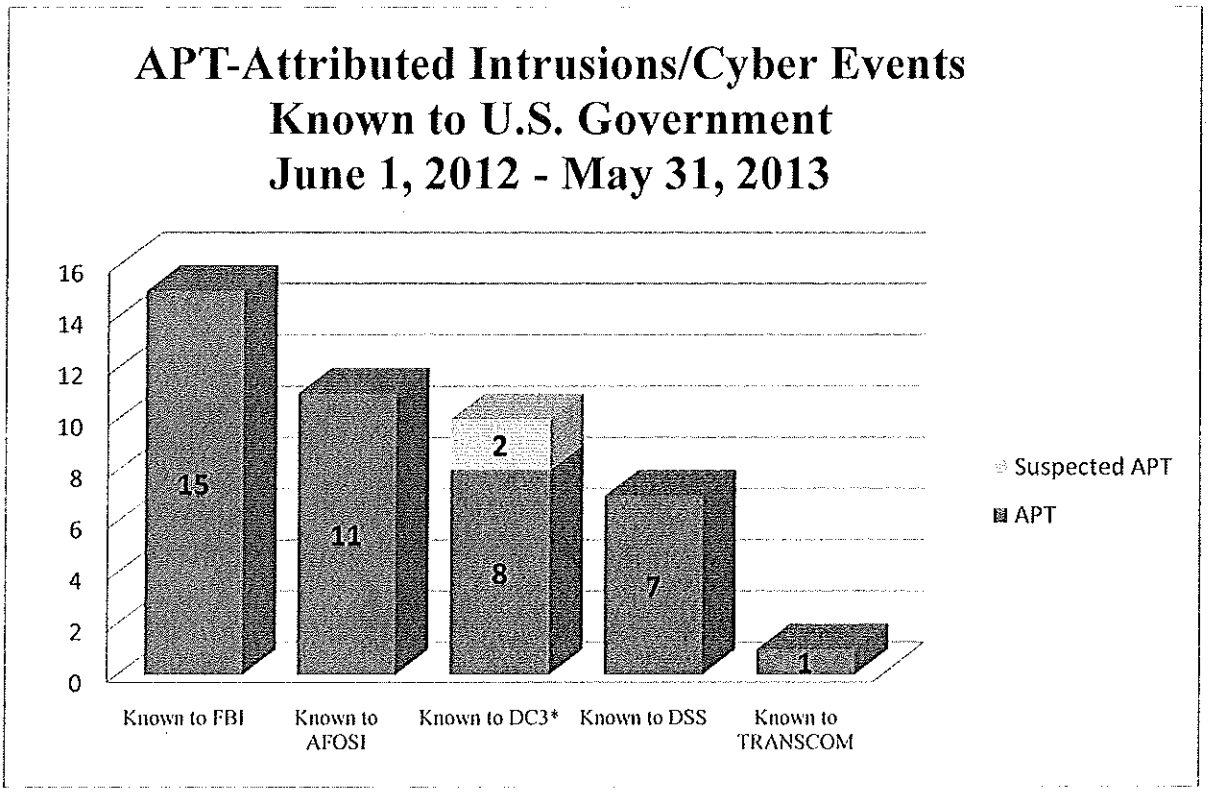
(U) Of those 11 APT intrusions, TRANSCOM was aware of only one. One reason for that was a lack of common understanding between the command and its contractors as to the scope of cyber intrusions that must be reported. In fact, none of the contractors with whom the committee discussed the issue interpreted their reporting obligation in a manner consistent with TRANSCOM's intent. In addition, TRANSCOM's contract clause limits the scope of what must be reported, only requiring companies to report intrusions into networks that are storing or communicating DOD data at the time of the compromise. That limitation could be highly problematic when, in the event of a major contingency, a contractor's ability to support defense requirements depended on the efficient functioning of computer networks normally reserved for commercial business. A prior or preexisting compromise of such networks could be exploited to affect the contractor and potentially TRANSCOM operations.

B. Intra-governmental Information Sharing

(U) Ensuring that defense contractors inform DOD about cyber intrusions into their networks is critical to mitigating cyber threats. However, that alone will not solve the problem. Timely *intra-governmental* information sharing about private sector network compromises is also essential, particularly when network compromises involve an APT.

(U) The committee's inquiry identified at least 20 successful intrusions or other events targeting TRANSCOM contractors that occurred between June 1, 2012 and May 31, 2013 and

were known to the FBI, DSS, DC3, or AFOSI. Fifteen of those 20 were associated with an advanced persistent threat actor (APT) and at least nine of those 15 were successful intrusions into a contractor network. TRANSCOM was aware of only one of those intrusions and none of the other events.



** DC3 categorizes intrusions as "probable" or "suspected" APT.*

(U) The reasons TRANSCOM was unaware of those intrusions include misperceptions about the rules governing how cyber intrusion-related information may be shared and a lack of common understanding between the command and other DOD components about what cyber information TRANSCOM needs to know.

(U) A 2011 FBI-DOD Memorandum of Understanding (MOU) requires the Bureau to share information on cyber intrusions with DOD when an intrusion is attributed to an APT *and the Bureau knows that the victim is a defense contractor.* While the FBI is in the process of integrating the full list of more than 10,000 cleared DOD contractors into their information-sharing database, no DOD component had provided the Bureau a list of specific operationally critical contractors about whom they would like to be informed when they have been the victim of a cyber intrusion. On January 30, 2014, TRANSCOM provided the FBI a list of 80 companies. That list, however, included all command contractors who are subject to TRANSCOM's cyber incident reporting clause and did not identify which of the 80 are operationally critical contractors.

(U) Depending on the identity of the victimized company and whether the FBI knows which military service has a contract with the victim, the DOD recipient of FBI information may include DSS and AFOSI, the military department counterintelligence office responsible for TRANSCOM. In fact, of the 15 APT intrusions and other cyber events identified by the FBI, AFOSI said that it was aware of 11. As to DSS, while the agency said that it was aware of eight intrusions affecting *victims* on the FBI's list, its records were not sufficient to determine whether the actual *intrusions* matched those identified by the FBI or whether DSS had been made aware of additional intrusions.

(U) The information sharing MOU requires DOD recipients of FBI information to seek the Bureau's permission in order to share FBI information outside of their organizations. The FBI did not receive a single request for a DOD agency to share information relating to the 15 APT intrusions and other events targeting TRANSCOM contractors. Neither DSS nor AFOSI identified a connection between TRANSCOM and victimized contractors on their own. Not until January 30, 2014 did TRANSCOM provide FBI and AFOSI a list of contractors about whom the command would like to be alerted when they were compromised by an APT. TRANSCOM was made aware of only one of the APT-attributed intrusions identified by the FBI.

(U) While it may receive cyber intrusion reports from the FBI, the Defense Cyber Crime Center (DC3) also receives reports of intrusions directly from companies who are members of the agency's Defense Industrial Base Cyber Security and Information Assurance (DIB CS/IA) Program. In fact, DC3 was informed of 10 successful intrusions affecting six TRANSCOM contractors who were DIB CS/IA members during the period covered by the committee's inquiry. TRANSCOM, however, was aware of only one of those 10 intrusions. While DC3 does not normally share the identity of DIB CS/IA members who have been victimized by the cyber intrusion, DOD has said that identity information may be shared when a national security interest is at stake. As of February 1, 2013, however, TRANSCOM had not requested that DC3 notify the command about cyber intrusions into specific operationally critical contractors. TRANSCOM did provide the FBI and AFOSI with a list of about 80 contractors on January 30, 2014, though that list did not specify which of the contractors were operationally critical.

(U) Cyber intrusions into operationally critical contractors pose a threat to defense operations. It is essential that potentially-affected commands, such as TRANSCOM, be aware of such intrusions so that they can take steps to mitigate the threat. The committee's inquiry identified serious gaps in intrusion reporting and information sharing that left TRANSCOM uninformed about the overwhelming majority of intrusions by APT actors into computer networks of its contractors. That is a problem that must be fixed. As General Dempsey put it, "[W]e can't stop an attack unless we can see it."

Conclusions of the Senate Armed Services Committee

(U) Conclusion 1: Cyber intrusions by foreign countries into the computer networks of U.S. Transportation Command (TRANSCOM) contractors pose a threat to U.S. military operations. The private sector plays a crucial role in force mobilization, deployment, and sustainment operations and the overwhelming majority of Department of Defense (DOD) deployment and distribution transactions occur over unclassified networks, many of which are owned by private companies. That reliance on the private sector is not lost on potential U.S. adversaries. For example, according to DOD, Chinese military analysts have identified logistics and mobilization as potential U.S. vulnerabilities "given the requirements for precision in coordinating transportation, communications, and logistics networks." U.S. experts, meanwhile, have raised the prospect of China using cyber capabilities to impede U.S. force deployment in the event of a contingency. Peacetime cyber compromises of the networks of operationally critical contractors could prove valuable to foreign governments as a source of intelligence about network operations or to establish a foothold in contractor networks, either of which could be exploited in a contingency.

(U) ~~(S//NF)~~ **Conclusion 2: Advanced persistent threat (APT) actors associated with the Chinese government successfully penetrated TRANSCOM contractor computer networks on more than 20 occasions during a single year.** The committee's inquiry identified approximately 50 successful intrusions or other cyber events targeting TRANSCOM contractor computer networks that occurred between June 1, 2012 and May 30, 2013. Of those, at least 20 were successful intrusions attributed to an "advanced persistent threat" (APT), a term used to distinguish sophisticated cyber threats that are frequently associated with foreign governments. All of those APT intrusions were attributed to China. Among those companies victimized by the intrusions were operationally critical contractors including airlines and shipping companies.

(U) Conclusion 3: TRANSCOM was unaware of the overwhelming majority of successful cyber intrusions by advanced persistent threat (APT) actors into the computer networks of their contractors. While nearly all of the at least 20 successful APT intrusions identified in the committee's inquiry were known to the Federal Bureau of Investigation (FBI), the Air Force Office of Special Investigations (AFOSI), the Defense Security Service (DSS), or the Defense Cyber Crime Center (DC3), TRANSCOM was aware of only two of those APT intrusions.

(U) ~~(FOUO)~~ **Conclusion 4: Rules governing information sharing do not preclude defense agencies from informing TRANSCOM about APT cyber intrusions such as those identified in the committee's inquiry.** TRANSCOM has said that information sharing rules have, at times, prevented the command from learning whether one of their contractors has been the victim of a cyber intrusion. Of the at least 20 successful APT intrusions discussed in the committee's report, about half were identified by the FBI. Most of those were known to DSS, AFOSI, or both. The committee's review did not identify any rules that should have prevented those defense agencies from informing TRANSCOM of the identity of the victimized contractors. While they may have had to seek FBI approval to do so, the committee identified no

restrictions that would have otherwise prevented DSS or AFOSI from providing FBI-related victim information to TRANSCOM. Nor is the committee aware of any internal DOD policies or guidelines that would have prevented those agencies from sharing information about the cyber intrusions with TRANSCOM. DC3 learned of eight "probable" APT intrusions from TRANSCOM contractors during the period covered by the committee's inquiry. While agreements between DC3 and companies that participate in its cyber intrusion information sharing program restrict the dissemination of victim identities, those agreements do not preclude such sharing when national security is at stake.

