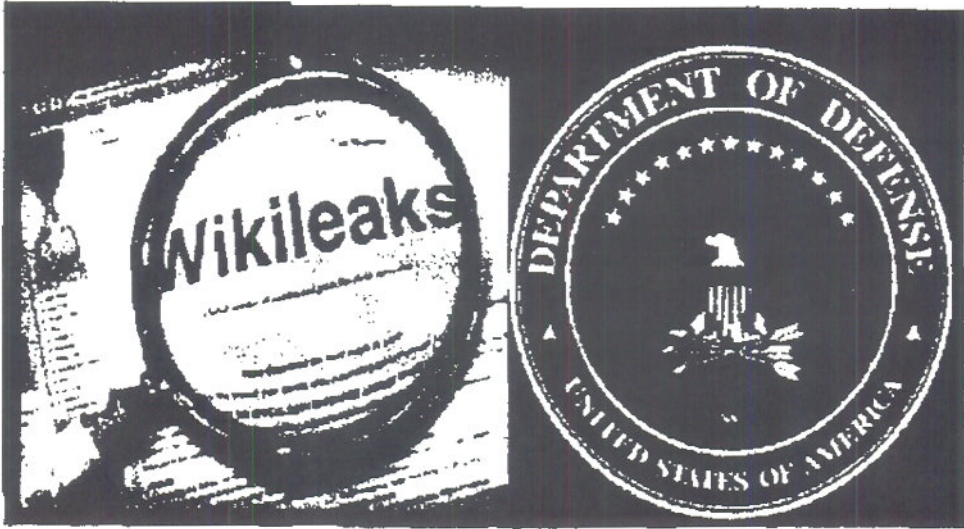


**(U) Final Report of the
Department of Defense Information Review Task Force**

June 15, 2011

20110615



(U) Information Review Task Force

(b)(3):10 USC 424

Defense Intelligence Agency

Derived from: DoDI C-5240.8
Reason: (b)(3)
Declassify on: 204005

(U) Final Report of the Department of Defense Information Review Task Force

(U) Table of Contents

(U) Executive Summary	3
(U) Introduction.....	8
(U) Data Sets and Review Process.....	10
(U) Chapter 1 (RTF Summary Report – Afghanistan Data Set).....	14
(U) Chapter 2 (RTF Summary Report – Iraq Data Set).....	34
(U) Chapter 3 (Joint Task Force – Guantanamo Records).....	58
(U) Chapter 4 (RTF Summary Report – Net Centric Diplomacy Data Set).....	72
(U) Chapter 5 (RTF Summary Report – ACIC Special Report).....	97
(U) Chapter 6 (RTF Summary Report – Gerani Airstrike).....	99
(U) Chapter 7 (RTF Summary Report – Baghdad Airstrike).....	101
(U) Conclusion.....	103
(U) Appendix A – Secretary of Defense (RTF) Memorandum.....	104
(U) Appendix B – General Background Information on WikiLeaks.....	106
(U) Appendix C – Foreign Nation Impact Chart.....	107
(U) Appendix D – Derogatory Information on Foreign Governments.....	108
(U) Appendix E – Index of Compromised JTF-Guantanamo Records Other than Detainee Assessments.....	112
(U) Appendix F – RTF-Produced Country Information Memorandums.....	114
(U) Cable Citations.....	115

(U) Final Report of the Department of Defense Information Review Task Force

(U) Executive Summary

(U) At the direction of the U.S. Secretary of Defense (SecDef), the Information Review Task Force (IRTF) assessed the impact of unauthorized WikiLeaks disclosure of United States Government (USG) records. The IRTF completed a comprehensive review of more than 740,000 records known or believed compromised to WikiLeaks, coordinated its review throughout the Intelligence Community (IC), and integrated its efforts with those of the National Counterintelligence Executive (NCIX).

(U) Given the enormity of the challenge, the IRTF reached out and received tremendous support from not only the affected Department of Defense (DoD) Components but also from the multiple affected federal departments and agencies as well. This whole-of-government approach, together with close coordination with the appropriate legal and foreign disclosure officials, enabled the IRTF to get ahead of the WikiLeaks public releases and to inform senior leaders and policymakers across the USG as well as coalition governments prior to public disclosure so that mitigation actions could be taken.

(U) *Overall Summary of Impact:* The IRTF reviewed compromised data sets using criteria established by the SecDef (see Appendix A). After a comprehensive review, the IRTF assessed the greatest impact to the following DoD equities:

- (U) Lives of cooperative Afghans, Iraqis, and other foreign interlocutors are at increased risk

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (c),1.4 (d)



~~SECRET//NOFORN~~

(b)(1),(b)(3):10 USC 424, 1.4 (a), 1.4 (c), 1.4 (d)

- ~~(U//FOUO)~~ Personally identifiable information (PII) concerning 23 U.S. military personnel, including full names and social security numbers. All affected individuals were notified.

(b)(1),(b)(3):10 USC 424, 1.4 (a), 1.4 (c), 1.4 (d)

~~SECRET//NOFORN~~

(U) Due to the sheer volume of information the IRTF reviewed, this report focuses on the most significant findings centered on the seven key focus areas, a general overview of what was learned, and selected examples and summaries of relevant reports to provide context.

(U) This report, along with associated analytical assessments and other IRTF products, is posted on the [redacted]

(b)(3):10 USC 424

(U) Interagency Collaboration

(U) ~~(FOUO)~~ The IRTF brought together representatives from over 20 agencies in the intelligence, law enforcement, and diplomatic communities (Figure 1) for the conduct of this review. The support of these partners was critical to timely completion of the Task Force's work.

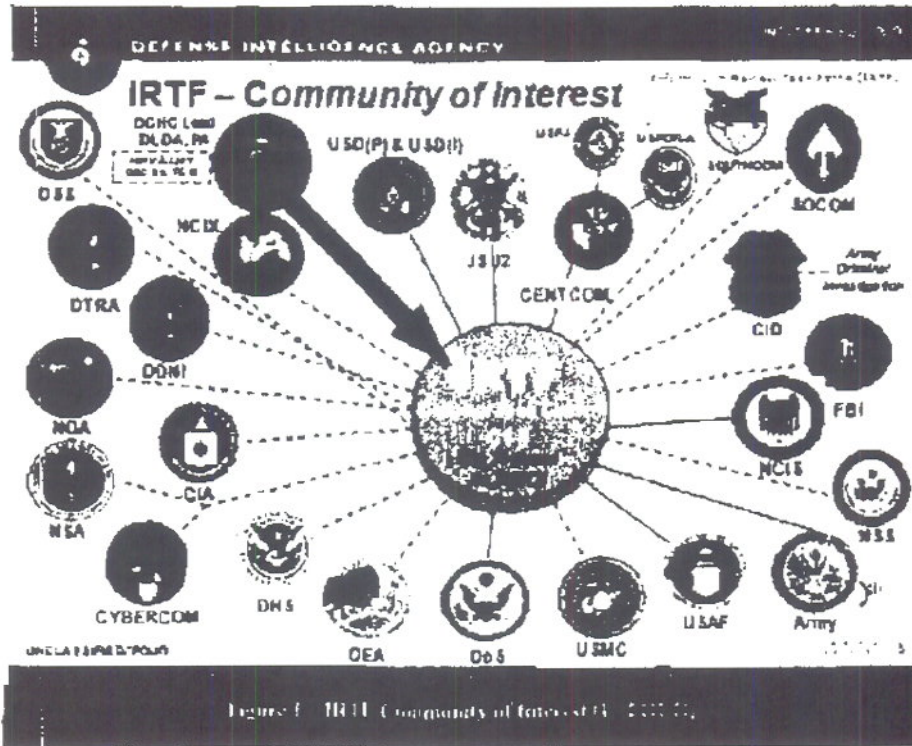


Figure 1. IRTF Community of Interest (U) (FOUO)

(U) Final Report of the Department of Defense Information Review Task Force

(U) Data Sets and Review Process

(U//~~FOUO~~) The compromised data encompasses four large data sets containing information up to the SECRET//NOFORN level. The IRTF reviewed this compromised information in its entirety, and a description of each of these data sets and the associated review process is outlined below. In addition, the IRTF reviewed two airstrike videos and an ACIC report also known to have been obtained by WikiLeaks.

(U) The Afghan Data Set

(U//~~FOUO~~) The 76,911 (76K) and 14,821 (15K) tactical reports downloaded from the USCENTCOM [redacted] contain information classified up to the SECRET//NOFORN level. The database contains detailed significant activity (SIGACT) reports and is the designated SIGACT reporting tool of record in the USCENTCOM area of responsibility (AOR). The compromised reports are dated between January 1, 2004, and December 31, 2009. The [redacted] reports contain the reporting unit designator as well as information on such event types as enemy action, explosive hazard, friendly action, detainee operations, friendly fire, counter-insurgency, and threat reports (Figure 2). WikiLeaks has not yet released the full text of the 15K data due to criticism that the release of "sensitive" threat report data could place the lives of innocent civilians at risk; however, several news organizations have included information from this data in their news reporting.

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

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

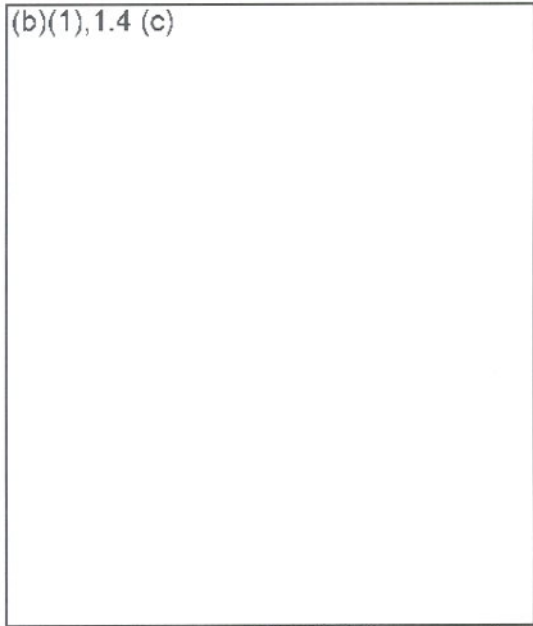
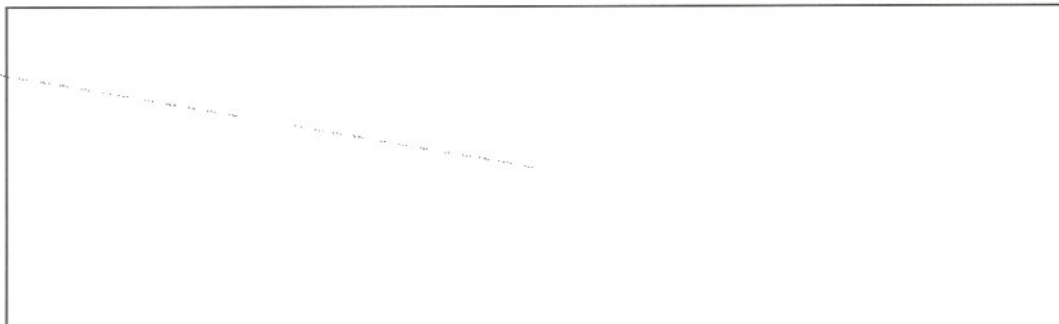


Figure 2. CIDNE-A Data Sets (SI)

- (S) (b)(3):10 USC 424 [redacted] 76K data set: 76,911 SIGACT and threat reports from USCENTCOM's CIDNE-A database covering the January 1, 2004, to December 31, 2009, timeframe and posted to the WikiLeaks website on July 25, 2010.



(b)(1),(b)(3):10
USC 424.1.4
(a),1.4 (c)



(U) The Iraq Data Set

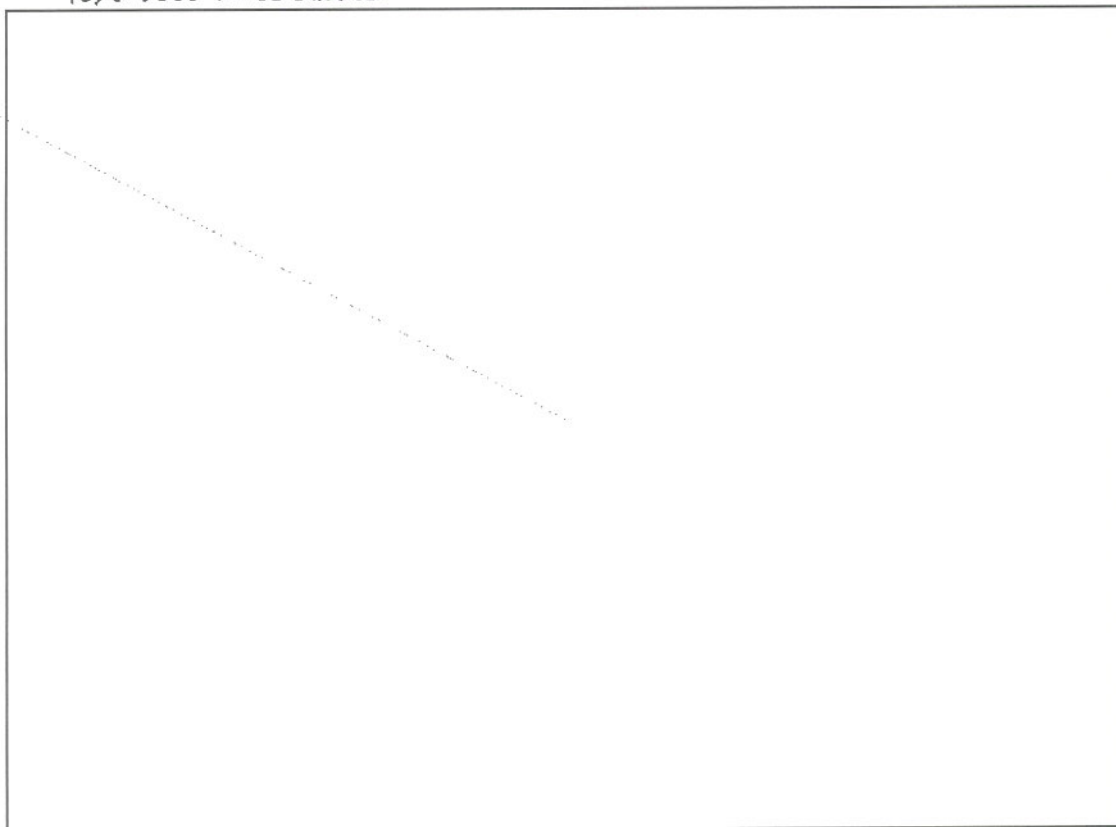
(b)(3):50 USC
3024(i)