(U) Conclusion 5: Prior to January 30, 2014, when the committee's inquiry was nearing completion, TRANSCOM had not identified for FBI or DOD agencies a list of contractors about whom the command would like to be alerted when an APT compromise occurred. It is important that government agencies that receive information about private sector cyber intrusions be aware when a victim of an APT-attributed intrusion is an operationally critical contractor. However, when the FBI or a DOD component acquires information identifying a U.S. company as a victim, it may not always be apparent that the company is a defense contractor. Even in cases where a victimized company is known to be a defense contractor, it may not always be easy to identify the DOD component with which the company has a contract or to determine whether the contractor provides a critical operational capability. That awareness would be facilitated if commands, such as TRANSCOM, identified contractors about whom they would like to be alerted when an APT compromise occurs. Prior to January 30, 2014, when it supplied FBI and AFOSI with a list of 80 contractors, TRANSCOM had not provided FBI or any of the defense agencies a list of contractors about whom the command would like to be alerted when an APT compromise occurred. That list, however, included all command contractors subject to TRANSCOM's cyber incident reporting requirement and did not specify which are operationally critical.

(U) Conclusion 6: TRANSCOM's cyber intrusion reporting clause and reporting requirements contained in the Fiscal Year 2013 National Defense Authorization Act (NDAA) contain gaps that leave TRANSCOM uninformed about cyber intrusions affecting operationally critical contractors. The intent of both TRANSCOM's cyber reporting clause and the cyber incident reporting provision contained in the 2013 NDAA was to require defense contractors to report cyber intrusions impacting systems that contain or process DOD information at the time of the compromise. In the event of a major contingency, however, a contractor's ability to support defense requirements might depend on the efficient functioning of computer networks normally reserved for commercial business. A prior or preexisting compromise of a commercial network could be exploited to affect TRANSCOM operations when the contractor was called upon to support defense operations.

(U) Conclusion 7: TRANSCOM and its contractors lack a common understanding about contractual cyber incident reporting requirements. Beginning in 2010, TRANSCOM began including a clause in its contracts requiring that certain cyber security incidents be reported to the command. However, the contract language is ambiguous and none of the contractors with whom the committee discussed the clause interpreted their reporting obligation in a manner consistent with TRANSCOM's intent. Even if contractors shared TRANSCOM's interpretation,

complying with the clause would depend on companies knowing the systems on which contract-related DOD information resides or transits. The committee found that contractors do not always know where contract-related documents and information are held or which of their networks are used to exchange them.

Introduction

(U) Numerous government and private sector reports have identified Department of Defense (DOD) contractors as high priority targets for foreign government cyber operations. While much of the discussion about the national defense implications of that targeting has focused on the theft of DOD information, cyber intrusions pose operational risks as well. In discussing China's cyber capabilities, for example, DOD has said that "the accesses and skills required for [intrusions targeted at stealing information] are similar to those necessary to conduct computer network *attacks*." Given that, it is critical that DOD be aware of cyber intrusions into contractor networks, particularly when those intrusions affect contractors on whom the department relies to meet critical military requirements in contingency situations.

(U) In April 2013, the committee initiated an inquiry into how much is known about cyber intrusions into private DOD contractors that support U.S. Transportation Command (TRANSCOM). The committee focused on TRANSCOM because of the central role that the command plays in contingency mobilization, deployment, and sustainment operations and the critical capabilities that TRANSCOM contractors provide to meet military requirements in contingency operations.

(U) In the course of the inquiry, the committee reviewed information provided by TRANSCOM, 11 command contractors, the Federal Bureau of Investigation (FBI), the Defense Security Service (DSS), the Defense Cyber Crime Center (DC3), and the U.S. Air Force Office of Special Investigations (AFOSI). The committee also reviewed TRANSCOM's cyber incident reporting requirement, cyber intrusion reporting provisions included in the Fiscal Year 2013 National Defense Authorization ACT (NDAA), and a number of executive branch guidelines, directives, and agreements to assess their impact on cyber threat information sharing. This report describes the committee's findings.

(U) The committee's inquiry identified about 50 successful intrusions and other cyber events targeting TRANSCOM contractors between June 1, 2012 and May 30, 2013. Of those, at least 20 were successful intrusions into TRANSCOM contractor networks attributed to an "advanced persistent threat" (APT), a term used to distinguish sophisticated cyber threats that are frequently associated with foreign governments. Of those APT-linked intrusions, TRANSCOM was aware of only one.

(U) Part I of the report is focused on the threat that cyber intrusions pose to defense operations. The report discusses TRANSCOM's reliance on unclassified computer networks and private contractors to conduct operations and describes intelligence assessments of the cyber threat to operations. Part I also discusses the importance of information sharing about intrusions to mitigate the cyber threat.

(U) Part II of the report discusses the committee's finding that TRANSCOM was not aware of the overwhelming majority of cyber intrusions known to have affected the sample of command contractors between June 1, 2012 and May 30, 2013. Those intrusions were known,

however, to the contractors themselves, to the FBI, or a DOD component. Part II details several factors that contributed to TRANSCOM's lack of awareness of the intrusions, including gaps in cyber intrusion reporting requirements; differences in understanding between TRANSCOM and its contractors as to the scope of cyber intrusions that must be reported; a lack of common understanding between TRANSCOM and other DOD components about what cyber information TRANSCOM needs to know; and misperceptions about the rules governing how cyber intrusion-related information that identifies a particular victim may be shared.

I. The Cyber Threat to Defense Operations

(U) Foreign governments regularly probe U.S. Department of Defense (DOD) and private contractor computer networks to identify vulnerabilities that could allow them to compromise systems and steal intellectual property (including weapons designs and other sensitive business information), collect intelligence on U.S. military capabilities and intentions, and establish a presence that could be exploited to degrade the U.S. response in the event of a contingency.

(U) The theft through cyberspace of U.S. company intellectual property risks long-term damage to U.S. economic security. The cyber theft of defense-related information and technologies, much of which also resides with private companies, threatens to erode U.S. military technical superiority, placing national security and the safety of our troops at risk. The national security implications of cyber intrusions into private U.S. companies go beyond those related to the theft of intellectual property. Such intrusions also have the potential to adversely impact military operations.

(U) The private sector plays a crucial role in force mobilization, deployment, and sustainment operations. For example, private airlines provide more than 90 percent of DOD's passenger movement capability and more than one-third of its bulk cargo capability. In addition, the overwhelming majority of DOD deployment and distribution transactions occur over unclassified networks, many of which are owned by private companies. Private companies also play an integral role in the development of software and systems to support military logistics. These arrangements, while necessary, create vulnerabilities that could be exploited to degrade or disrupt the U.S. military's response to contingencies.

(U) Information sharing about cyber intrusions into private sector computer networks is one key to combating such threats. As Chairman of the Joint Chiefs of Staff Martin Dempsey has said, "every day, adversaries are injecting malware into our networks; the worst of this malware is equivalent to cyber bullets and bombs. We must share what it looks like so that we can stop it before it detonates." As General Dempsey put it, "We can't stop an attack unless we can see it."

A. Defense Intellectual Property Theft

(U) Every day, U.S companies face an onslaught of cyber attacks targeting their intellectual property. Though it is difficult to estimate the economic losses suffered by companies who have their intellectual property stolen, General Keith B. Alexander, head of the National Security Agency and U.S. Cyber Command, has called the theft of intellectual property through cyberspace "the greatest transfer of wealth in history."[3]

(U) In March 2013, Mandiant, a company that investigates private sector cyber security breaches, published a report describing how a cyber-espionage unit of the Chinese People's Liberation Army (PLA) had raided the computers of at least 141 different organizations, stealing "technology blueprints, proprietary manufacturing processes, test results, business plans, pricing

[3] Statement of General Keith Alexander, American Enterprise Institute (July 9, 2012).

documents, [and] partnership agreements."[4] Industries identified in the Mandiant report as being compromised by the PLA included many critical to U.S. national defense, such as information technology, aerospace, and satellites and telecommunications.[5] In fact, companies that develop, manufacture, and sustain critical weapons and information systems for DOD are a frequent target of cybertheft and the Mandiant report was only one among many accounts of defense industrial base companies being raided by the PLA.[6]

B. Operational Implications of Cyber Intrusions

(U) The damage inflicted by compromises of the defense industry goes well beyond economic impacts, as the theft has operational implications as well. As the Defense Science Board stated in a January 2013 report:

> The DOD, and its contractor base are high priority targets that have sustained staggering losses of system design information incorporating years of combat knowledge and experience. Employing reverse engineering techniques, adversaries can exploit weapon system technical plans for their benefit. Perhaps even more significant, they gained insight to operational concepts and system use ... developed from decades of U.S. operational and developmental experience.... Such information provides tremendous benefit to an adversary, shortening time for development of countermeasures by years.[7]

(U) Likewise, the Director of National Intelligence has said that cybertheft "is almost certainly allowing our adversaries to close the technological gap between our respective militaries, slowly neutralizing one of our key advantages in the international arena."[8]

(U) Network intrusions that enable the theft of defense information and erode our operational advantage in the long term may pose more immediate threats to defense operations. In discussing China's cyber capabilities, DOD has stated that "the accesses and skills required for [intrusions targeted at stealing information] are similar to those necessary to conduct computer network *attacks*."[9] As the Defense Science Board (DSB) said in its 2013 report:

---

[4] Mandiant, *APT1 Exposing One of China's Cyber Espionage Units* (February 2013) at 3.
[5] *Id.* at 24.
[6] *See e.g.* On May 2, 2013 Bloomberg news reported on the theft by the Chinese PLA of information from a company called QinetiQ, a U.S. defense contractor. The report said the theft "jeopardized the [victim] company's sensitive technology involving drones, satellites, the U.S. Army's combat helicopter fleet, and military robotics, both already-deployed systems and those still in development." According to Bloomberg, "hackers had burrowed into almost every corner of QinetiQ's U.S. operations, including production facilities and engineering labs in St. Louis, Pittsburgh, Long Beach, Mississippi, Huntsville, Alabama and Albuquerque, New Mexico, where QinetiQ engineers work on satellite-based espionage, among other projects." Michael Riley and Ben Elgin, *China's Cyberspies Outwit Model for Bond's Q*, Bloomberg (May 2, 2013).
[7] Department of Defense, Defense Science Board Task Force Report, *Resilient Military Systems and the Advanced Cyber Threat* (January 2013).
[8] James C. Clapper, U.S. Senate Select Committee on Intelligence hearing on Current and Projected National Security Threats to the United States (March 12, 2013).
[9] *Military and Security Developments Involving the People's Republic of China* 2013 Annual Report to Congress at 36. (emphasis added)

> Should the United States find itself in a full-scale conflict with a peer adversary, attacks would be expected to include denial of service, data corruption, supply chain corruption, traitorous insiders, kinetic and related non-kinetic attacks at all altitudes from underwater to space. U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed. Military Commanders may rapidly lose trust in the information and ability to control U.S. systems and forces. Once lost, that trust is very difficult to regain.[10]

(U) As the DSB suggests, the ability to establish a foothold in DOD or contractor computer networks could provide a valuable position from which to target operations and affect the U.S. military's ability to respond quickly or effectively in the event of a contingency.