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

~~(U//FOUO)~~ Using a combination of analytic concepts and technical means, the IRTF conducted a review of approximately 409,000 [redacted] records produced from November 1, 2003, to May 27, 2010, hereafter referred to as the Iraq data set. These reports are very similar in type and format to the [redacted] reports described above. At the time of the initial review, the IRTF was unsure how many of the 409,000 records were in WikiLeaks' possession; however, we now assess with high confidence that only 391,832 reports dated through December 31, 2009, were compromised. All reports are tactical in nature and contain information classified up to the SECRET//NOFORN level.

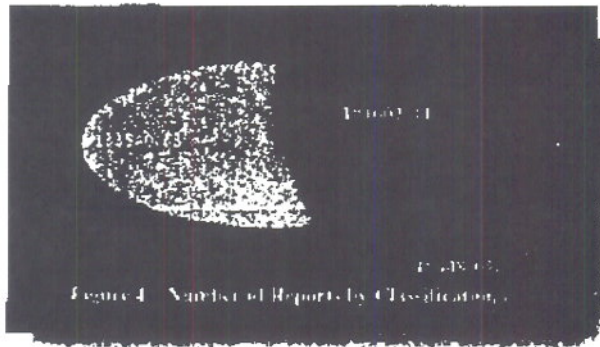
(U) The JTF-GTMO Data Set

(b)(1),1.4
(a),1.4 (c)



(U) The NCD Data Set

(U//FOUO) WikiLeaks has a total of 251,287 DoS cables classified up to the SECRET//NOFORN level and has begun releasing them into the public domain. The release contains some reporting from as early as 1966; however, the bulk of the reporting is from 2002 to February 28, 2010.

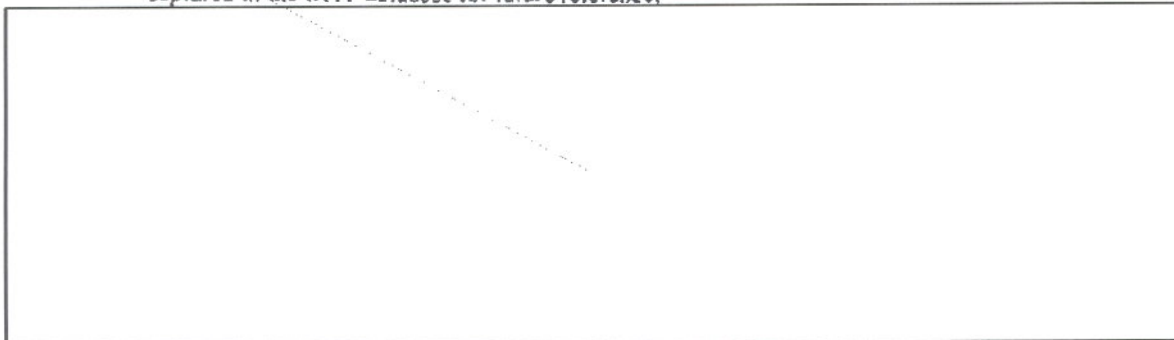


~~(S//NF)~~ The compromised diplomatic cables are derived from the DoS NCD database. NCD is a program that promotes information sharing and supports the interagency information requirements of cleared USG personnel in the foreign affairs and national security communities. NCD brings together information from more than 200 diplomatic posts and contains copies of cables, e-mails without attachments, and webforms. Unless specifically labeled otherwise, content in NCD is not releasable to foreign nationals. Some webforms and e-mails available in the database, such as Political-Military Action Team (PMAT) reports, have not been compromised.

(U) The Review Process

(b)(1), 1.4
(a), 1.4 (c)

(U) The IRTF used search engines to initially triage, sort, and categorize the reports in each data set. This allowed IRTF analysts to focus their initial efforts on reports with a high probability of yielding information relevant to one of the key SecDef focus areas. Once the initial triage of information was completed, analysts began a line-by-line review of every report within that data set. Each report received a two-tier review. The first-tier review, conducted by analysts aided by an automated checklist, captured significant findings and passed the information to a senior analyst for a tier two review. All significant reporting was identified, placed in context, and captured in the IRTF database for future reference.



(b)(1), 1.4 (a), 1.4 (c), 1.4 (d)

(U) Additional Data

(U) WikiLeaks also posted a 1.4 gigabyte (GB) encrypted file to the "Afghan War Diary, 2004-2010" webpage, which is labeled "insurance file." Minimal information about this file is disclosed on the website, other than "name: insurance.aes256" and "type: unknown file type, 1.3nGB." It appears to be encrypted with AES-256, a publicly available symmetric-key encryption standard.³ This file is publicly available for download in its encrypted form, but WikiLeaks has not released the key/password required to read its contents. Numerous websites have confirmed that they have downloaded the "insurance file" and are awaiting the release of the password to unlock its contents. Julian Assange, an Australian who is described in open source reporting as WikiLeaks' founder, publicly insists he can release the key to the public at any time that he feels his continued ability to disseminate the compromised information is at risk. Based on public statements by Assange, the IRTF assesses with moderate confidence that the "Insurance File" does not contain any additional USG data beyond that which the IRTF has already reviewed.

³ (U) AES-256: Advanced Encryption System (AES) that uses a 256-bit encryption key (password).

Chapter One

(U) IRTF Summary Report – Afghanistan Data Set

(U) Background

(U) On July 25, 2010, at 1700 hours Eastern Daylight Time (EDT), the WikiLeaks organization released 76,911 Government reports to the general public through its website, WikiLeaks.org (dedicated webpage at <http://wardiary.wikileaks.org>). WikiLeaks refers to these documents as the "Afghan War Diary."⁴ The 76,911 SIGACTs released by WikiLeaks on July 25, 2010, cover the period January 1, 2004, to December 31, 2009. They originated from USCENTCOM's [redacted] which resides on Secret Internet Protocol Router Network (SIPRNET). The posted documents were not redacted or altered by WikiLeaks.

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

(U) At the time, WikiLeaks also claimed to have approximately 15,000 additional reports it would not post to its website until they had undergone a "harm minimization process" review. WikiLeaks advised that "After further review, these [15,000] reports will be released, with occasional redactions, and eventually in full, as the security situation in Afghanistan permits." As of June 2011, these reports have been reported on and released in a limited form by a handful of select WikiLeaks media partners. IRTF maintains high confidence that these 14,821 reports withheld by WikiLeaks are a subset of the same [redacted] data set described above.

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

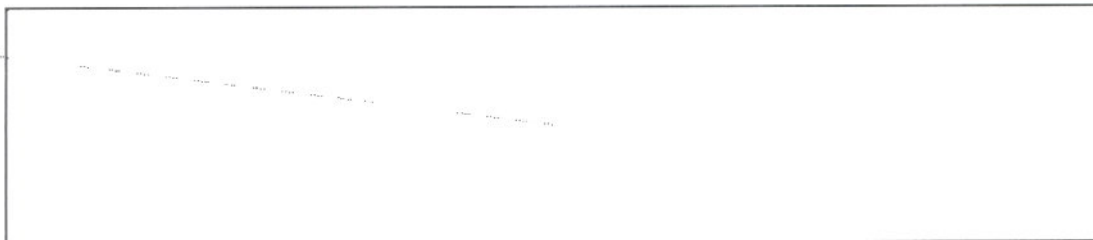
(U) The WikiLeaks website provided access to the Afghan data in a variety of formats, including HTML (web), CSV (comma-separated values), SQL (database), and KML (Keyhole Markup Language) geospatial data that can be used with visualization tools such as Google Earth.

(U) Prior to the July 25, 2010, public posting of reports from [redacted] WikiLeaks provided *The New York Times*, *Der Spiegel*, and *The Guardian* copies of the 76,911 reports subsequently posted online, along with the remaining approximately 15,000 reports. Each of these media outlets has used this information in their reporting and posted a small number of redacted reports beyond what is available on the WikiLeaks website. In addition, in early April 2011, Denmark's *Dagbladet Information* began a series of reports based on 14,821 reports that IRTF assesses with high confidence are the remaining [redacted] reports that WikiLeaks had held back. *Dagbladet Information* claims to have received these from WikiLeaks and has posted only metadata and associated metrics rather than the full text of these reports.

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

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

(b)(1),1.4
(a),1.4 (c)



~~SECRET//NOFORN~~

(U) Key Findings

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c)

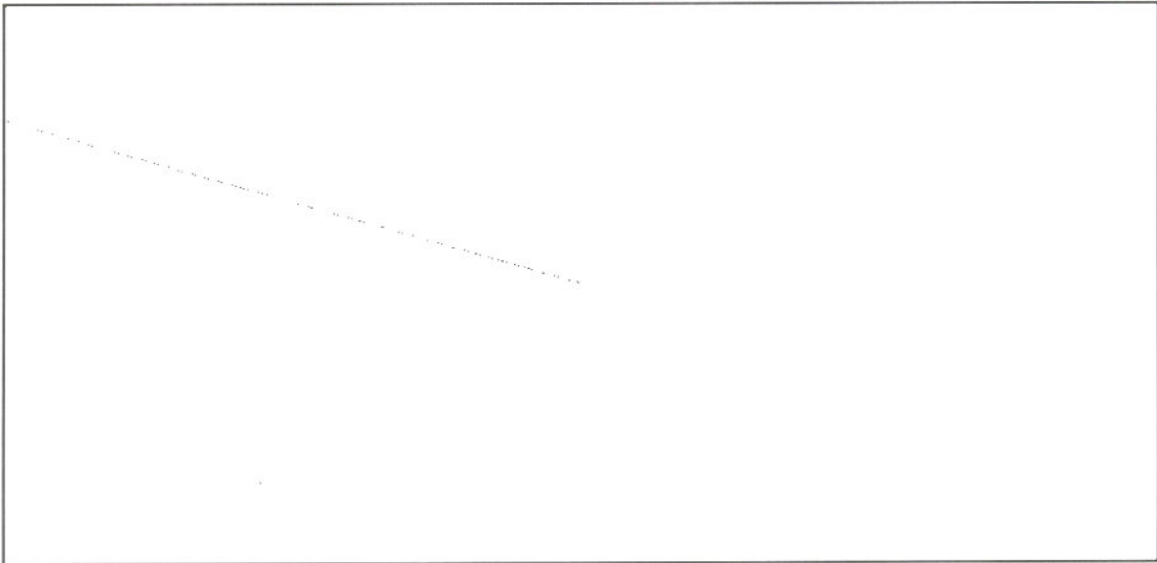
- (U//~~FOUO~~) PII concerning 23 U.S. soldiers, including full names and social security numbers. All affected individuals have been notified.

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c)

~~SECRET//NOFORN~~

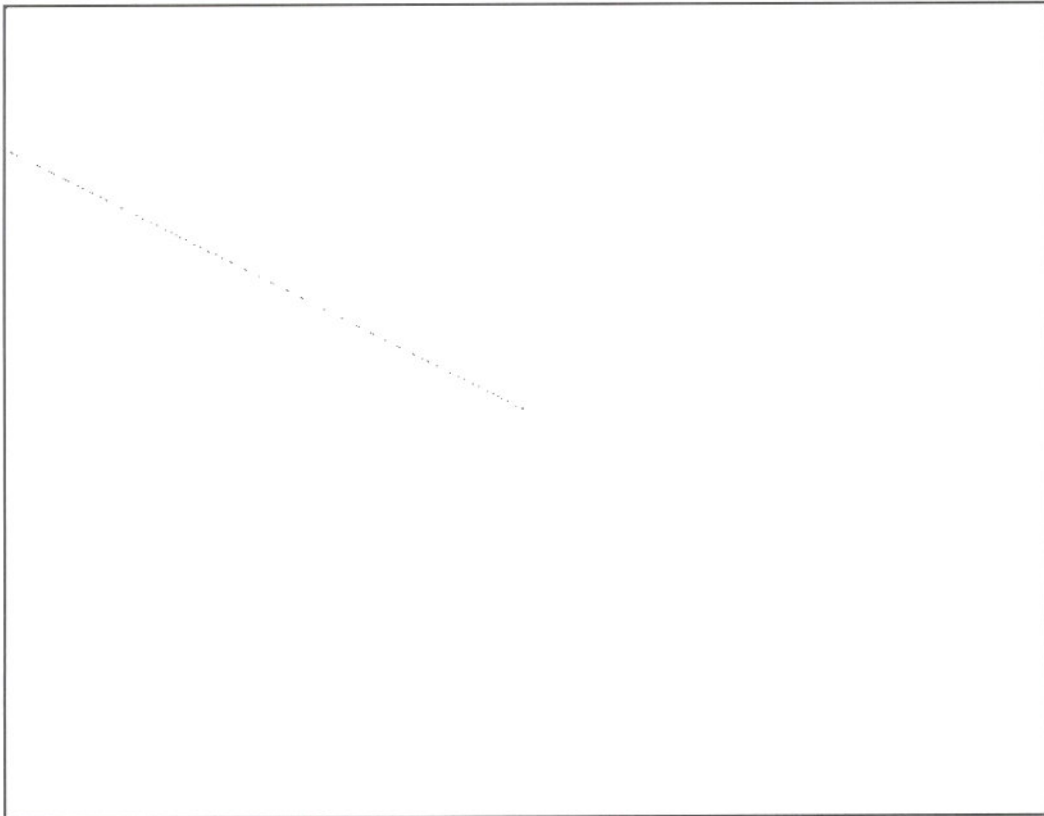
~~SECRET//NOFORN~~

(b)(1),1.4
(a),1.4
(c),1.4 (d)



(U) Unreleased Documents in the 15K Data Set: Four reports in the 15K data set are deemed to be of minimal significance.