C. Network-Dependent Military Logistics

(U) The Department of Defense relies heavily on the private sector for logistics support. In fact, the head of U.S. Cyber Command has estimated that "more than 80 percent of our logistics are transported by private companies."[11] The overwhelming majority of that business activity takes place on unclassified networks. The Commander of U.S. Transportation Command (TRANSCOM), which provides transportation services and logistical support to DOD and the military services, has estimated that "over 90 percent of DOD deployment and distribution information transactions are handled on unclassified systems."[12] TRANSCOM's Civil Reserve Air Fleet (CRAF) and Voluntary Intermodal Sealift Agreement (VISA) programs are two examples of how DOD relies on private sector capabilities to meet military mobilization, deployment, and sustainment requirements.

1. Civil Reserve Air Fleet (CRAF)

(U) The Civil Reserve Air Fleet (CRAF) is a voluntary cooperative program between private airlines, the Department of Transportation, and TRANSCOM to augment Department of Defense airlift assets with commercial aircraft during emergencies such as war or natural disasters. In exchange for making their aircraft available for deployments of military forces or supplies during contingencies, CRAF companies are eligible to receive preference for DOD peacetime business.[13] Approximately 30 airlines participate in the program, although that

---

[10] Department of Defense Science Board Task Force report *Resilient Military Systems and the Advanced Cyber Threat* (January 2013).
[11] General Keith Alexander, Center for Strategic and International Studies (June 3, 2010) at 8.
[12] Hearing to receive testimony on U.S. Africa Command and U.S. Transportation Command in review of the Defense Authorization Request for Fiscal Year 2014 and the Future Years Defense Program. Prepared statement of General William M. Fraser III, Senate Armed Services Committee (March 7, 2013) at 19.
[13] U.S. Air Force Fact Sheet: Civil Reserve Air Fleet. http://www.amc.af.mil/library/factsheets/factsheet.asp?id=234; Issues *Regarding the Current and Future Use of the Civil Reserve Air Fleet*, Congressional Budget Office (October 2007) at 1.

number can change from year to year.[14] The CRAF program provides more than 90 percent of DOD's passenger movement capability and more than one-third of the bulk cargo capability.[15]

(U) TRANSCOM's Commander can activate the CRAF program with the concurrence of the Secretary of Defense.[16] Stage 1 activation is for regional contingencies that only require a small augmentation of the military's fleet.[17] Stage 1 was activated during Operation Desert Shield and Operation Iraqi Freedom.[18] Stage 2 is intended for activation in the event of a major theater war and was activated in support of Operation Desert Shield/Desert Storm.[19] Stage 3 activation is reserved for contingencies requiring the mobilization of all DOD resources.[20] A Stage 3 CRAF activation has yet to occur.[21]

2. Voluntary Intermodal Sealift Agreement (VISA) program

(U) Similar to the CRAF program, the Voluntary Intermodal Sealift Agreement (VISA) program is a partnership between the government and private shipping companies to meet military sealift requirements. In exchange for their commitment to make ships and intermodal facilities available during contingencies, VISA participants receive preference for DOD peacetime business. DOD is extremely dependent on commercial shippers to deploy and sustain forces. According to TRANSCOM, in 2012 commercial vessels moved 95 percent of DOD dry cargoes.[22]

(U) Like the CRAF program, VISA is activated in three stages based on military requirements and may be activated by the TRANSCOM Commander with approval of the Secretary of Defense.[23] The majority of VISA capacity is provided by ships that are enrolled in the Maritime Security Program (MSP) which is intended to ensure that the U.S. military has access to commercial ships to meet national defense and other security requirements. The MSP provides funding to vessel operators to offset costs associated with operating under U.S. flag.[24]

---

[14] U.S. Transportation Command, *Based Upon CY10 Block Hours* (undated); U.S. Transportation Command, calendar year 2011 CRAF block hours (June 24, 2013).
[15] U.S. Transportation Command, 2012 Annual Report at 4.
[16] *Issues Regarding the Current and Future Use of the Civil Reserve Air Fleet*, Congressional Budget Office (October 2007) at 2.
[17] *Id.* at 2.
[18] *Id.* at 2-3.
[19] *Id.* at 3.
[20] Performance Work Statement for Airlift Services in Support of the Department of Defense and the Civil Reserve Air Fleet (October 2012) at 1; Issues *Regarding the Current and Future Use of the Civil Reserve Air Fleet*, Congressional Budget Office (October 2007) at 3.
[21] *Issues Regarding the Current and Future Use of the Civil Reserve Air Fleet*, Congressional Budget Office (October 2007) at 3.
[22] U.S. Transportation Command, 2012 Annual Report (undated) at 15.
[23] U.S. Department of Transportation Maritime Administration, Voluntary Intermodal Sealift Agreement pamphlet (December 2011).
[24] U.S. Department of Transportation Maritime Administration, Maritime Security Program pamphlet (March 2011); Econometrica, Inc. Maritime Security Program Impact Evaluation (July 2009) at 7.

D. Cyber Threats to TRANSCOM

(U) The critical role of defense logistics in military operations and the Department's reliance on private contractors and unclassified computer networks to conduct those operations makes logistics-related networks attractive targets for cyber attacks.

(U) According to DOD, Chinese military analysts, for example, have identified logistics and mobilization as potential U.S. vulnerabilities "given the requirements for precision in coordinating transportation, communications, and logistics networks."[25] The Department has said that Chinese military doctrine "advocate[es] targeting adversary command and control and logistics networks to impact their ability to operate during the early stages of conflict."[26] U.S. experts on Chinese military planning raise the prospect of China using cyber capabilities to impede U.S. force deployment in the event of a contingency.[27] TRANSCOM and private sector networks that enable command operations are logical targets.

[redacted]

[25] Office of the Secretary of Defense Annual Report to Congress *Military Power of the People's Republic of China 2008*

[26] Military and Security Developments Involving the People's Republic of China 2011 Annual Report to Congress at 6.

[27] James Mulvenon, *PLA Computer Network Operation: Scenarios, Doctrine, Organizations, and Capability* (September 2008); Martin Libicki, *Chinese Use of Cyberwar as an Anti-Access Strategy Two Scenarios*, Statement before the U.S. China Economic and Security Review Commission (January 27, 2011).

[redacted]

(U) ~~(S//NF)~~ As mentioned above, U.S. experts on Chinese military planning suggest that China could seek to use cyber capabilities to impede U.S. force deployment in a contingency.[33]

[redacted]

(U) As discussed below, while TRANSCOM mission execution depends on the ability of private sector contractors to provide critical capabilities, the command has only limited information about successful intrusions into computer networks of its contractors.

E. Information Sharing as Key to Protecting Military Operations

(U) Chairman of the Joint Chiefs of Staff General Martin Dempsey has said "[W]e can't stop an attack unless we can see it."[36] While it is critical that the Department and the military commands monitor their own networks, it is also important that they have information about cyber intrusions into private sector networks that could impact defense operations. For example, TRANSCOM's ability to mobilize, deploy and sustain forces depends on the efficient functioning of computer networks at both the command and the private sector service providers on whom it relies.

(U) ~~(S//NF)~~ China, for one, has exhibited both the capability and intent to compromise private sector computer networks used to support TRANSCOM operations. [redacted] reports that Chinese military cyber operations "collect against [redacted] by exploiting the systems, networks, personnel, and partners USTRANSCOM relies upon to accomplish assigned missions."[37] [redacted] "Chinese cyber efforts target a variety of civilian institutions...largely because DOD logistics continues to integrate commercial, government, military and international partners."[38]

(U) A failure to share information about cyber intrusions into private contractor networks can reduce DOD's ability to mitigate such intrusions and permit foreign governments to establish a presence that could be exploited to impact operations.

---

[33] James Mulvenon, *PLA Computer Network Operation: Scenarios, Doctrine, Organizations, and Capability* (September 2008); Martin Libicki, *Chinese Use of Cyberwar as an Anti-Access Strategy Two Scenarios*, Statement before the U.S. China Economic and Security Review Commission (January 27, 2011).

[redacted]

[36] Dempsey at Brookings (June 27, 2013)

[redacted]

[redacted]

(U) ~~(S/NF)~~ Intelligence reporting on China's specific efforts evidence the threat posed by cyber compromises.

(U) • ~~(S/NF)~~ Between 2008 and 2010, a USTRANSCOM contractor [redacted] was compromised by the Chinese military who stole emails, documents, user accounts, passwords and even source code [redacted]

• [redacted]

(U) • ~~(S/NF)~~ [redacted] the Chinese military compromised the computer network of one of TRANSCOM's CRAF partners, stealing [redacted] documents, flight details, credentials and personal identification numbers and passwords for encrypted email.[43]

(U) • ~~(S/NF)~~ [redacted] the Chinese military compromised systems [redacted] The Chinese targeted [redacted] again later that year, exploiting [redacted]

[redacted]

[41] U.S. Transportation Command answers to committee questions (August 13, 2013).
[42] U.S. Transportation Command answers to committee questions (August 13, 2013)
[43] U.S. Transportation Command answers to committee questions (August 13, 2013).
[44] *Id.*
[45] *Id.*

(U) • ~~(S/NF)~~ [redacted] the Chinese military compromised "multiple systems" onboard a commercial ship contracted by TRANSCOM for logistics routes.[46]

• [redacted]

(U) • ~~(S/NF)~~ In 2013, [redacted] "PLA Spear-phishing campaigns targeting: commercial logistics partners that support USTRANSCOM operations in USCENTCOM AOR (particularly commercial sealift companies completing [redacted] trucking company [name]."[49]

(U) • ~~(S/NF)~~ [redacted] a CRAF airline was the victim of a phishing email which is suspected to have led to malware being downloaded.[50] The intrusion was attributed to the Chinese government.[51]

(U) These are just those intrusions of which TRANSCOM is aware. As described in Section II, between May 30, 2012 and August 15, 2013, there were at least 20 successful intrusions into TRANSCOM contractors that were attributed to advanced persistent threat actors. The term "advanced persistent threat" (APT) is used to distinguish sophisticated cyber threats from hackers or cyber criminals. While not limited to threats associated with foreign governments, the FBI has said "the sophistication, resources, and types of information sought [by APT actors] suggest governmental support."[52]

F. Cyber Information Sharing

(U) While TRANSCOM can monitor its own network for possible cyber intrusions, the command's knowledge of intrusions into the computer networks of private sector service providers depends on reporting from the contractors themselves, other DOD components, the FBI and other government agencies. That information sharing is critical to remediating compromises that could impact TRANSCOM operations and strengthening network defenses to keep potential adversaries at bay.

[redacted]

[50] Contractor response to committee questions (September 30, 2013).

[redacted]

[52] Federal Bureau of Investigation Private Sector Advisory (July 10, 2013).

(U) There are concerns about the amount of cyber threat information that the private sector shares with the government. According to General Dempsey:

> Right now, threat information runs primarily in one direction; from the government into the operators of critical infrastructure. Very little information flows back to the government.[53]

(U) There have been efforts to remedy that situation.

- (U) The Defense Cyber Crime Center (DC3), a center within the Air Force's Office of Special Investigations, stood up the Defense Industrial Base Cyber Security and Information Assurance (DIB CS/IA) Program.[54] Through the DIB CS/IA program, DOD contractors voluntarily report cyber intrusions they experience to DC3.

- (U) In 2010, TRANSCOM began including a clause in its contracts requiring contractors to report certain cyber intrusions.[55] (Those requirements are described in more detail in Section II.)

- (U) In July 2013, the Defense Security Service (DSS), a DOD component that acts as an interface between the government and cleared defense contractors, issued guidance requiring cleared defense contractors, some of which have contracts with TRANSCOM, to report certain cyber intrusions.

- (U) The Senate Armed Services Committee included a provision in the 2013 National Defense Authorization Act (NDAA) requiring cleared defense contractors to report certain cyber intrusions into their networks.

(U) These initiatives have increased the amount of information that private companies share with the government about cyber intrusions that affect private networks. However, as discussed in Section II, critical gaps remain.

(U) It is also crucial that the government agency that receives such reports shares them with the potentially affected military commands. That is particularly important when a compromise involves an advanced persistent threat such as a foreign government. Unfortunately, as discussed in Section II, intra-governmental information sharing about cyber intrusions affecting DOD contractors is lacking.

(U) Finally, it is important that the potential operational impacts of cyber intrusions into defense contractors be considered and that operational plans be adjusted, if appropriate, to

---

[53] General Martin E. Dempsey, The Brookings Institution (June 27, 2013)
[54] https://www.facebook.com/pages/DoD-Cyber-Crime-Center-DC3/176854735730162?id=176854735730162
[55] In 2010, TRANSCOM began including the clause in its information technology contracts and, in October 2012, began inserting the clause in its transportation contracts. U.S. TRANSCOM response to committee request for information (March 15, 2013).

mitigate the risk of a compromise affecting operations. TRANSCOM has said that the command would stand up a joint planning team (JPT) to consider the operational risk of an intrusion into a command contractor network that impacted TRANSCOM data but would not likely stand up a JPT if TRANSCOM data were not affected by a compromise.[56] As discussed in Section II, however, even in those cases where command data was unaffected, intrusions into the computer networks of operationally critical contractors could prove valuable to foreign governments as a source of intelligence about network operations or to establish a foothold in contractor networks, either of which could be exploited in a contingency.

[56] U.S. Transportation Command emails to committee staff (January 31, 2014, February 3, 2014).

II. SASC Inquiry

(U) In April 2013, the Senate Armed Services Committee initiated an inquiry into how much information was known to the U.S. Transportation Command (TRANSCOM) about successful cyber intrusions affecting the command's contractors. In the course of the inquiry, the committee reviewed information provided by TRANSCOM itself, 11 TRANSCOM contractors, the FBI, the Defense Security Service (DSS), the Defense Cyber Crime Center (DC3), and the U.S. Air Force Office of Special Investigations.

(U) The committee also reviewed TRANSCOM's cyber incident reporting requirement, cyber intrusion reporting provisions included in the Fiscal Year 2013 National Defense Authorization ACT (NDAA), and a number of executive branch guidelines, directives, and agreements to assess their impact on cyber threat information sharing.

(U) With respect to contractor cyber incident reporting, the committee found a lack of common understanding between TRANSCOM and its contractors as to the scope of cyber intrusions that must be reported. The committee also identified gaps both in contractual reporting requirements and in the law that leave TRANSCOM uninformed about successful compromises of contractor networks by advanced persistent threat (APT) actors, including foreign governments.

(U) As to intra-government information sharing, the committee found that TRANSCOM is frequently unaware of reports of cyber intrusions that have been identified by the government in the course of investigations or have been provided by contractors to the FBI or other DOD components. The reasons for TRANSCOM being unaware of intrusions affecting its contractors include a lack of common understanding between TRANSCOM and other DOD components about what cyber information TRANSCOM needs to know and misperceptions about the rules governing how cyber intrusion-related information identifying a particular victim may be shared.

A. Cyber Incident Reporting from TRANSCOM Contractors

(U) In 2010, TRANSCOM began including a clause in its information technology contracts requiring contractors to report certain cyber security incidents to TRANSCOM. In October 2012, the command expanded that requirement to its transportation contracts.[57] As of late 2012, more than 80 companies were subject to the cyber incident reporting clause as prime or subcontractors.[58]

(U) The cyber reporting clause requires companies to report any intrusion event that "affects DOD information resident on or transiting the contractor's unclassified information systems" and lists reportable cyber intrusions as those appearing to be an advanced persistent threat; intrusions involving the exfiltration, manipulation or loss of DOD data; or those allowing

[57] *Id.*
[58] U.S. Transportation Command list of contracts containing cyber incident reporting clause (April 30, 2013).

unauthorized access to an unclassified information system on which DOD information is resident or transiting.[59]

(U) Between October 2010, when TRANSCOM first began inserting the clause in its contracts, and August 2013, the command received only two reports of cyber intrusions directly from contractors subject to the clause.[60]

(U) ~~(S//NF)~~ The first of those was [redacted] report from a commercial transportation company relating to an intrusion that impacted computers located in Africa and China. [redacted] a contractor that supplies maritime shipping services reported that multiple computer systems had been compromised. [redacted] the intrusion was suspected to be the work of an APT [redacted] The company that submitted the report told the committee that it advised TRANSCOM of the incident even though the intrusion did not meet the reporting threshold in the company's contract with TRANSCOM.[62]

(U) The second of the two incidents reported to TRANSCOM affected a commercial airline that is a TRANSCOM Civil Reserve Air Fleet (CRAF) contractor. (The CRAF program is described in Section I.) The affected company advised the committee that the incident was not determined to be reportable under the company's contract with TRANSCOM but that they reported it anyway "out of an abundance of caution."[63]

(U) ~~(S//NF)~~ That intrusion was attributed to China.[64]

(U) That only two incidents were reported by TRANSCOM contractors contrasts with reports suggesting widespread targeting of private sector computer networks, including those of defense industrial base companies.

(U) In order to assess how companies were complying with TRANSCOM's clause, the committee requested information from 11 TRANSCOM contractors who are subject to the clause, about cyber intrusions they experienced in the first five months of 2013, and how they determined whether or not the intrusions were reportable. The 11 companies included six Civil Reserve Air Fleet (CRAF) contractors and three contractors who are participants in the Voluntary Intermodal Sealift Agreement (VISA) program. As discussed above, CRAF and VISA members provide essential capabilities for deploying and sustaining U.S. forces. The committee also sought information from two contractors that provide services to support TRANSCOM logistics systems.

---

[59] U.S. Transportation Command Cyber Security Incident Reporting Requirements (multiple dates).
[60] U.S. Transportation Command responses to committee requests for information (March 15, 2013, August 13, 2013).
[redacted]
[62] Email from TRANSCOM contractor to committee staff (December 2, 2013).
[63] Email from TRANSCOM contractor to committee staff (September 4, 2013).
[redacted]

1. Cyber Intrusions Known to TRANSCOM Contractors

(U) Of the 11 contractors from whom the committee sought information, eight said that they were not aware of any cyber intrusions affecting their networks between January 1, 2013 and June 10, 2013. The three remaining contractors, two of which provide information technology support and one of which was a CRAF contractor, identified a total of 31 intrusions during that period. The CRAF contractor also identified an additional intrusion that occurred later, in August 2013, bringing the total to 32 intrusions experienced by the three companies.

(U) One of the two information technology support contractors experienced 24 of the 32 intrusions. However, while the cyber incident reporting requirement was included in TRANSCOM's contract with the company, it was included as an option that TRANSCOM did not exercise.[65] As a result, the company did not report any of the 24 incidents to TRANSCOM. Nor did the company evaluate the incidents to determine whether they would have been reportable had they been subject to the requirement.[66] The company did report those intrusions deemed significant to the Defense Cyber Crime Center's (DC3) Defense Industrial Base Collaborative Information Sharing Environment (DCISE). DCISE is discussed in more detail below.

(U) The second of the two information technology support contractors identified four intrusions into their computer networks during the period in question. The company did not report any of the four intrusions to TRANSCOM. The company advised the committee that it interpreted the cyber incident reporting clause to only apply to intrusions affecting a single computer network operated by a subcontractor, an interpretation that appears inconsistent with the reporting clause's requirements and that TRANSCOM has subsequently said was not reasonable.[67] The company did report the intrusions to DC3's DCISE, though the company failed to do so for anywhere from four to nearly seven months after they were discovered.[68]

(U) The CRAF contractor advised the committee that it was also the victim of four intrusions, none of which it determined were reportable under TRANSCOM's reporting clause. The company, however, reported one of the four intrusions to the Defense Security Service (DSS) and provided the same report to TRANSCOM "out of an abundance of caution."[69]

2. Contractor-Identified Intrusions Attributed to Advanced Persistent Threat (APT) Actors

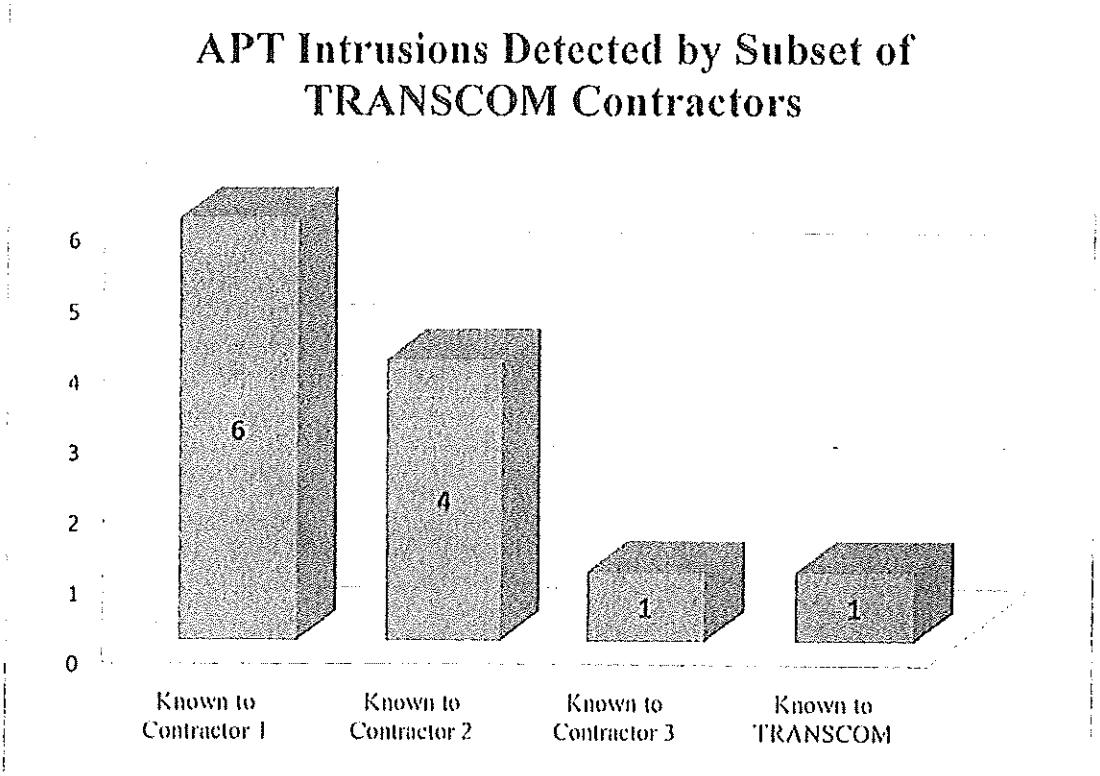
(U) As discussed above, foreign governments see military logistics networks and the deployment phase in contingency operations as potential U.S. vulnerabilities. As a result, it is

[65] Committee staff meeting with US TRANSCOM staff (November 25, 2013).
[66] Letter from contractor to Senator Carl Levin (July 2, 2013). The company reported that that the incidents "were mitigated and did not lead to the exfiltration (i.e., loss) of data and were isolated to a single device."
[67] Email from TRANSCOM contractor to committee staff (August 2, 2013); Committee staff meeting with U.S. Transportation Command (November 25, 2013).
[68] Contractor response to letter from Senator Carl Levin (November 7, 2013).
[69] Contractor responses to committee questions (July 9, 2013, September 4, 2013, September 30, 2013).

particularly important that TRANSCOM be aware of APT intrusions into the networks of companies who enable logistics and support contingency operations.