(b)(1),1.4 (a),1.4
(c),1.4 (d)



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(3):50
USC 3024

(U) The IRTF, with the assistance of USCENTCOM, NSA, NGA, and CIA, reviewed the Afghanistan [redacted] for information concerning intelligence sources and methods. This review yielded HUMINT, SIGINT, and GEOINT capabilities, reporting, and TTP. This information has been divided into three categories: 1) Human Sources and Methods, 2) SIGINT, and 3) GEOINT. Although the IRTF assesses there is not any significant "strategic impact" to the release of this information, there is the potential for serious damage in two critical areas: 1) risks to intelligence sources, informants, and the Afghan population, and 2) U.S./NATO SIGINT collection methods and capabilities.

(1) Human Sources and Methods

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

(b)(3):50
USC 3024

(U) Selected examples of [redacted] disclosing cooperative local national names:

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

~~SECRET//NOFORN~~

(b)(1),(b)(3):10
USC 424,1.4
(a),1.4 (c),1.4 (d)

(b)(3):10
USC 424

~~SECRET//NOFORN~~

[Redacted]

- (S) [Redacted] Additional SIGINT reporting in early August revealed that an insurgent leader ordered Internet documents pertaining to Coalition operations in Afghanistan distributed among subordinate elements.

(b)(3):10
USC 424

- (S) [Redacted] A Jihadist website posted a link to a British newspaper article "Afghanistan: The War Logs" which offers readers [Redacted]

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

I think we have a moral obligation, not only to our troops but to those who have worked with us. And as we go through these documents and identify people who have helped us, it seems to me we have an obligation to take some responsibility for their security.

— Robert Gates, Secretary of Defense, July 29, 2010

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

[Redacted]

~~SECRET//NOFORN~~

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

(U) GEOINT Sources and Methods

(U//~~FOUO~~) NGA analyzed 147 Google Earth documents posted to the WikiLeaks website that depict the location and event for reports in the 76K data set. These Google Earth files, commonly called KML, include one file with all of the 76K records. The remaining 146 files contain subsets of the 76K data that portray various themes selected by WikiLeaks, such as: direct fire, indirect fire, explosive hazards, mines found and cleared, IEDs, and others.

(U//~~FOUO~~) The KML documents posted to WikiLeaks containing classified SIGACT reporting were likely created using third-party software by the WikiLeaks staff, as they are not structured in the same manner as the KML files that are available for download via the CIDNE database on SIPRNET. Additionally, the parallels between the spreadsheets and KML files posted to WikiLeaks suggest that the WikiLeaks staff likely derived the WikiLeaks-posted KML files from the spreadsheets in order to provide a visual representation of the data.

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c),1.4 (d)

~~SECRET//NOFORN~~

(b)(1),(b)(5),1.4 (a),1.4 (c)

~~(U//FOUO)~~ Civilian Casualties Not Previously Reported

(U) The IRTF used keyword searches to identify civilian casualties within the data sets. The search for casualties also encompassed serious injuries to civilians. Reports revealing in-depth details were searched and compared against open-source reporting.

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c),1.4 (d)

(U) The following two summaries are of reports not found in open source that could be used by the press or our adversaries to negatively impact support for current operations in the region:

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (b),1.4 (c),1.4 (d)

(U) Cultural Impact

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c),1.4 (d)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Chapter Two

(U) IRTF Summary Report – Iraq Data Set

(U) Background

(U) On October 22, 2010, at 1700 EDT, the WikiLeaks organization released 391,832 government records to the general public through its website; WikiLeaks.org (dedicated webpage at <http://wardiary.wikileaks.org>). Prior to the October 22 public posting of reports from WikiLeaks provided *The New York Times*, *Der Spiegel*, *Al Jazeera*, and *The Guardian* complete un-redacted copies of these reports in early August. Each of the media outlets has selectively used this information in their reporting

(b)(3):50
USC 3024

(b)(3):50
USC 3024

(b)(1),(b)(3):10 USC 424, 1.4 (a), 1.4 (c), 1.4 (d)

(U) Key Findings

(b)(1),(b)(3):10 USC 424, 1.4 (a), 1.4 (c), 1.4 (d), 1.4 (g)

~~SECRET//NOFORN~~

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

(U) Analytical Assessments

(b)(3):10 USC 424 The following IRTF analytical assessments, organized by seven key focus areas, are based on the results of an initial keyword search, followed by an in-depth, "line-by-line" review of each report in the Iraq data set.

(U) Force Protection Implications

(U) The IRTF's review for force protection implications resulted in three categories of reporting: *U.S. Persons PII*, *Current and Previous Senior U.S. Leadership in Iraq*, and *Special Operations Forces Identifying Unit Information*. Summaries and assessments of the corresponding data are addressed below.

(U) U.S. Persons PII

(b)(1),(b)(3):10 USC 424,(b)(6),1.4 (a),1.4 (c),1.4 (d)

(U) Enemy Inflicted Deaths

(b)(1),(b)(3):10 USC 424,(b)(6),1.4 (a),1.4 (c),1.4 (d)

- ~~(b)(3):10 USC 424,(b)~~ Another report includes significant details of an IED incident resulting in a vehicle commander's death and another seriously wounded member receiving burns covering 90 percent of his body.

(U) Accidental Death

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

- (U) Self-Inflicted GSW:

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

- (U) Fratricide Incidents:

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

- (U) Other Causes:

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

~~SECRET//NOFORN~~

(U) Murder

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c),1.4 (d)

(U) Current and Former Senior U.S. Leadership in Iraq

(U//FOUO) The IRTF searched the Iraq data set for reports containing references to current and former senior U.S. leadership in Iraq. The IRTF found two reports with references to, or comments by, General David H. Petraeus, and one report with reference to General Ricardo Sanchez. None of the reports are damaging in any way.

(U//FOUO) **IRTF Assessment:** The IRTF assesses with high confidence that disclosure of the Iraq data set will have no direct personal impact on current and former senior U.S. leadership in Iraq.

(U) Identifying Unit Information: Special Operations Forces (SOF)

(b)(1),1.4
(a),1.4
(c),1.4 (d)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1),(b)(3);10 USC 424,(b)(5),1.4 (a),1.4 (c),1.4 (d)

¹⁴ (U) On July 16, 2010, the U.S. Court of Appeals for the District of Columbia directed the U.S. Secretary of State to further review the MeK designation as a Foreign Terrorist Organization, since due process of the law was violated during the State Department's previous decision to maintain the MeK's designated status.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c),1.4 (d)

¹² ~~(U//FOUO)~~ The Sol program includes coalitions of tribal sheikhs that unite to maintain security. Funded by the United States, the Sol program has been criticized by Government of Iraq leaders as a separate military force.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Chapter Three

(U) Joint Task Force – Guantanamo Records

(U) Background

(U) On April 25, 2011 at 1700 EDT, the WikiLeaks organization, through a series of international media outlets, began releasing Guantanamo detainee files to the general public. By April 28, 2011, a total of 769 compromised JTF-GTMO documents were posted to the WikiLeaks website (<http://wikileaks.org/gtmo>). Prior to the public posting of reports from JTF-GTMO, WikiLeaks provided complete un-redacted copies of these reports to 10 media outlets, including *The Washington Post*, *The Telegraph*, *Der Spiegel*, *Le Monde*, *El Pais*, the *McClatchy Company*, and several others. *The New York Times*, *National Public Radio*, and *The Guardian* also acquired the JTF-GTMO data independently from a separate source, likely formerly associated with WikiLeaks.

(b)(1),(b)(3):10 USC 424,1.4 (a),1.4 (c),1.4 (d)

(U) Key Findings

(b)(1),1.4
(a),1.4
(c),1.4 (d)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Chapter Four

(U) IRTF Summary Report -- Net Centric Diplomacy Data Set

(U) Background

(U//~~FOUO~~) On November 28, 2010, the WikiLeaks organization released 243 DoS cables from the NCD database to the general public through the WikiLeaks website. WikiLeaks had provided *The New York Times*, *Der Spiegel*, *The Guardian*, *Le Monde*, and *El Pais* complete, un-redacted copies of these reports in advance. Each of these media outlets has selectively used this information in their initial reporting, which has included concerns about the Iranian nuclear program, information on historical events (e.g., Nelson Mandela's release, Iran hostages, and Manuel Noriega), biographies (e.g., Qaddafi, Mugabe, Ahmed and Wali Karzai), information on domestic politics (e.g., Germany and Turkey), information on Yemen CT operations, legal analysis of the Honduran coup, North Korean missile concerns, information on sanctions against Iran, and procedures for walk-in/defector handling. As of June 10, 2011, WikiLeaks and its global partners have released more than 14,600 of 251,287 records from the NCD.

(U//~~FOUO~~) Based on information being publicly released by WikiLeaks and its media partners, the IRTF has confirmed that as many as 251,287 cables from the DoS NCD database have been compromised, with an information cutoff date of February 28, 2010. WikiLeaks has stated that "[t]he embassy cables will be released in stages over the next few months. The subject matter of these cables is of such importance, and the geographical spread so broad, that to do otherwise would not do this material justice."

(U) Key Findings

(b)(1),(b)(5), 1.4 (a), 1.4 (c), 1.4 (d)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Analytical Assessments

(U) The following IRTF analytical assessments, organized by focus areas, are based on the results of an initial keyword search, followed by an in-depth, line-by-line review of each report in the NCD data set.

(U) Force Protection Implications

(b)(1),(b)(5),1.4 (a),1.4 (d)

(U) U.S. Persons Identifying Information

(b)(3):10
USC 424.(b)
(3).50 USC
3024(i)

(U) Force Dispositions and Vulnerabilities

(b)(1),1.4 (a),1.4 (c),1.4 (d)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

b)(1),(b)(5),1.4 (a),1.4 (c)



(U) Current Operations or Military Plans

(b)(1),1.4
(a),1.4 (c)



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Chapter Five

(U) IRTF Summary Report – ACIC Special Report

(b)(1),(b)(5),1.4 (a),1.4 (c),1.4 (d)

- ~~(S//FOUO)~~ WikiLeaks founder Julian Assange views the ACIC report as a “declaration of war,” based on a June 2010 interview with *The New Yorker*, which may serve as motivation for further releases.

(b)(1),1.4 (a),1.4 (c),1.4 (d)

(U) Data Characterization

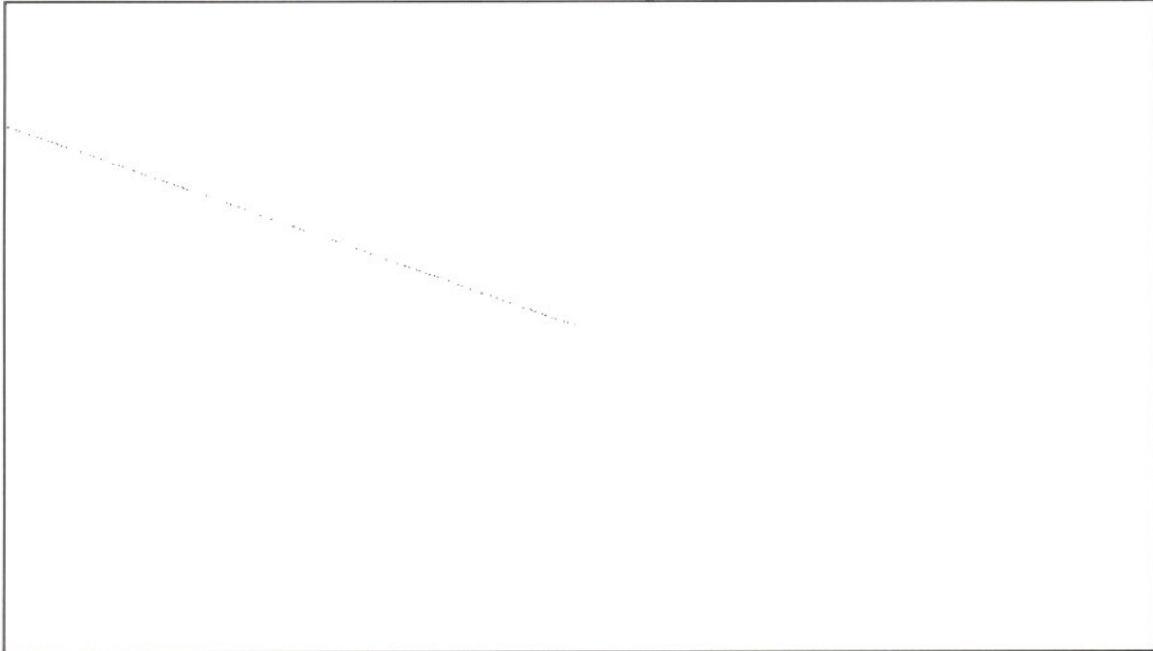
(b)(1),(b)(3):10 USC 424,(b)(3):50 USC 3024(i),1.4 (a),1.4 (c)

~~SECRET//NOFORN~~

Chapter Seven

(U) IRTF Summary Report - Baghdad Airstrike

(b), 1.4
(a), 1.4
(c), 1.4 (d)



(U) Background

~~(U//FOUO)~~ There are three distinct engagements shown in the leaked footage. According to CNN reports, the soldiers of Bravo Company 2-16 Infantry had been under fire all morning on July 12, 2007, from RPGs and small arms fire. Air Weapons Teams (AWTs) consisting of two Apache AH-64's were providing aerial support to ground units involved with Operation Ilaaj. The AWT spotted a group consisting of 15-20 men believed to be insurgents, some of whom were brandishing AK-47s. After receiving permission to engage, the AWT dispensed 30 mm rounds, killing several men, including one Reuters staff member, and severely wounding the other. Crew members mistook their video recording equipment for RPGs.

~~(U//FOUO)~~ Shortly after the initial engagement, a van arrived on scene. Purportedly unarmed men attempted to load the wounded Reuters staff member into the vehicle. The Apache crews believed the men to be additional insurgents attempting to recover bodies and weapons from the scene and requested permission to engage. The AWT opened fire on the van, killing the second Reuters reporter and one other man. Two children sitting in the van were severely wounded in the incident.