(U) As reflected in Chart 1, of the 32 intrusions reported to the committee by the three TRANSCOM contractors, 11 were determined by either DOD or FBI to be associated with an APT threat. The remaining 21 were determined not to be associated with an APT.[70] As discussed above, only one of the 11 intrusions associated with an APT was reported to TRANSCOM. That intrusion, however, was not determined by the victimized company to be reportable under the cyber incident reporting clause and was only reported in "an abundance of caution."[71]

Chart 1



(U) ~~(S//NF)~~ Of the 11 intrusions attributed to a known or suspected APT, all 11 were attributed to China.[72]

[70] Email from contractor to committee staff (September 13, 2013).
[71] Email from contractor to committee staff (September 4, 2013).

3. Cyber Incident Reporting Clause

(U) In addition to asking the TRANSCOM contractors to identify cyber intrusions, the committee also asked them how they determined whether or not the intrusions were reportable under the requirements of the cyber incident reporting clause contained in their contracts with TRANSCOM. The committee's analysis of contractor responses and the contract clause itself revealed that a lack of common understanding of contractor reporting obligations, the clause's limited scope, and some contractors' inability to distinguish APT from other cyber threats, limit the clause's effectiveness. The discussion below focuses on the 11 intrusions reflected in Chart 1 as having been attributed to an APT as those intrusions pose a particular threat to defense operations.

a. *Common understanding of reporting obligations is lacking*

(U) In 2010 TRANSCOM began including a clause in its contracts requiring contractors to report certain cyber security incidents.[73] The clause states:

> The contractor shall report...any suspected cyber intrusion events that affect DOD information resident or transiting the contractor's unclassified information systems... Reportable cyber intrusion events include the following:
>
> 1. A cyber intrusion event appearing to be an advanced persistent threat.
> 2. A cyber intrusion event involving data exfiltration or manipulation or other loss of any DOD information resident on or transiting the contractor's, or its subcontractors', unclassified information systems.
> 3. Intrusion activities that allow unauthorized access to an unclassified information system on which DOD information is resident or transiting.[74]

(U) While the first sentence in the clause refers to intrusions that "affect DOD *information*," TRANSCOM has said that it intended the clause to require contractors to report any intrusion that allow access to a *system* on which DOD information resides or is transiting.[75] However, none of the contractors with whom the committee discussed the clause interpreted their reporting obligation in a manner consistent with TRANSCOM's intent.

(U) One CRAF participant advised the committee that it interpreted the clause to require reporting of intrusions into their systems only if those intrusions affected DOD information, for example through data exfiltration or corruption.[76] Another CRAF contractor told the committee that the clause required reporting of cyber intrusions that affect nonpublic DOD information.[77]

---

[73] U.S. Transportation Command response to committee request for information (March 15, 2013).
[74] U.S. Transportation Command Cyber Security Incident Reporting Requirements (multiple dates).
[75] U.S. Transportation Command responses to committee request for information (September 23, 2013) (emphasis added).
[76] Contractor response to committee request for information (August 28, 2013).
[77] Contractor response to committee request for information (September 6, 2013).

(U) In any case, complying with the reporting clause depends on a contractor knowing the systems on which DOD information resides or transits. Given the extent to which information is exchanged electronically, contractors may not always know where all contract-related documents and information are held and what networks are used to exchange them. For example, one TRANSCOM prime contractor advised the committee that it subcontracted most contract tasks to another company. The prime contractor only considered intrusions into a computer network operated by that subcontractor as reportable.[78] In response to a committee request, however, the prime contractor found that contract deliverables were produced, circulated and maintained outside of that subcontractor network. In fact, the prime contractor found that contract-related documents were not only maintained on multiple subcontractor networks but were also maintained on the prime contractor's own systems.[79]

(U) Setting aside the lack of common understanding between the command and its contractors about the cyber incident reporting clause, TRANSCOM's own view that reportable intrusions are limited to those that affect systems on which DOD information resides or transits leaves a critical gap.

b. Clause language limits scope of reporting

(U) With respect to intrusions attributed to an APT, TRANSCOM has said that it intended the cyber incident reporting clause to "require contractors to report cyber intrusions that appear to be an APT, *and* that affect systems on which DOD information is residing or transits."[80] Requiring companies to report only those APT-attributed intrusions that affect systems on which DOD information is resident or transits at the time of the compromise risks the command being uninformed about intrusions that could affect future operations.

(U) For example, some commercial airlines that participate in the CRAF program may fly either no or only a small number of CRAF flights in peacetime.[81] Such airlines are likely to retain only a relatively small amount of DOD information in the normal course and the number of systems that information transits are likely similarly limited.[82] Under TRANSCOM's reporting clause, an intrusion into an airline computer network that is not storing or communicating DOD data at the time of the compromise is not reportable, even if the intrusion is extensive and linked to an advanced persistent threat such as a foreign government. Meanwhile, unbeknownst to TRANSCOM, the foreign government that perpetrated the intrusion could be performing reconnaissance or establishing a foothold in the compromised contractor's network, either of which could potentially be exploited to impact defense operations.

---

[78] Contractor response to committee request for information (August 2, 2013).
[79] Contractor response to committee request for information (August 30, 2013).
[80] According to TRANSCOM, the clause is limited to DOD information residing or transiting systems as a result of accomplishing the tasks in a company's contract. U.S. Transportation Command response to committee request for information (September 23, 2013). (emphasis added)
[81] U.S. Transportation Command, calendar year 2011 CRAF block hours (June 24, 2013).
[82] While all airlines that participate in the CRAF program have some DOD information on their systems, those airlines that fly few or no CRAF flights have significantly less. U.S. Transportation Command meeting with committee staff (November 25, 2013).

(U) In the event of a major contingency requiring the activation of CRAF Stage II or III, an airline's ability to support defense requirements might depend on the efficient functioning of computer networks that are normally reserved for commercial business. A prior compromise of such networks could be exploited to affect the airline and potentially TRANSCOM operations.

(U) To illustrate the limited scope of TRANSCOM's reporting clause, the committee reviewed the clause's applicability to certain CRAF airlines.

c. Analysis of cyber reporting clause gap

(U) As discussed above, the CRAF program was established to ensure DOD access to critical airlift capabilities in contingency operations. TRANSCOM calculates "Mobility Value Points" (MVP) to determine the value of aircraft that individual airlines commit to the CRAF program.[83] For example, total airline commitments to the international long-range passenger component of CRAF were valued at 9,000 MVP in calendar year 2011. The value of commitments made by individual airlines to that program ranged from zero to nearly 1,800 MVP per airline.[84]

(U) The committee's analysis indicates that more than 57 percent of the nearly 9,000 MVP for the 2011 international long-range passenger component of CRAF were assigned to airlines whose 2011 CRAF-related business, measured by block hours flown, composed less than 0.01 percent of their total business for that year. Because they flew few or no CRAF flights, it is likely that those companies received or retained only limited CRAF-related DOD information during that period. As discussed above, TRANSCOM's cyber incident reporting clause extends only to intrusions that affect systems on which DOD information resides or transits as a result of the company accomplishing CRAF-related tasks. As such, the number of systems implicated by the reporting clause for companies who flew few or no CRAF-related flights in 2011 was likely very small.

(U) This gap in the scope of intrusions that defense contractors are required to report is not limited to TRANSCOM's reporting clause. The information sharing provision that the committee included in the 2013 National Defense Authorization Act is similarly limited. The NDAA provision requires DOD to establish procedures requiring cleared defense contractors[85] to report when a network or information system is successfully penetrated. However, the reporting requirement applies only to networks or information systems that "contain[] or process[] information created by or for the Department of Defense with respect to which such contractor is required to apply enhanced protection."[86]

---

[83] U.S. Transportation Command paper, "Calculation of Mobility Value Points" (May 7, 2013).
[84] U.S. Transportation Command, Planned CRAF Fleet Data MV Point Summary (July 20, 2013).
[85] The law defines "cleared defense contractor" as a private entity granted clearance by DOD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any DOD program. There are more than 10,000 cleared defense contractors.
[86] National Defense Authorization Act for Fiscal Year 2013 Sec. 941 (e)(2).

(U) While the NDAA provision can be expected to advance information sharing about cyber intrusions that result in the theft or manipulation of certain DOD information residing on contractor systems, it is not clear that it will increase contractor reporting about intrusions into commercial networks, like those of companies in the CRAF program, that may not typically contain or process DOD information. Further, the NDAA provision limits reportable intrusions to those that affect DOD information to which a contractor is required to apply "enhanced protection." It seems unlikely that intrusions affecting information maintained by a contractor in the course of conducting their commercial business would fall within the scope of the law's reporting requirement. As described above, however, even networks that typically conduct commercial business and process little or no DOD information may be critical to military operations in the event of a contingency.

(U) The NDAA provision is further limiting in that, even when a contractor does report a cyber intrusion, it explicitly prohibits the report's dissemination outside the DOD, unless that dissemination is approved by the contractor that submitted the report.[87] That prohibition could impede the efficient flow of time-sensitive information relating to cyber intrusions to other government agencies such as the FBI or other components of the Intelligence Community.

d. Ability to Identify TRANSCOM-Defined Advanced Persistent Threat

(U) Among reportable events listed in TRANSCOM's cyber incident reporting clause are intrusions appearing to be an advanced persistent threat (APT). The contract clause defines an APT as "an extremely proficient, patient, determined, and capable adversary, including two or more adversaries working together."[88] The committee's review found that contractors are not always able to determine whether an intrusion is APT-related, or meets TRANSCOM's definition.[89]

(U) According to one TRANSCOM contractor, after reporting an intrusion to government, the company was advised verbally by the FBI that the intrusion was APT-related. However, the contractor told the committee that they "were not able to confirm that the incident met the definition of APT specified in [the company's] contract with USTRANSCOM."[90] Another contractor told the committee that, with respect to four intrusions they experienced, indicators of compromise "did not provide sufficient evidence to enable [the company] to conclude whether the attack was or was not APT related."[91] (The Department of Defense subsequently advised the committee that the intrusions at issue were APT-related.[92])

---

[87] Id at Sec. 941 (c)(3).
[88] U.S. Transportation Command Cyber Security Incident Reporting Requirements (multiple dates).
[89] The same company may have an obligation to report cyber intrusions to multiple DOD components and it is worth noting that there is no DOD-wide definition of APT. For example, DSS's definition of APT differs from that used by the DC3 and TRANSCOM.
[90] Contractor response to committee staff questions (September 30, 2013).
[91] Email from contractor to committee staff (September 13, 2013).
[92] Email from Office of Secretary of Defense, Legislative Affairs (November 8, 2013).

B. Intra-Governmental Information Sharing

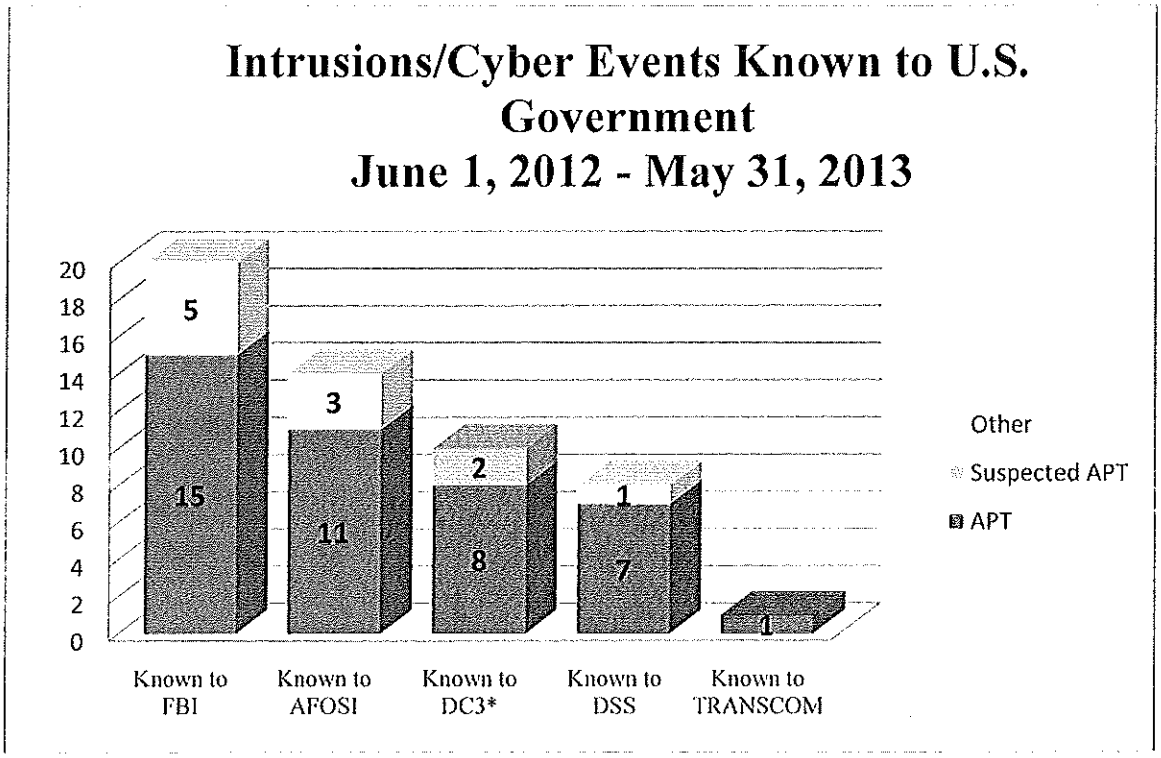
(U) As discussed in Section I, some private sector network compromises have the potential to impact defense operations. Increasing the amount of cyber threat information that the private sector shares with the government is critical to mitigating such threats. However, improving the flow of cyber threat information for the private sector will not, on its own, solve the problem. Timely *intra-governmental* information sharing about private sector network compromises is also critical, particularly when network compromises involve an APT threat such as a foreign government.

(U) To assess the state of intra-government information sharing, the committee sought information from U.S. Transportation Command, the FBI, the Defense Security Service (DSS), the Defense Cyber Crime Center (DC3), and the Air Force Office of Special Investigations about cyber intrusions experienced by 79 TRANSCOM contractors, how information about those intrusions was shared within the government, and how current law, agency practices and preexisting agreements with defense contractors impact information sharing.

(U) As reflected in Chart 2, the committee found that TRANSCOM is frequently unaware of reports of cyber intrusions that have been identified by other DOD components and government agencies. The reasons for that include a lack of common understanding between TRANSCOM and other DOD components about what cyber information TRANSCOM needs to know and misperceptions about the rules governing how cyber intrusion-related information that identifies a particular victim may be shared.

(U) Chart 2 reflects agency responses and depicts cyber intrusions between June 1, 2012 and May 30, 2013 that affected contractors subject to TRANSCOM's cyber incident reporting clause.

Chart 2



** DC3 categorizes intrusions as "probable" or "suspected" APT.*

(U) Chart 2 reflects at least 20[93] successful intrusions or other cyber events[94] targeting TRANSCOM contractors over the one year period. Of those 20, at least 15 were associated with an APT, and at least nine of those 15 were successful intrusions of a contractor network. TRANSCOM was aware of only one of those nine.[95]

1. Federal Bureau of Investigation

(U) During the course of its investigations, the FBI may learn that a U.S. company has been the victim of a cyber-intrusion. In such cases, the FBI typically notifies the victimized company. If the company is a defense contractor, that notification may be coordinated with DOD's Defense Security Service (DSS), a DOD component that acts as an interface between the government and cleared defense contractors.

[93] The total number of intrusions known across the government cannot be determined. Though each AFOSI identified intrusion corresponded with an FBI identified intrusion, neither DSS, nor the DC3 was able to determine whether intrusions known to the FBI corresponded to intrusions of which either DSS or DC3 was aware.

[94] Cyber events include incidents that may not be confirmed successful intrusions but which the FBI determined that a victim notification was warranted.

[95] A second intrusion was reported to TRANSCOM by a commercial transportation company in February 2013. The company that made the report, however, told the committee that the incident affected an affiliated company that was not among the 79 identified by the committee.

a. Cyber Intrusions of TRANSCOM Contractors Known to the FBI

(U) The committee provided the FBI a list of 79 TRANSCOM contractors and subcontractors subject to the cyber incident reporting requirement and asked the Bureau to identify how many were notified between June 1, 2012 and May 30, 2013 that they were the victim of a cyber-intrusion.

(U) In response, the FBI told the committee that it notified 16 contractors on the list that they were victims of a cyber-intrusion or other cyber events during the period in question.[96] The FBI notified four of those 16 companies of two discrete events each, bringing the total number of cyber intrusions or other events known to FBI and affecting companies of the list of TRANSCOM contractors to 20.[97]

(U) ~~(S)~~ Of the 16 targeted companies identified by the FBI, six were airlines, two were shipping companies, and eight were providers of technical services and other support to enable TRANSCOM operations.[98] As discussed in Section I, DOD relies on commercial airlines and shipping companies to meet military requirements in contingencies.

(U) Of the 20 total events, FBI advised the committee that 15 appeared to be associated with an Advanced Persistent Threat (APT) actor.[99] Nine of those 15 were successful intrusions of a TRANSCOM contractor. TRANSCOM was only aware of one of those.[100]

(U) ~~(S)~~ FBI attributed all those 15 APT-linked events, including all nine successful intrusions, to China.[101]

b. FBI Information Sharing

(U) ~~(FOUO)~~ Information sharing between the FBI and DOD, including information relating to counterintelligence, counterterrorism, and foreign intelligence, is governed by a Memorandum of Understanding (MOU) signed by the Attorney General and the Secretary of Defense in 2011.[102] An annex to that MOU that includes procedures for sharing counterintelligence information and specifically addresses cyber threat information sharing states:

---

[96] In a small number of cases, the FBI's discussions with the targeted company were initiated by the company.
[97] Letter from Federal Bureau of Investigation Assistant Director, Cyber Division to Senator Carl Levin (August 29, 2013).
[98] U.S. Transportation Command response to committee questions (December 20, 2013).
[99] Federal Bureau of Investigation Cyber Division email to committee staff (September 16, 2013); A July 2013 FBI advisory describes APT threats. "Advanced persistent threat actors differ from common hackers or cyber criminals by conducting targeted, rather than opportunistic, attacks that seek precise information rather than monetary gain, more closely resembling espionage. While the activity cannot often be definitively linked to any particular nation state, the sophistication, resources, and types of information sought suggests governmental support." Federal Bureau of Investigation Cyber Division Private Sector Advisory (July 10, 2013).
[100] U.S. Transportation Command response to committee request (December 20, 2013).
[redacted]
[102] Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Attorney General and the Secretary of Defense on June 24, 2011 and August 2, 2011, respectively).

> When FBI investigations, including assessments, collect any information which indicates that a DOD organization or a contractor providing services to a DOD organization has been targeted by a foreign power using the cyber domain, the FBI will report this to DOD in accordance with the procedures identified in paragraph 5 below. The FBI shall provide information needed by DOD to effectively assess the impact of the intrusion on DOD operations and to defend against the intrusion activity. Thereafter, DOD will coordinate all investigative and operational activity with the FBI.[103]

(U) ~~(FOUO)~~ In cases where the FBI knows that an identified victim of a cyber intrusion is a DOD contractor, information sharing procedures contained in the annex state that FBI will report DOD-related counterintelligence information to the Defense Counterintelligence and Human Intelligence Center (DCHC) and the Military Department Counterintelligence Investigative Organization (MDCO) "if specific military service affiliation is known" and to DCHC alone if it is not.[104] The Air Force is the Executive Agent[105] for TRANSCOM and the Air Force Office of Special Investigations (AFOSI) is the Air Force MDCO.

(U) The information sharing procedures also state that FBI will report counterintelligence information to DCHC and the Defense Security Service (DSS) "if the information pertains to a cleared DOD contractor."[106]

(U) According to DSS, there are approximately 10,000 cleared contractors.[107] The FBI Cyber Division has said that they are in the process of integrating the full list of cleared contractors into their information-sharing database so they will be better able to determine when an identified victim is a DOD contractor. However, even in cases where the FBI knows that a company compromised by a cyber intrusion is a defense contractor, the Bureau may not be aware which DOD component does business with the victimized contractor. No DOD component has provided the FBI with a list identifying specific operationally critical contractors about whom they would like to be informed when they were the victim of a cyber intrusion.[108] On January

---

[103] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 4.

[104] *Id.* at 5.

[105] Executive Agent is the "Head of a DOD component to whom the Secretary of defense or the deputy Secretary of defense has assigned specific responsibilities, functions, and authorities to provide defined levels of support for operational missions, or administrative or other designative activities that involve two or more of the DOD components." Department of Defense Directive 5101.1 (September 3, 2002) at 2.