~~SECRET//NOFORN~~

(U//~~FOUO~~) There is a period of 20 minutes not included in the edited WikiLeaks version of video footage that showed the AWT engaging armed insurgents in a firefight on the ground. Some of the insurgents were seen entering a building. The edited WikiLeaks video resumes showing two men holding weapons entering the building. The aircrews request permission to engage the target, stating that they believed the buildings to be abandoned. Upon receiving permission, the AWT fires a total of three Hellfire missiles into the target. One of the gunners can be heard on the video stating, "There it goes! Look at that bitch go! Patoosh!"

(U) Media Coverage

(U) The footage was released by WikiLeaks founder Julian Assange during an April 5, 2010, press conference at the National Press Club, and subsequently under a designated website titled "Collateral Murder." Publicity of the incident spiked following the release of the footage. Some of the more notable media outlets covering the issue were Al Jazeera English, RT, Reuters, *The Washington Post*, *The New York Times*, the *Christian Science Monitor*, the BBC, and CNN. Coverage of the event in the mainstream media was largely unfavorable towards the U.S. position in this incident.

(U) WikiLeaks prefaces one of their videos with a disclaimer that some of the men may have been armed. Fox News claims that, "at least one man in that group was carrying an RPG, a clearly visible weapon that runs nearly two-thirds the length of his body." However, Glenn Greenwald of Salon.com said that the "vast majority of the men were unarmed" and called the incident "plainly unjustified killing of a group of unarmed men carrying away an unarmed, seriously wounded man to safety." *The Guardian* stated, "It is unclear if some of the men are armed but Noor-Eldeen (Reuters staff) can be seen with a camera." The Australian newspaper described the group as displaying "no obvious hostile action." Reuters further claims that it could not locate any witnesses who had seen gunmen in the immediate area of the incident.

(U) Military Legal Review

(U//~~FOUO~~) On April 5, 2010, USCENTCOM released two separate I5-6 investigative reports to coincide with the WikiLeaks press conference on the same day. One investigation was commissioned by the 1st Air Cavalry Brigade, 1st Cavalry Division, and another by the 2nd Brigade Combat Team, 2nd Infantry Division (MND-B). Both investigations exonerated the individuals involved in this event, concluding that they followed the rules of engagement to a satisfactory degree. Furthermore, the 2nd Brigade investigation provided stills from the gun cameras and photos from the ground identifying definitively that there were weapons present on the scene and that the Reuters Staff did not have any identification or clothing identifying them as members of the press while traveling with armed insurgents.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Final Report of the Department of Defense Information Review Task Force

(U) Conclusion

(b)(1),(b)(3):10 USC 424,(b)(5),1.4 (a),1.4 (c),1.4 (d)



(U) This report along with associated analytical assessments and other IRTF products are posted on (b)(3):10 USC 424. If you have any questions regarding this report please contact the IRTF through the RFI link on the IRTF Intelligence website referenced above.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

APPENDIX A

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

AUG 5 2010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

Subject: Task Force to Review Unauthorized Disclosure of Classified Information ~~(FOUO)~~

~~(FOUO)~~ On July 28, 2010, I directed the Director, Defense Intelligence Agency (DIA) to establish an Information Review Task Force (IRTF) to lead a comprehensive Department of Defense (DoD) review of classified documents posted to the WikiLeaks website (www.wikileaks.org) on July 25, 2010, and any other associated materials. Department of Defense Components should provide DIA any assistance required to ensure the timely completion of the review.

~~(FOUO)~~ The IRTF will review the impact of the unauthorized disclosure of classified information specified above. The IRTF will coordinate throughout the Intelligence Community in conducting this time-sensitive review and integrate its efforts with those of the National Counterintelligence Executive.

~~(FOUO)~~ The IRTF will provide regular updates to the Office of the Secretary of Defense (OSD) on its findings. A more comprehensive interim report will be provided as the effort progresses. That report will include the following items:

- ~~(FOUO)~~ Any released information with immediate force protection implications;
- ~~(FOUO)~~ Any released information concerning allies or coalition partners that may negatively impact foreign policy;
- ~~(FOUO)~~ Any military plans;



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OSD 02114-10
OPERATIONAL TEST AND EVALUATION

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

- ~~(U//FOUO)~~ Any intelligence reporting;
- ~~(U//FOUO)~~ Any released information concerning intelligence sources or methods;
- ~~(U//FOUO)~~ Any information on civilian casualties not previously released;
- ~~(U//FOUO)~~ Any derogatory comments regarding Afghan culture or Islam; and
- ~~(U//FOUO)~~ Any related data that may have also have been released to WikiLeaks, but not posted.

A final report will be produced once all documents are assessed.

~~(U//FOUO)~~ The IRTF is the single DoD organization with authority and responsibility to conduct the DoD review regarding this unauthorized disclosure. By separate tasking, I am directing USDI to conduct an assessment of the Department's procedures for accessing and transporting classified information.

~~(U//FOUO)~~ This review is separate from, and unrelated to, any criminal investigation of the leaked information. The assessment and review of the leaked documents is not intended to, and shall not limit in any way, the ability of Department, Federal Bureau of Investigation or any other federal criminal investigators, trial counsel and prosecutors to conduct investigative and trial proceedings in support of possible prosecutions under the Uniform Code of Military Justice or federal criminal provisions.



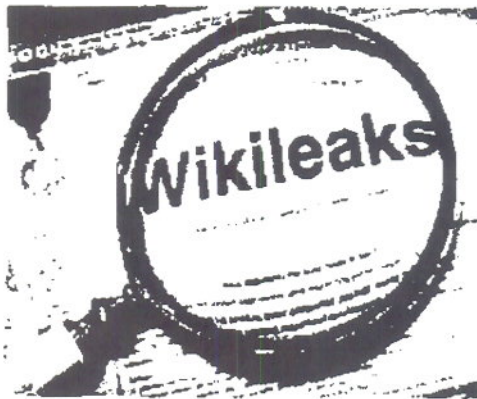
cc:
Director of National Intelligence
Director, Central Intelligence Agency
Assistant Secretary of State for Intelligence & Research
National Counterintelligence Center

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

APPENDIX B (U) GENERAL BACKGROUND INFORMATION ON WIKILEAKS



(U) WikiLeaks is a publicly accessible Internet website that host worldwide submissions of sensitive and classified military, government, corporate, and religious documents, while attempting to preserve the anonymity and untraceability of its contributors.

(U) It has been described as a web-based medium for people with damning, potentially helpful, or embarrassing information to reach the public, without providing any linkage back to the source who disclosed the information.

(U) "WikiLeaks describes itself as 'an uncensorable system for untraceable mass document leaking.' WikiLeaks is hosted by PRQ, a Sweden-based company providing 'highly secure, no-questions-asked hosting services.' PRQ is said to have 'almost no information about its clientele and maintains few if any of its own logs.' The servers are spread around the world with the central server located in Sweden."

— Source: Wikipedia at <http://en.wikipedia.org/wiki/WikiLeaks> (retrieved 18 Sep 2010)

(U) The WikiLeaks website, launched in 2006, is run by The Sunshine Press (<http://sunshinepress.org/>). Julian Paul Assange, an Australian, is described in open source reporting as the WikiLeaks founder. According to Assange, WikiLeaks maintains its web content on more than twenty servers around the world and on hundreds of domain names.

(U//FOUO) WikiLeaks' main website is accessible via <http://wikileaks.org> (straight plaintext HTTP) or via <https://secure.wikileaks.org> over TLS.²⁰ The domain name is registered under [possible U.S. person name deleted] c/o Dynadot Privacy, PO Box 701, San Mateo, CA, 94401 (a domain lookup resolves to 88.80.28.193, which geolocates to Stockholm, Sweden). The domain used to host mail for contacting the owners, is registered to Slava Tomaz, c/o WLK, PO Box 8098-00200, Nairobi, Kenya (a domain lookup resolves to 88.80.13.160, which also geolocates to Stockholm, Sweden).

²⁰ (U) TLS (Transport Layer Security) a cryptographic protocol that provides security for communication over networks such as the Internet. TLS protocol allows client/server applications to communicate across a network in a way to prevent eavesdropping and tampering. A prominent use of TLS is for securing World Web traffic by HTTP to form HTTPS.

~~SECRET//NOFORN~~

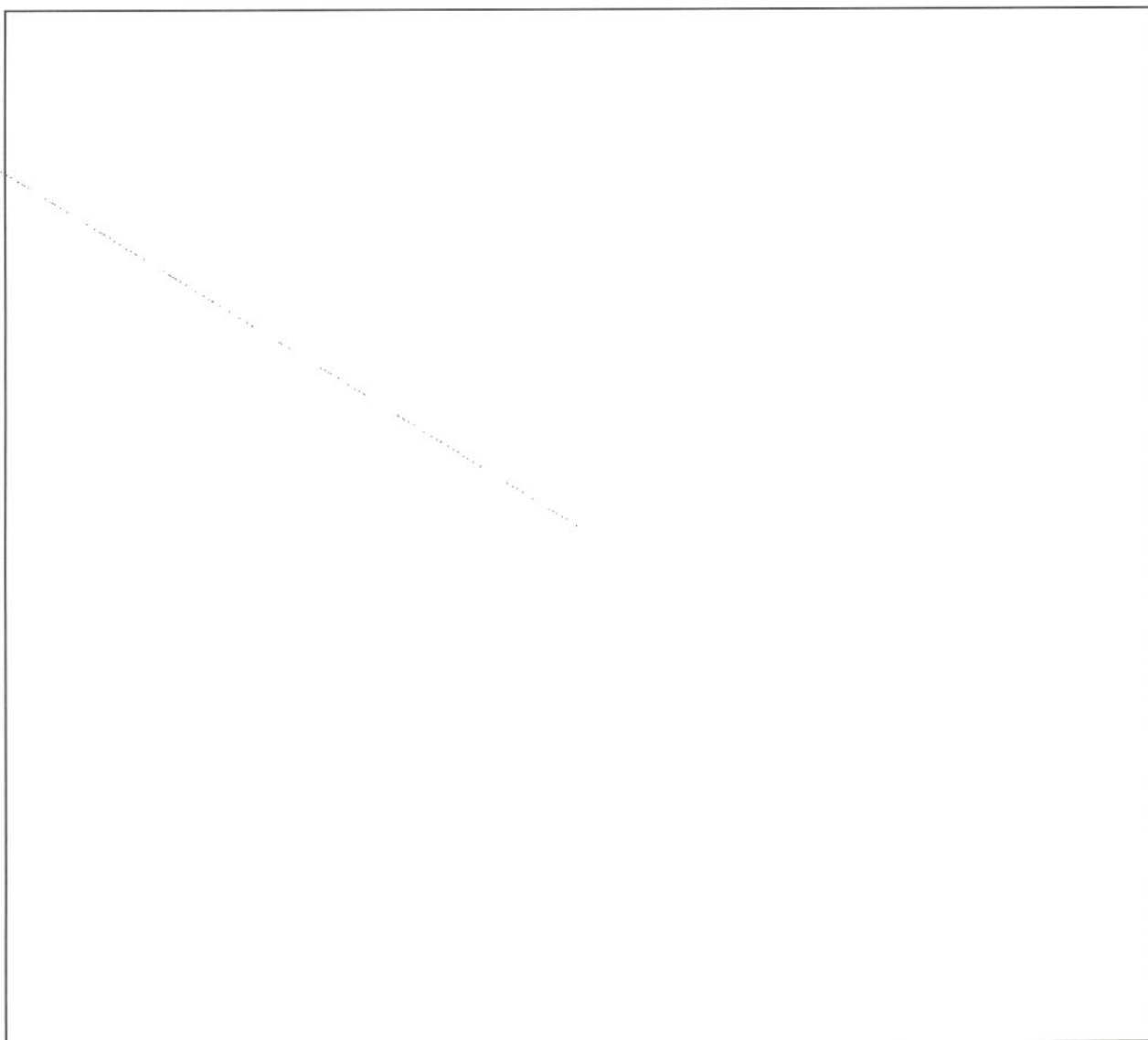
~~SECRET//NOFORN~~

APPENDIX D (U) DEROGATORY INFORMATION ON FOREIGN GOVERNMENTS

(U) The following are summaries of reporting found in the Joint Task Force-Guantanamo (JTF-GTMO) data set that provide information on the nefarious activities of a foreign government, its personnel, or institutions. Most of this information is detainee reported but some of it is derived from JTF-GTMO assessments and intelligence reporting.

(U) *Pakistan*

(b)(1), 1.4
(a), 1.4
(b), 1.4
(c), 1.4 (d)



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

APPENDIX F
(U) IRTF-Produced Country Information Memorandums

(U) Country specific information memoranda (IMs) are available on the IRTF's [redacted]

(b)(3):10 USC
424, (b)(3):50
USC 3024(i)

Afghanistan	India	South Africa
Africa	Indonesia	South Asia
Albania	Iran	Spain
Argentina	Iraq	Sweden
Australia	Israeli	Syria
Azerbaijan	Italy	Taiwan
Bahrain	Japan	Tajikistan
Baltic States	Jordan	Timor Leste
Belarus	Kazakhstan	Uganda
Belgium	Korea	Ukraine
Bolivia	Kuwait	United Arab Emirates
Bosnia-Herzegovina	Lebanon	United Kingdom
Brazil	Macedonia	Uruguay
Bulgaria	Malaysia	Uzbekistan
Burkina Faso	Mali	Venezuela
Burma	Mauritius	Vietnam
Cambodia	Mexico	Yemen
Canada	Mozambique	Zimbabwe
Cape Verde	Netherlands	
Chile	New Zealand	
China	Nicaragua	
Colombia	Nigeria	
Congo	Oman	
Croatia	Pakistan	
Cote d'Ivoire	Panama	
Cuba	Peru	
Cyprus	Philippines	
Czech Republic	Poland	
Denmark	Portugal	
Ecuador	Principe	
Egypt	Qatar	
France	Romania	
Georgia	Rwanda	
Germany	Saudi Arabia	
Greece	Sao Tome	
Guatemala	Senegal	
Guinea	Serbia	
Haiti	Seychelles	
Honduras	Singapore	
Hungary	Somalia	

~~SECRET//NOFORN~~



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