[106] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 5.

[107] Email from Defense Security Service Office of Public and Legislative Affairs to committee staff (January 8, 2014).

[108] Committee staff meeting with Federal Bureau of Investigation Cyber Division (December 19, 2013).

30, 2014 TRANSCOM provided the FBI with a list of 80 companies. That list, however, included all command contractors who are subject to TRANSCOM's cyber incident reporting clause and did not identify which of the 80 are operationally critical contractors.[109]

(U) ~~(FOUO)~~ The MOU annex states that FBI "will report DOD-related cyber [counterintelligence] investigation information" to MDCOs and DSS by notifying personnel detailed from those agencies to the National Cyber Investigative Joint Task Force (NCIJTF).[110] NCIJTF is the focal point for government agencies to share information about cyber threat investigations and the FBI is the lead agency.[111] In addition to DSS and AFOSI, several other DOD components are members of the NCIJTF, including the Naval Criminal Investigative Service (NCIS), the Defense Cyber Crime Center (DC3), U.S. Cyber Command (CYBERCOM), and the Defense Intelligence Agency (DIA).

(U) The FBI could not determine whether each of the 15 intrusions and other events targeting TRANSCOM contractors and attributed to an APT was shared with AFOSI or DSS through NCIJTF or other channels. However, as discussed below, while DSS was unable to determine how many of the 15 FBI-identified APT intrusions and other events they were aware of, AFOSI has said they were aware of 11.[112] The FBI is transitioning to a new computer system called Cyber Guardian that will allow it to better record and track information about cyber intrusions. NCIJTF members have direct access to FBI cyber incident reporting through the Cyber Guardian system.[113]

(U) ~~(FOUO)~~ DSS, the MDCOs, and DCHC may share FBI counterintelligence information within their own organizations. However, the FBI-DOD MOU annex stipulates that the Bureau must approve those agencies providing that information to other DOD components.[114] As stated above, TRANSCOM was aware of one FBI-identified intrusion which was reported directly to the command by the contractor.[115]

---

[109] Email from U.S. Transportation Command to committee staff (February 4, 2014).

[110] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 5.

[111] FBI web site, *National Cyber Investigative Joint Task Force*, http://www.fbi.gov/about-us/investigate/cyber/ncijtf

[112] Email from U.S. Air Force to committee staff (January 9, 2014). Information later provided to the committee raised the possibility that AFOSI may have been aware of one additional event. The committee was unable to confirm that.

[113] Letter from Federal Bureau of Investigation Assistant Director, Cyber Division, to Senator Carl Levin (August 29, 2013). The FBI operates the NCIJTF, which is responsible for coordinating U.S. government information related to domestic cyber threat investigations.

[114] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 5.

[115] U.S. Transportation Command response to committee request (December 20, 2013); Contractor email to committee staff (December 2, 2013).

(U) According to the FBI Cyber Division neither DSS nor AFOSI requested approval to share victim identity information with TRANSCOM relating to any of the cyber intrusions affecting a TRANSCOM contractor and attributed to an APT.[116]

2. Defense Security Service

(U) The Defense Security Service (DSS) oversees cleared defense contractor facilities to ensure that classified information is protected. In a 2013 report to Congress, DSS stated that in 2012 it "began personal outreach to the cleared contractors to emphasize the requirement to report suspicious contacts, *including cyber incidents*."[117] In July 2013, DSS issued an Industrial Security Letter (ISL) describing cyber incident reporting requirements for cleared defense contractors. The ISL states:

> Although this requirement is not directed to unclassified information or systems, contractors must report [to DSS] activities that otherwise meet the threshold for reporting,[118] *including activities that may have occurred on its unclassified information systems.*[119]

(U) In addition to reports of cyber intrusions that the agency receives directly from cleared defense contractors, DSS also receives reports of cyber intrusions from the FBI. As discussed above, the FBI and DSS frequently coordinate efforts to notify victims of cyber attacks that they have been compromised and DSS is designated by an FBI-DOD information-sharing MOU to receive FBI counterintelligence information, including information relating to cyber intrusions, if the information pertains to a cleared DOD contractor.[120]

a. Cyber incidents known to DSS

(U) As discussed above, the FBI identified 20 intrusions or other cyber events targeting 16 of 79 TRANSCOM contractors. The committee asked DSS to review those 20 events and identify how many of which the agency was aware.

---

[116] Committee staff meeting with Federal Bureau of Investigation Cyber Division (December 19, 2013).
[117] U.S. Department of Defense Biennial Report to Congress on Improving Industrial Security (February 2013) at 29 (emphasis added).
[118] The ISL states that a cyber intrusion may fall under the reporting requirements of the National Industrial Security Program Operating Manual (NISPOM) paragraph 1-301, "regardless of the classification level of information or information system involved in the intrusion, provided that the contractor has determined that (i) the facts and circumstances of the intrusion are sufficient to qualify as 'actual, probable or possible espionage, sabotage, terrorism, or subversive activities' and (ii) these activities constitute a threat to the protection of classified information, information systems, or programs that are otherwise covered by the NISPOM." Defense Security Service, Industrial Security Letter 2013-05 (July 2, 2013) (emphasis added).
[119] *Id.* (emphasis added).
[120] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 5.

(U) While DSS frequently coordinates with the FBI to notify victims of cyber intrusions, the agency was only able to confirm awareness of eight intrusions into FBI-identified victims during the period in question. However, DSS's records are not complete and the agency may have been made aware of additional intrusions about which it was unable to identify records.[121] Further, while the eight intrusions affected *companies* that were among those identified by the FBI as victims of a cyber-intrusion, DSS was unable to determine how many of the eight *intrusions* actually correspond to intrusions identified by the FBI.[122]

(U) Of the eight confirmed intrusions DSS identified, seven were attributed to an APT.[123] TRANSCOM was not aware of any of those seven.[124]

(U) ~~(S//NF)~~ All seven of the intrusions known to DSS and associated with an APT were attributed to China.[125]

b. DSS information sharing

(U) DSS's charter states that the agency may disseminate reports of suspicious contacts or activities in accordance with Department of Defense Procedures Governing the Activities of DOD Intelligence Components That Affect U.S. Persons.[126] Those procedures permit the sharing of lawfully obtained foreign intelligence information, including for example, that a U.S. company was the victim of an APT-related cyber intrusion, outside the DOD component that collected and retained the information, provided that the recipient "is reasonably believed to have a need to receive such information for the performance of a lawful governmental function" and falls into one of several categories, including DOD employees that have a need to know the information.[127]

(U) As discussed above, under the FBI-DOD Memorandum of Understanding DSS must seek FBI approval to share Bureau-supplied counterintelligence information, including information indicating cyber compromise of a DOD contractor, with DOD components that are not members of the NCIJTF.[128]

---

[121] Committee staff call with Defense Security Service (November 7, 2013).
[122] Defense Security Service response to committee staff questions (October 22, 2013).
[123] *Id.*
[124] U.S. Transportation Command response to committee request (January 9, 2014).
[125] Committee staff call with Defense Security Service (November 6, 2013).
[126] DSS's charter also states that the agency will "Collaborate with the DOD components, other [U.S. Government] departments and agencies, and cleared contractors to share threat information as part of the Defense Industrial Base Cyber Security and Information Assurance Program" The DIB CS/IA program is operated by DC3. Department of Defense Directive 5105.42 (August 3, 2010) at 4.
[127] Department of Defense Procedures Governing the Activities of DOD Intelligence Components That Affect U.S. Persons (December 1982) at 22.
[128] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 5.

(U) When DSS receives a report that a cleared defense contractor's computer network has been compromised, it memorializes the incident in a suspicious contact report (SCR). It is DSS practice to share SCRs at the NCIJTF with all DOD and FBI components represented.[129] As discussed above, several DOD components are members of the NCIJTF, including AFOSI, the Naval Criminal Investigative Service (NCIS), the Defense Cyber Crime Center (DC3), U.S. Cyber Command (CYBERCOM), and the Defense Intelligence Agency (DIA).[130]

(U) DSS may also circulate SCRs through "letterhead memoranda" (LHM). LHM may be sent to the FBI and military service investigative units, e.g. AFOSI. LHM are typically prepared in DSS field offices and shared with local FBI and service investigative counterparts in the field. They are sometimes shared with counterpart headquarter offices.[131] DSS determines what agencies should be copied on LHM based on a number of factors, including an assessment of who has jurisdiction over the issue and which DOD component has a nexus to the victimized company through a contractual relationship or otherwise.[132]

(U) DSS told the committee that available records indicated that the agency was aware of eight intrusions affecting TRANSCOM contractors. That number could be higher, however, as DSS records are incomplete. DSS was unable to determine how many suspicious contact reports associated with the eight intrusions were shared at the NCIJTF. However, DSS records indicate that the agency produced letterhead memoranda for four of those eight intrusions. Three of those four LHM were sent to the AFOSI. DSS records do not indicate whether the three LHMs were shared through headquarters offices or were only shared between field offices.[133]

3. Air Force Office of Special Investigations

(U) The Air Force Office of Special Investigations (AFOSI) is the Air Force's investigative service and is responsible for criminal and counterintelligence investigations, including those related to cyber intrusions. The Air Force is also the Executive Agent for TRANSCOM. AFOSI may learn of cyber intrusions through its own investigations. According to AFOSI, the agency always notifies the FBI of such intrusions so that the Bureau can conduct victim notifications.[134]

a. Cyber Intrusions of TRANSCOM Contractors known to AFOSI

(U) The committee asked AFOSI to review the 20 intrusions and other cyber events targeting TRANSCOM contractors that the FBI identified and indicate how many were known to

[129] Committee staff call with Defense Security Service (November 7, 2013).
[130] Federal Bureau of Investigation email to committee staff (November 19, 2013).
[131] Committee staff call with Defense Security Service (November 7, 2013).
[132] Committee staff call with Defense Security Service (November 7, 2013); Committee staff meeting with Defense Security Service (September 26, 2013).
[133] Committee staff call with Defense Security Service (November 7, 2013).
[134] Committee staff meeting with Air Force Office of Special Investigations (December 3, 2013).

AFOSI. AFOSI advised the committee that it was aware of 13 of the 20.[135] Of those 13, 11 were attributed to an APT.[136] TRANSCOM was aware of only one of those 11.[137]

(U) ~~(S)~~ According to AFOSI, of the 11 intrusions and other cyber events targeting TRANSCOM contractors that were known to AFOSI and associated with an APT, nine were attributed to China. [redacted]

b. AFOSI Information Sharing

(U) ~~(FOUO)~~ Because the Air Force is the Executive Agent for TRANSCOM, AFOSI is the relevant military department counterintelligence organization designated by the FBI-DOD information-sharing MOU to receive information identified by the Bureau indicating that a TRANSCOM contractor was the victim of an APT-related cyber intrusion.[139]

(U) While available FBI records do not indicate how many of the 15 intrusions and other cyber events targeting TRANSCOM contractors and attributed to an APT were shared with AFOSI, AFOSI itself reports that it was made aware of 11 of those 15.[140]

(U) When AFOSI receives a report of a cyber intrusion involving a private company, (such reports can come from one of several sources, including the FBI, DSS, the victimized company, or AFOSI's own investigations) the agency determines whether or not the information needs to be shared with other Air Force components based on its judgment as to the potential impact of the compromise.[141]

(U) ~~(FOUO)~~ Under the FBI-DOD MOU, AFOSI may only share FBI counterintelligence information outside their organization with the FBI's approval.[142] AFOSI must also comply with Department of Defense Procedures Governing the Activities of DOD Intelligence Components That Affect U.S. Persons.[143] Those procedures permit the sharing of lawfully obtained foreign

---

[135] Email from U.S. Air Force to committee staff (December 23, 2013).
[136] Email from U.S. Air Force to committee staff (January 9, 2014).
[137] U.S. Transportation Command response to committee questions (August 13, 2013).
[138] Committee staff call with U.S. Air Force
[139] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 5.
[140] Email from U.S. Air Force to committee staff (January 9, 2014).
[141] Committee staff meeting with U.S. Air Force Office of Special Investigations (December 3, 2013).
[142] Annex B, Counterintelligence Investigative Information Sharing, to the Memorandum of Understanding between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities (signed by the Executive Assistant Director, National Security Branch, Federal Bureau of Investigation and Under Secretary of Defense for Intelligence on December 9, 2011 and December 7, 2011, respectively) at 5.
[143] DSS's charter also states that the agency will "Collaborate with the DOD components, other [U.S. Government] departments and agencies, and cleared contractors to share threat information as part of the Defense Industrial Base

intelligence information outside the DOD component that collected and retained the information, provided that the recipient "is reasonably believed to have a need to receive such information for the performance of a lawful governmental function" and falls into one of several categories, including DOD employees that have a need to know the information.[144]

(U) As discussed in Section I, computer networks that support defense logistics and mobilization are seen as potential U.S. vulnerabilities in cyberspace. However, AFOSI did not request approval to share information with TRANSCOM relating to any of cyber intrusions the FBI identified as having affected a TRANSCOM contractor and attributed to an APT.[145] Nor had TRANSCOM provided AFOSI with a list of operationally critical contractors or requested that they be informed about cyber intrusions of specific contractors.[146] On January 30, 2014, TRANSCOM provided AFOSI a list of 80 companies. That list, however, included all command contractors who are subject to TRANSCOM's cyber incident reporting clause and did not identify which of the 80 are operationally critical contractors.[147]

(U) As to why it did not seek to share information with TRANSCOM relating to the intrusions of which it was aware, AFOSI told the committee that:

> [I]nvestigative actions on each incident were dependent on the level of DOD nexus. In the majority of these situations, the reporting only described spearphishing[148] activity and did not indicate why the victim was being targeted... Without the clear DOD/Air Force nexus, OSI prioritized our investigative and operational response based on priority threats, and available resources."[149]

(U) In the end, TRANSCOM was only aware of one of the 11 APT-related intrusions and other cyber events of which AFOSI was aware.[150]

4. Defense Cyber Crime Center

(U) The Defense Cyber Crime Center (DC3) is a national center within the Air Force's Office of Special Investigations (AFOSI) that provides training, cyber forensics, analytics and computer network defense to DOD and other government agencies. DC3 also operates the

---

cyber security and information assurance program" The DIB CS/IA program is operated by DC3. Department of Defense Directive 5105.42 (August 3, 2010) at 4.

[144] Department of Defense Procedures Governing the Activities of DOD Intelligence Components That Affect U.S. Persons (December 1982) at 22.

[145] Committee staff meeting with Federal Bureau of Investigation Cyber Division (December 19, 2013).

[146] Email from TRANSCOM to committee staff (January 31, 2014).

[147] U.S. Transportation Command email to committee staff (January 31, 2014).

[148] "Spearphishing" involves the use of official looking emails tailored for sending to a targeted individual or group of individuals. Spearphishing emails often use official looking attachments that, when opened by a recipient, allow the sender to compromise the targeted victim's computer. Spearphishing emails are a common tactic of APT actors. *See e.g.* Trend Micro Incorporated research paper *Spear-Phishing Email: Most Favored APT Attack Bait* (2012).

[149] Email from U.S. Air Force to committee staff (December 23, 2013).

[150] U.S. Transportation Command response to committee request (August 13, 2013).

Defense Industrial Base Cyber Security and Information Assurance (DIB CS/IA) Program.[151] DOD contractors who are members of the DIB CS/IA program sign a "Framework Agreement" with DOD where they agree to voluntarily report certain cyber intrusions they experience to the Defense Industrial Base Collaborative Information Sharing Environment (DCISE). [152] DCISE, in turn, analyzes those reports, helps develop responses, and disseminates threat information derived from the reports within the government and to other participating DIB CS/IA companies. As of December 2013, there were 98 companies in the DIB CS/IA program.

a. Cyber Intrusions of TRANSCOM Contractors Known to DC3

(U) The committee requested information from DC3 about 79 TRANSCOM contractors subject to the cyber incident reporting clause. Of those 79 TRANSCOM contractors, nine were members of the DIB CS/IA program for at least some portion of the period between June 1, 2012 and May 30, 2013.[153] During that period, seven of those nine companies reported a total of 146 "incidents" to DC3.[154] Among those 146 incidents were ten successful intrusions involving a network on which DOD information was stored. Those ten successful intrusions impacted six companies.[155]

(U) Each of the six companies who were the victims of intrusions was also represented on the list of 16 companies that the FBI identified as having been the victim of an intrusion or other cyber event during that same period. However, DC3 was unable to determine whether FBI-identified incidents corresponded with incidents reported to DC3 by those same companies.[156]

(U) Eight of the 10 intrusions known to DC3 and involving a network on which DOD information was stored were determined to be "probable" APT intrusions. The remaining two were deemed "suspected" APT.[157] TRANSCOM was aware of only one of those 10 intrusions.[158]

(U) ~~(S/NF)~~ All eight of the intrusions DC3 determined to be probable APT were attributed to China.[159]

---

[151] https://www.facebook.com/pages/DoD-Cyber-Crime-Center-DC3/176854735730162?id=176854735730162
[152] Defense Industrial Base Cyber Security/Information Assurance, "Framework Agreement" (undated);
[153] A tenth company joined the program in September 2013. Defense Cyber Crime Center response to committee staff questions (October 9, 2013).
[154] Included as "incident" are successful intrusions, attempts, denial of service attacks, or anomalies that a DIB CS/IA member may choose to report. Email from Office of the Secretary of Defense Legislative Affairs to committee staff (October 22, 2013).
[155] Defense Cyber Crime Center response to committee staff questions (October 9, 2013).
[156] Email from Office of the Secretary of Defense Legislative Affairs to committee staff (November 12, 2013).
[157] The latter two intrusions were suspected of being associated with an APT but did not meet DC3's analytical threshold for a "probable" APT. Defense Cyber Crime Center response to committee staff questions (October 22, 2013).
[158] Email from contractor to committee staff (December 2, 2013).
[159] Committee staff call with Office of the Secretary of Defense Legislative Affairs (August 22, 2013).

(U) The timely sharing of information about cyber intrusions is critical for the DOD to keep pace with the evolving cyber threat environment and to ensure DOD is aware of any compromise that could impact military operations. To that end, the DCISE Framework Agreement states that members of the DIB CS/IA program "will provide initial reports to DC3/DCISE within 72 hours of discovery or as soon as reasonably practicable."[160] The committee found, however, that companies do not always report intrusions consistent with the Framework Agreement. In fact, one TRANSCOM contractor who was member of the DIB CS/IA program reported intrusions to DC3 anywhere from four to nearly seven months after the company discovered them.[161]

b. DCISE Framework Agreement

(U) Under terms of the DCISE Framework Agreement, contractors are required to report cyber incidents involving the compromise or potential compromise of certain unclassified defense information on an information system "that processes, stores, or transmits" such information.[162] If an intrusion does not involve the compromise or potential compromise of DOD information or such systems, the DIB CS/IA company is not obligated to report the event.[163] In that respect, the agreement contains a similar limitation to TRANSCOM's cyber incident reporting clause, i.e. companies that may not currently store or process DOD information but on whom TRANSCOM operations depend do not have to report certain intrusions -- even when those intrusions are associated with an APT threat.

c. DC3 Information Sharing

(U) The DCISE Framework Agreement outlines the terms under which information reported by contractors may be shared outside DC3/DCISE.

(U) Under the Agreement, DC3 may share information, other than the identity of the victimized company, with other companies who are members of the DIB CS/IA and with other government agencies. It states that identifying information will be maintained at DC3 "to the maximum extent practicable" and that such information will be made available on a need-to-know basis and upon the submission by a government agency of a written request and justification.[164]

(U) According to TRANSCOM, because intelligence products, such as those produced from contractor reports to DCISE, do not normally include the identity of the company that has been compromised, it is difficult for the command to determine whether a compromise is relevant to the TRANSCOM mission. The inability to make such a determination makes it difficult for the command to know when it should request the identity of a victimized company and also to justify such requests. TRANSCOM advised the committee that it has not requested

[160] Defense Industrial Base Cyber Security/Information Assurance, "Framework Agreement" (undated);
[161] Contractor response to letter from Senator Carl Levin (November 7, 2013).
[162] Defense Industrial Base Cyber Security/Information Assurance, "Framework Agreement" (undated) at 2.
[163] Defense Cyber Crime Center response to committee questions (October 22, 2013).
[164] Defense Industrial Base Cyber Security/Information Assurance, "Framework Agreement" (undated).

information from DC3 that would have identified the identity of a company who was the victim of a cyber intrusion.[165]

(U) The DCISE Framework Agreement also states, however, that "none of the restrictions on the Government's use or sharing of information in this [Framework Agreement] shall limit the Government's ability to conduct law enforcement or [counterintelligence activities], or other activities in the interest of national security."[166] DOD advised the committee that the exception articulated in that section of the Framework Agreement provides authority for DC3 to share the identity of a victimized company when a national security interest was at stake. As of February 1, 2014 TRANSCOM had not submitted a list of operationally critical contractors to DC3 or requested that the command be notified about cyber intrusions into such companies.[167] On January 30, 2014, TRANSCOM provided the FBI and AFOSI a list of 80 companies. That list, however, included all command contractors who are subject to TRANSCOM's cyber incident reporting clause and did not identify which of the 80 are operationally critical contractors.[168]

[165] Committee staff meeting with U.S. Transportation Command (November 25, 2013).
[166] Defense Industrial Base Cyber Security/Information Assurance, "Framework Agreement" (undated) at 12.
[167] Committee staff meeting with Defense Cyber Crime Center, Office of the Deputy Assistant Secretary of Defense for Cyber Policy, and Office of the Department of Defense Chief Information Officer (December 16, 2013).
[168] Email from U.S. Transportation Command to committee staff (January 31, 2014).

Committee Action

(U) On Wednesday March 26, 2014, by voice vote, the committee adopted the report and conclusions of the inquiry into cyber intrusions affecting U.S. Transportation Command contractors. Twenty senators were present. No senator voted in the negative.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu