

#540

20110829 (Monday)

<http://wikileaks.org/Wikileaks-Statement-on-the-9-Month.html>

00. Editorial - Wikileaks Statement on the 9 Month Anniversary of Cablegate: Release of 133,887 Cables

29th August 2011

Over the past week, WikiLeaks has released 133,887 US diplomatic cables from around the world - more than half of the entire Cablegate material (251,287 cables). The new release was met with a sustained Denial of Service (DOS) attack during the first 36 hours. WikiLeaks had to rely on back-up servers for some hours. With supporters' help, WikiLeaks was able to bring in additional servers to stave off the attack.

For the first time, the diplomatic cables are available from every country that has US diplomatic representation. Until now, many countries had been excluded from the news stories, partly due to WikiLeaks media partners' geographical bias, and partly due to Wikileaks' resource constraints in establishing new media partnerships (there are now over 90).

Background

Nine months ago today, WikiLeaks launched Cablegate together with four media partners (Der Spiegel, El Pais, Le Monde, the Guardian) and the New York Times (who obtained the cables from the Guardian). The US administration and allied media groups responded with threats and intimidation. WikiLeaks and an alleged source, US intelligence analyst Bradley Manning, bore the brunt of these attacks. During the first weeks, calls to kidnap and assassinate WikiLeaks staff, and particularly its founder and editor-in-chief Julian Assange, were frequent. Shortly thereafter, VISA, MasterCard, PayPal, Bank of America and Western Union unilaterally prevented WikiLeaks from receiving donations from its supporters. The unlawful financial blockade of our publication continues, although WikiLeaks is suing VISA Europe and MasterCard, and has filed a complaint with the European Commission for serious breach. (For ways to donate, see <http://wikileaks.org/support>). A secret grand jury in Virginia is deciding whether Julian Assange, a journalist and Australian national, can be charged with espionage for the publication of this material.

Rationale: release of 133,887 cables

Cablegate launched nine months ago today. Despite the amount of material yet to be reported on, mainstream media organisations in Europe and the United States have slowed their rate of publishing Cablegate derived stories. This has led to the **misperception in Europe and the US that WikiLeaks has been less active in recent months**. In fact, WikiLeaks has stepped up its activity, establishing new partnerships on each continent with local media organisations that can contextualise the cables and carry out in-depth analysis. WikiLeaks has gone from its four original partners in November 2010 to over ninety as of this month (August 2011).

The decision to publish 133,877 cables was taken in accordance with WikiLeaks' commitment to maximising impact, and making information available to all. At the beginning of the month, the number of cables published had only reached the 20,000 mark – under 10% of the total. The cables that had been reported on also demonstrated a less than satisfactory representation on the world map.

Through crowdsourcing, WikiLeaks hopes to maximise the impact of the information in the diplomatic cables by allowing universities, investigative journalists, human rights advocates, lawyers, and prosecutors to access the source material all over the world. Crowdsourcing has proved to be a success: regional issues overlooked by our initial Western partners have been picked up around the world even

journalists who did not have access to our materials at institutions like the Guardian are revealing important stories. Mainstream newspapers, chiefly outside of Europe and the United States, are picking up on the #wfind hashtag on twitter. People across the globe are looking at the cables that report on their own countries: they are finding stories of corruption, risky local construction projects, stories of environmental degradation and candid analysis of their political landscape.

New stories include nuclear safety in China, a letter from the UN rapporteur to the US mission in Geneva inquiring on the reason why a US army soldier was not prosecuted for the killing of a Reuters journalist, a cable suggesting that the peaceful resolution of the conflict with North Korea may pose a risk to US interests in China because it may lead to China asking the US to leave its army base (some of the #wfind stories are listed below).

Crowdsourcing and journalism

Stories of the recently released material is being shared on twitter under the #wfind hashtag. The site www.cablegatesearch.net is a powerful tool for those scouring the cables: it enables keyword searches for over 140,000 released cables. This page also has a 'comments' field where readers can share research and valuable contextual knowledge regarding the cables, as well as link cables across themes and countries. Crowdsourcing allows for the significance of the material to grow organically: along with readers' geographical diversity comes a diversification of subject matters and a plurality of angles.

Crowdsourcing is not at odds with journalism. WikiLeaks has witnessed how the #wfind hashtag has led to stories being published in the mainstream press. The crowdsourcing of the bulk of the cables will assist journalists to sift through the tens if not hundreds of thousands of cables relating to the contemporary history of their own region. Readers are discovering that even the media organisations with the most resources, WikiLeaks' original partners, do not have the capacity to sift through all the cables nor report on all the big stories. It is a shared responsibility, then, for citizens, journalists, and researchers to comb through the material and find its local and global significance. Those stories that established media organisations are unable or unwilling to report on due to fear of being sued, or conflict of interest, or both, should nevertheless be in the public domain and available for everyone to access.

With crowdsourcing, WikiLeaks is also observing another interesting phenomenon: cables that have been previously published are also finding their way to the #wfind hashtag. Cablegate stories that have already been reported in national papers or in a different language have not transcended borders – this is now changing as the readers scour the cables. Crowdsourcing is drawing attention to new angles on previously published cables and helping to maximise the impact of the release.

We encourage you to use the cablegatesearch.net tool and to share your finds through articles, or applying the hashtag #wfinds on blogs and social networking sites such as twitter and Facebook. Readers are also encouraged to stay informed on how to optimise research through the WikiLeaks twitter feed and website.

WikiLeaks



Attack the Network – Defeat the Device – Train the Force



Joint IED Defeat Organization Counter IED Operations Integration Center

Classified By: Multiple Sources
Reason: 1.4 (a), (e) and (g)
Declassify on: MR
Prepared by: (b)(6)



RFS 69307
Red Team Analysis of IZ WikiLeaks

Published on: 07 JAN 2011
Information Cutoff Date: 06 JAN 2011

Prepared by: COIC MID
COIC Reston (COIC Red Team)

This information has been verified to be releasable to the foreign governments and/or international organizations indicated on this cover slide by the JIEDDO Foreign Disclosure Office. Provision of this information does not imply a commitment on the part of the US Government to loan, sell, transfer, provide, or convey information, technology, or equipment referred to herein.

Direct all inquiries to _COICFDO@atac.smil.mil

This Slide is **UNCLASSIFIED** When Separated from the Rest of the Presentation



(U) Agenda / Product Overview



Agenda

- (U) Executive Summary
- (U) Methodology
- (U) Key Findings
- (U) Red Team Methodology
- (U) ORSA Methodology
- (U) Way-Ahead
- (U) Points of Contact

Product Overview

- (U) Requestor: BG James Nixon, USCENTCOM J3 FP
 - Unit: CENTCOM
 - Phone: (b)(6)
 - (b)(6)@centcom.smil.mil
- (U//~~FOUO~~) What was requested:
 - Request a Red Team Analysis of the level of compromise regarding IED related WIKI-Leaks
- (U//~~FOUO~~) What was provided:
 - Red Team assessments based on a by hand reading of a statistically relevant sample (1890) of the 111k records that were provided by the customer and a complete read of the entire set of records by computational linguistics model developed by ORSA (Operations Research / Systems Analysis).
 - The primary response to the RFS is in the form of a Microsoft Excel Spreadsheet (embedded in this product) that lists in great detail all of the possible compromises found in the 111k released records that were provided by CENTCOM.
 - This PowerPoint Presentation presents the key findings derived from the study of the released records.
 - A supplementary briefing by OSAAC (Open Source Analysis Augmentation Center) with analysis of the societal reaction to the released records will be provided as an addendum within 14 days from the publishing of this report.

17-LR-0074 (Leopold)/DIA/REFERRAL/002



(U) Executive Summary



- (U//~~FOUO~~) Purpose:

Determine the pertinent information from 111k IED-related released "Wiki Leaks" records that may lead to the compromise of Counter IED tactics, techniques and procedures (TTPs) used by Coalition Forces conducting exploitation of IED events.

- ~~(S//REL)~~ Key Findings:

- ~40% of the 111k released reports (44k) were determined to be compromises.
- Of the 44k possible compromises:
 - 13% were determined to be **high severity** in that they inferred methods of collection or codified the Coalition understanding of the insurgents' relationship to other entities.
 - 17% were determined to be **medium severity** in that they disclosed tactical procedure that may be observed and possibly countered by insurgents.
 - 10% were determined to be **low severity** in that they disclosed tactical procedure that are easily observed but cannot easily be countered by insurgents.
- The release of the reports will facilitate the migration of IED "Best Practices" throughout theaters of operation and across various worldwide insurgent groups.
- Insurgents will change their TTPs to account for an improved awareness of CF capabilities and vulnerabilities.
- The release of local national names will mean an increase in intimidation and/or assassination.

17-LR-0074 (Leopold)/DIA/REFERRAL/003



(U) Methodology



ORSA

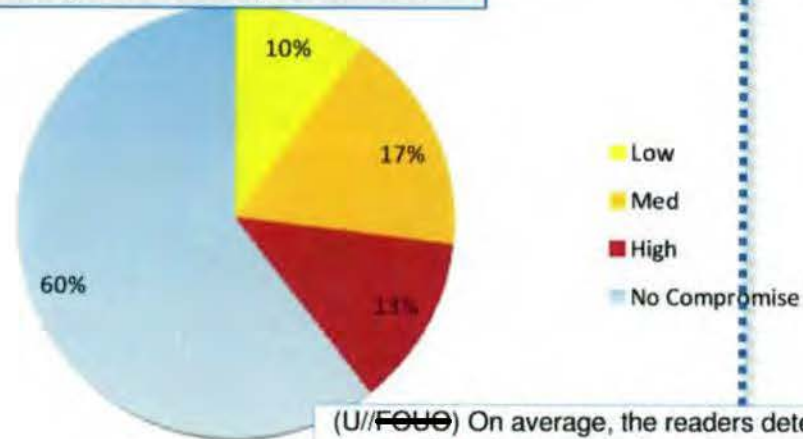
- (U//~~FOUO~~) Computational Linguistics techniques were applied to the records to determine which events were relevant to the current study.
- (U//~~FOUO~~) The requestor prescreened all of the WikiLeaks documents and determined that 133K records were specific to the IED problem set. Of those records, 111K provided sufficient fidelity for assessment and scope of this product.
- (U//~~FOUO~~) Red Team used human intervention to read a statistically relevant sample (1890 records). When they had processed a few hundred of the records, ORSA used the partial Red Team results to determine an initial set of compromise types to be used in appending the compromised CIDNE records. ORSA conducted additional passes at the data each time the human readers discovered new possible search criteria. Several runs (>20) simulations were conducted.
- (U//~~FOUO~~) In the initial effort, some records were not appended. Text Mining techniques were applied to the records not appended to seek additional compromises and compromise types. These additional compromise types were reviewed and selected ones were appended to the relevant records.
- (U//~~FOUO~~) This process substitutes computer processing for human reading of every record. Although every effort was made to produce an accurate, high-quality product, incomplete and inconsistent reporting together with the inherent weaknesses of computer processing means that a few reports may have been mischaracterized. The number of such mischaracterizations is a small portion of all of the data and will not significantly change the conclusions.



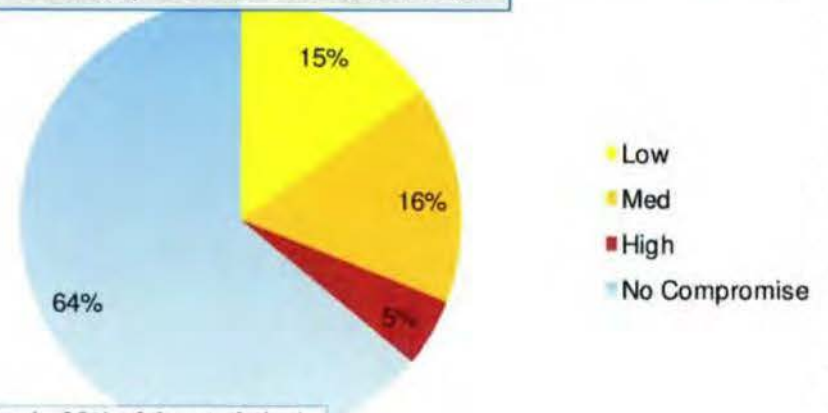
(U) Methodology



Computational Linguistics Read



Statistically Relevant Human Read



(U//~~FOUO~~) On average, the readers determined ~36% of the statistical sample to be compromises of various severities. This is within 4% of the computational read.

(U//~~FOUO~~) Red Team determines through an analytical methodology whether, and to what extent, there is compromise concerning a particular released report

(U//~~FOUO~~) Red Team read a statistically relevant and random sample (1,890 records). This sample size achieves +/-3% certainty that the sample is representative of the complete set of records.

(U//~~FOUO~~) Red Team used several readers in order to mitigate the influence of bias in the analysis.

(U//~~FOUO~~) No reader read more than ~300 records in order to mitigate the occurrence of cognitive drift and excessive cognitive load.

(U//~~FOUO~~) The readers had various military backgrounds (Chiefly: Explosive Ordnance Disposal, Special Forces and Army Intelligence)

(U//~~FOUO~~) Red Team (the human read) and ORSA (the computational read) are combined and categorized to determine whether there is a compromise and the concomitant level of severity.

High Severity: Infers methods or means of collection or codifies the Coalition understanding of the insurgents' relationship to other entities.

Medium Severity: Tactical procedures that may be observed and possibly countered by insurgents.

Low Severity: Tactical procedures that are easily observed and cannot be easily countered by insurgents.



(U) Key Findings (Computational Linguistics)

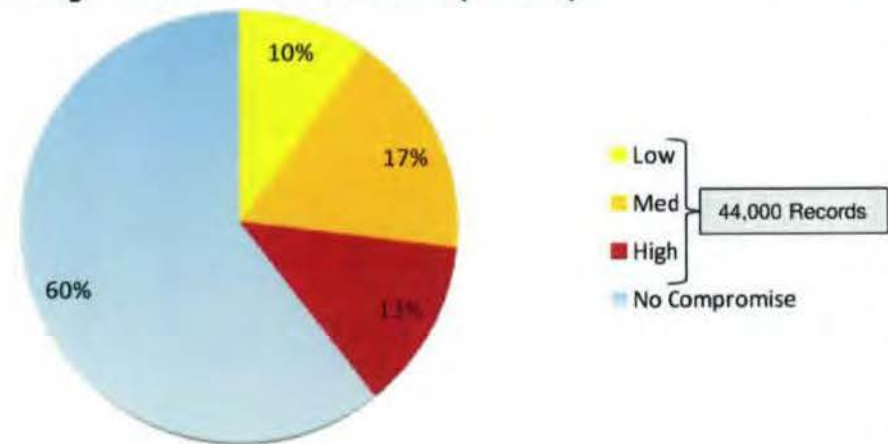


High Severity: Infers methods or means of collection or codifies the Coalition understanding of the insurgents' relationship to other entities.

Medium Severity: Tactical procedures that may be observed and possibly countered by insurgents.

Low Severity: Tactical procedures that are easily observed and cannot be easily countered by insurgents.

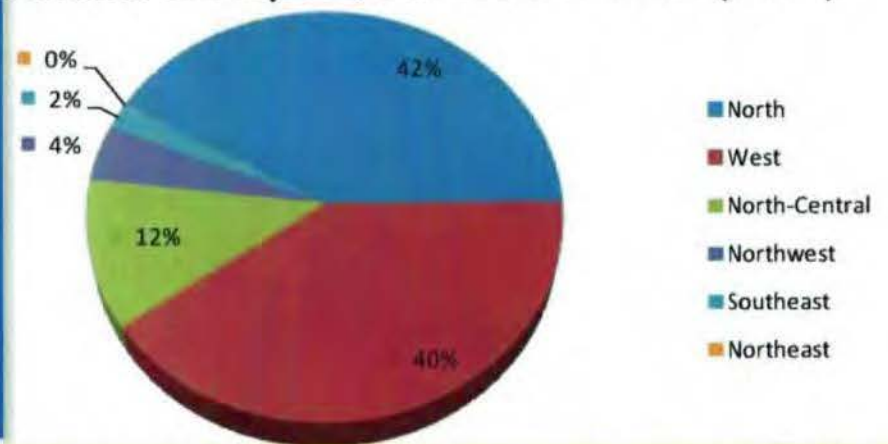
Severity: Percent of Total (111k)



(S//REL) ORSA determined that ~40% (44k reports) of the 111k records were compromises of various levels of severity. ~13% (14k reports) of the compromised records are considered high severity.

(S//REL) ORSA Determined that the vast majority of the released records pertain to North and West Iraq (~82%).

Location of Report: Percent of Total (111k)



Analysis: (S//REL) The impact of the compromise is not affected by the location to which the released report pertains. Insurgents in the North and West can make full use of compromised Friendly Force TTPs in the East and South. Additionally, compromised reports will significantly aid in the migration and improvement of Insurgent TTPs throughout Iraq, across other theatres of operation and across insurgent networks.



(U) Key Findings (Computational Linguistics: Severity)



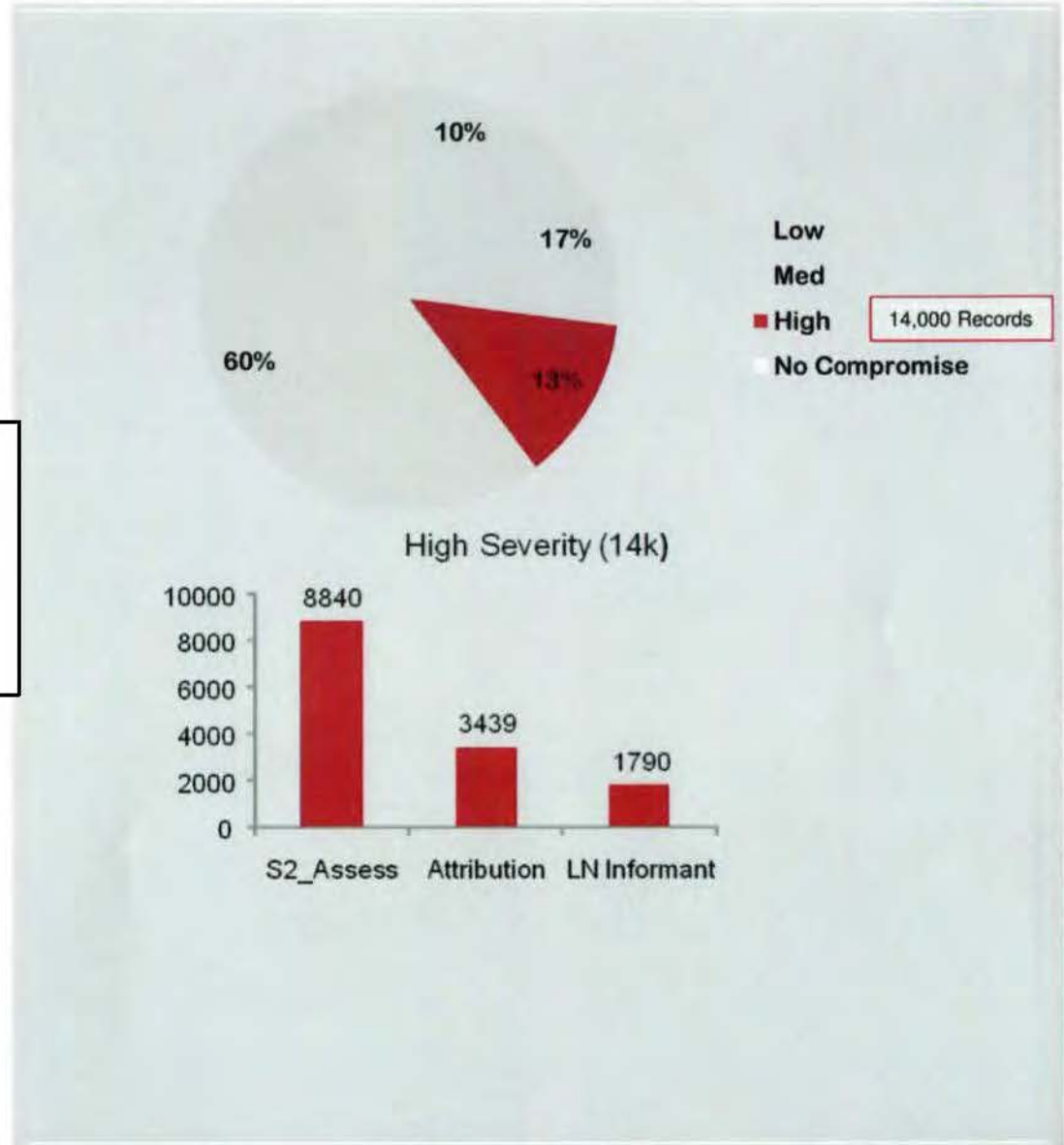
High Severity: Infers methods or means of collection or codifies the Coalition understanding of the insurgents' relationship to other entities.

Medium Severity: Tactical procedures that may be observed and possibly countered by insurgents.

Low Severity: Tactical procedures that are easily observed and cannot be easily countered by insurgents.

(S//REL) Released reports (b)(1), Sec. 1.4(a)

(b)(1), Sec. 1.4(a)



17-LR-0074 (Leopold)/DIA/REFERRAL/007



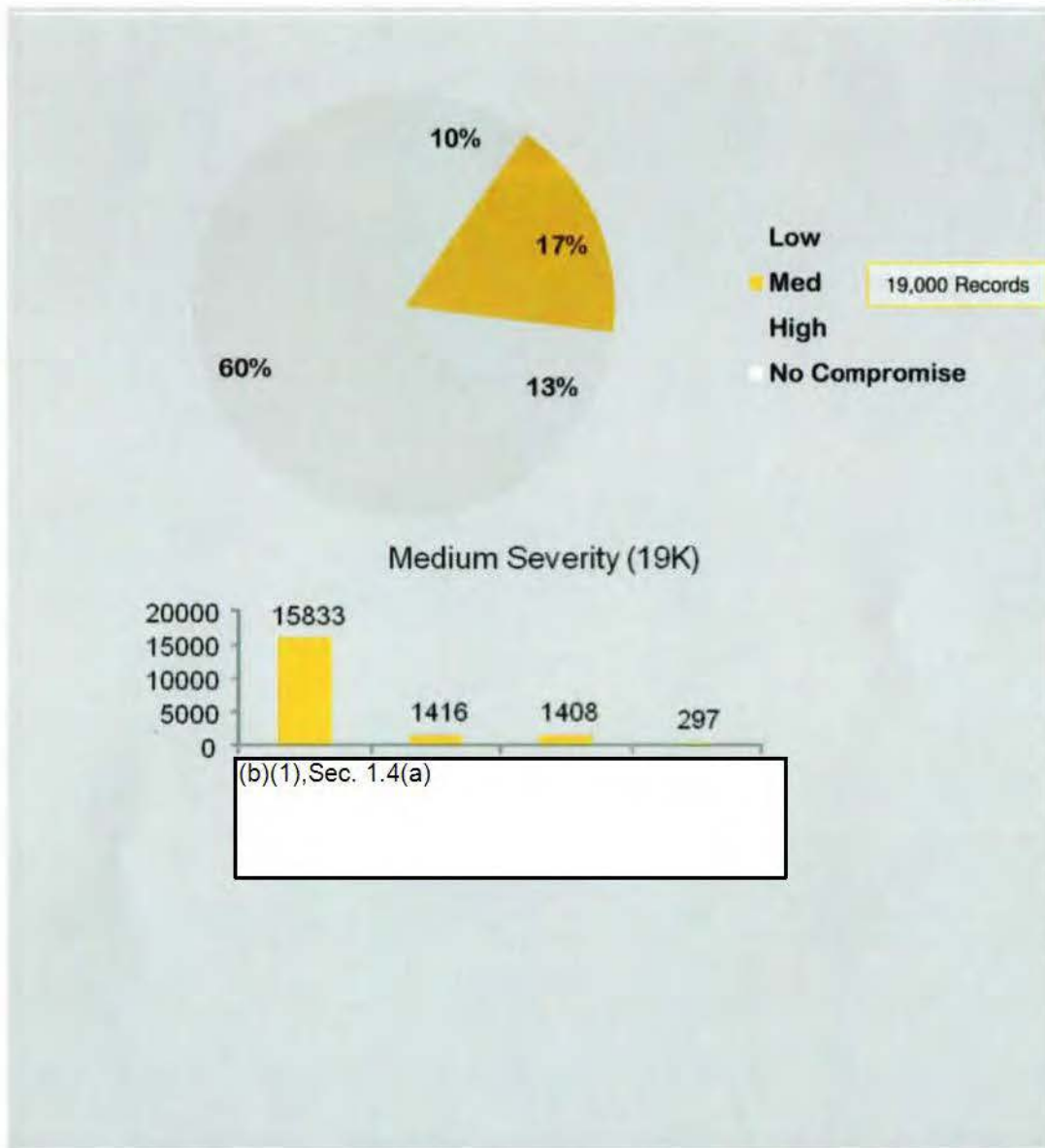
(U) Key Findings (Computational Linguistics: Severity)



High Severity: Infers methods or means of collection or codifies the Coalition understanding of the insurgents' relationship to other entities.

Medium Severity: Tactical procedures that may be observed and possibly countered by insurgents.

Low Severity: Tactical procedures that are easily observed and cannot be easily countered by insurgents.



(S//REL) (b)(1), Sec. 1.4(a)

(b)(1), Sec. 1.4(a)

(b)(1), Sec. 1.4(a)

17-LR-0074 (Leopold)/DIA/REFERRAL/008



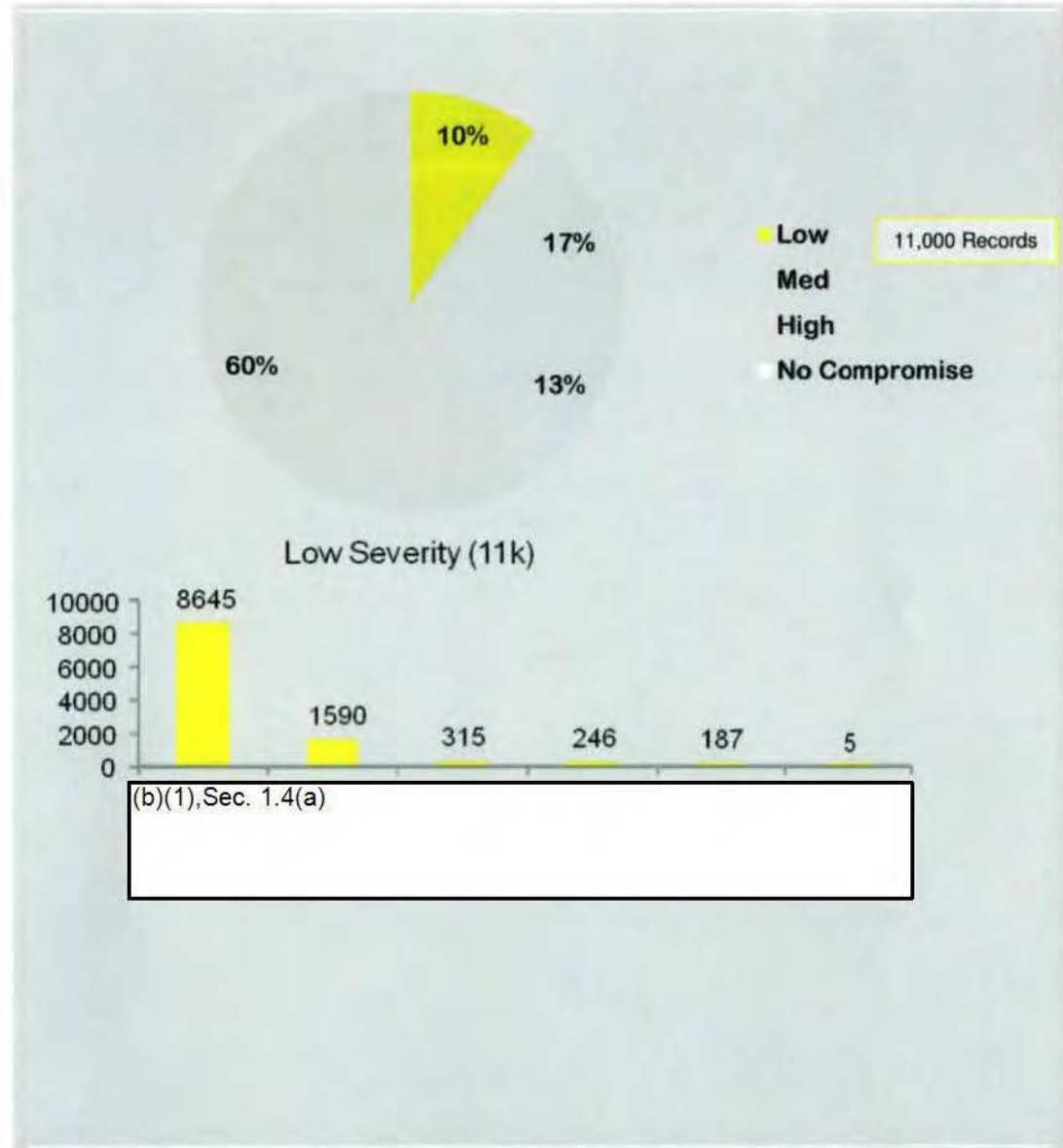
(U) Key Findings (Computational Linguistics: Severity)



High Severity: Infers methods or means of collection or codifies the Coalition understanding of the insurgents' relationship to other entities.

Medium Severity: Tactical procedures that may be observed and possibly countered by insurgents.

Low Severity: Tactical procedures that are easily observed and cannot be easily countered by insurgents.



(S//REL) (b)(1), Sec. 1.4(a)
(b)(1), Sec. 1.4(a)

(b)(1), Sec. 1.4(a)

17-LR-0074 (Leopold)/DIA/REFERRAL/009



(U) Key Findings (Statistical Human Read: Categories)



Categorized Compromises

Intelligence and EOD Analysis
CF Tactical and Operational Intent
CF Capabilities and Vulnerabilities
CF Unit Specifics
Networks and Names w/ IEDs
INS Capabilities and Vulnerabilities

Insurgent Response

Improve OPSEC
Improve Targeting Effort
Improve IED Construction
Exploit CF limitations of CF SOP
Effectively Target Local Nationals
Migrate IED Best Practices

(S//REL) (b)(1), Sec. 1.4(a)

(b)(1), Sec. 1.4(a)

-
-
-
-
-
-
-

(S//REL) These slides categorize the possible compromises. The categories are determined by an assessment of the human read of a statistically relevant sample of the data set. Trends noted are assessed to be statistically relevant to the entire data set. Certainty is 97% +/- 3%.



(U) Key Findings (Statistical Human Read: Categories)



Categorized Compromises

Intelligence and EOD Analysis

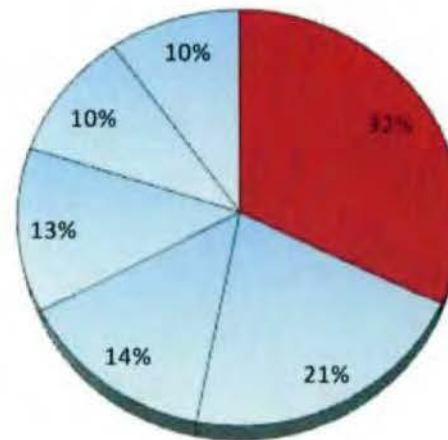
- CF Tactical and Operational Intent
- CF Capabilities and Vulnerabilities
- CF Unit Specifics
- Networks and Names w/ IEDs
- INS Capabilities and Vulnerabilities

Insurgent Response

Improve OPSEC

- Improve Targeting Effort
- Improve IED Construction
- Exploit CF limitations of CF SOP
- Effectively Target Local Nationals
- Migrate IED Best Practices

~~(S//REL)~~ 32% (14k) of the 44k possible compromises involve intelligence or EOD assessments.



- Intelligence and EOD Analysis
- CF Tactical and Operational Intent, TTPs
- CF Capabilities and Vulnerabilities
- Specifics Regarding CF Unit, SOP and Equipment
- Persons and Networks Named and Associated with IEDs
- INS Capabilities and Vulnerabilities

~~(S//REL)~~ Insurgents will use the information in the released records to better understand and plan against the abilities the Coalition's collection efforts.

~~(S//REL)~~ These slides categorize the possible compromises. The categories are determined by an assessment of the human read of a statistically relevant sample of the data set. Trends noted are assessed to be statistically relevant to the entire data set. Certainty is 97% +/- 3%.



(U) Key Findings (Statistical Human Read: Categories)



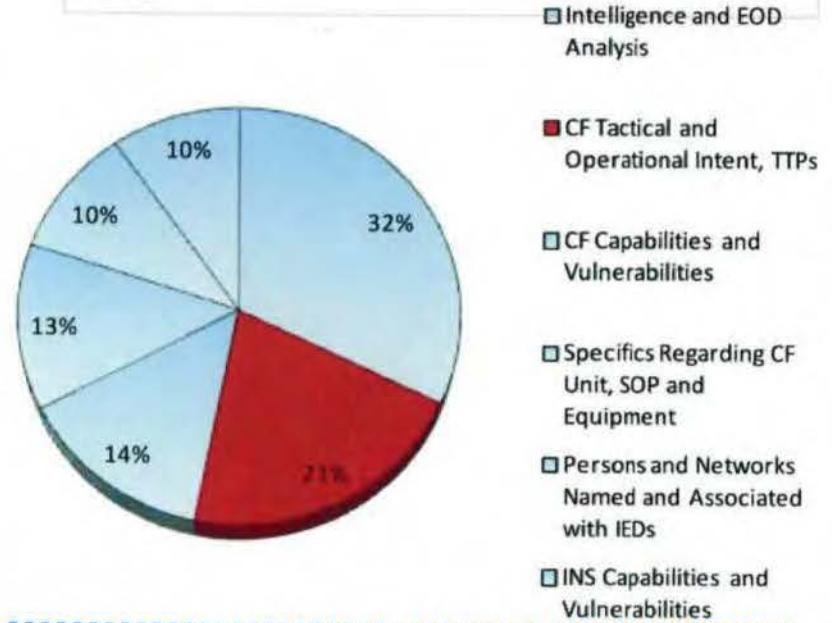
Categorized Compromises

- Intelligence and EOD Analysis
- CF Tactical and Operational Intent
- CF Capabilities and Vulnerabilities
- CF Unit Specifics
- Networks and Names w/ IEDs
- INS Capabilities and Vulnerabilities

Insurgent Response

- Improve OPSEC
- Improve Targeting Effort
- Improve IED Construction
- Exploit CF limitations of CF SOP
- Effectively Target Local Nationals
- Migrate IED Best Practices

(S//REL) 21% (9k) of the 44k possible compromises involve Coalition tactical and operational intent and TTPs



(S//REL) Insurgents will modify their methods of operations in order to mitigate Coalition procedures.

(S//REL) Insurgents will discover, verify and exploit patterns in Coalition TTPs.

(S//REL) These slides categorize the possible compromises. The categories are determined by an assessment of the human read of a statistically relevant sample of the data set. Trends noted are assessed to be statistically relevant to the entire data set. Certainty is 97% +/- 3%.



(U) Key Findings (Statistical Human Read: Categories)



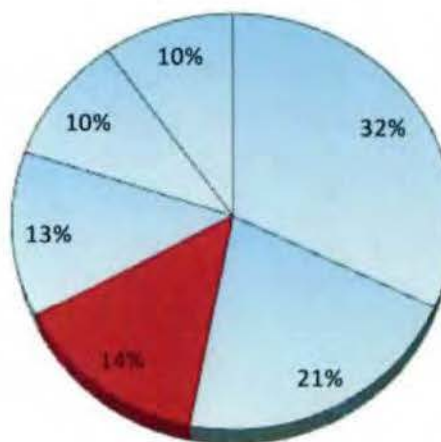
Categorized Compromises

- Intelligence and EOD Analysis
- CF Tactical and Operational Intent
- CF Capabilities and Vulnerabilities
- CF Unit Specifics
- Networks and Names w/ IEDs
- INS Capabilities and Vulnerabilities

Insurgent Response

- Improve OPSEC
- Improve Targeting Effort
- Improve IED Construction
- Exploit CF limitations of CF SOP
- Effectively Target Local Nationals
- Migrate IED Best Practices

~~(S//REL)~~ 14% (6k) of the 44k possible compromises involve details of Coalition capabilities and vulnerabilities.



- Intelligence and EOD Analysis
- CF Tactical and Operational Intent, TTPs
- CF Capabilities and Vulnerabilities
- Specifics Regarding CF Unit, SOP and Equipment
- Persons and Networks Named and Associated with IEDs
- INS Capabilities and Vulnerabilities

~~(S//REL)~~ Insurgents will develop IEDs that mitigate Coalition capabilities and exploit Coalition vulnerabilities.

~~(S//REL)~~ These slides categorize the possible compromises. The categories are determined by an assessment of the human read of a statistically relevant sample of the data set. Trends noted are assessed to be statistically relevant to the entire data set. Certainty is 97% +/- 3%.



(U) Key Findings (Statistical Human Read: Categories)



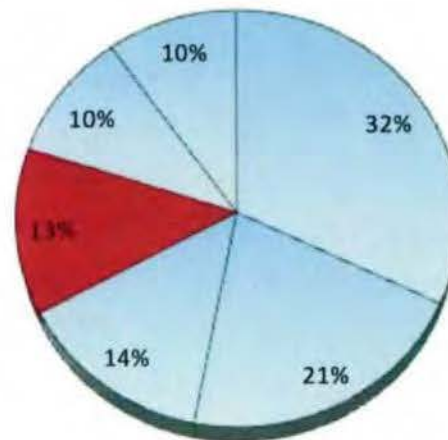
Categorized Compromises

- Intelligence and EOD Analysis
- CF Tactical and Operational Intent
- CF Capabilities and Vulnerabilities
- CF Unit Specifics
- Networks and Names w/ IEDs
- INS Capabilities and Vulnerabilities

Insurgent Response

- Improve OPSEC
- Improve Targeting Effort
- Improve IED Construction
- Exploit CF limitations of CF SOP
- Effectively Target Local Nationals
- Migrate IED Best Practices

(S//REL) 13% (6k) of the 44k possible compromises involve unit specifics such as details of SOP and equipment.



- Intelligence and EOD Analysis
- CF Tactical and Operational Intent, TTPs
- CF Capabilities and Vulnerabilities
- Specifics Regarding CF Unit, SOP and Equipment
- Persons and Networks Named and Associated with IEDs
- INS Capabilities and Vulnerabilities

(S//REL) Insurgents will modify their methods of operations in order to mitigate Coalition procedures.

(S//REL) Insurgents will discover, verify and exploit patterns in Coalition TTPs.

(S//REL) These slides categorize the possible compromises. The categories are determined by an assessment of the human read of a statistically relevant sample of the data set. Trends noted are assessed to be statistically relevant to the entire data set. Certainty is 97% +/- 3%.



(U) Key Findings (Statistical Human Read: Categories)



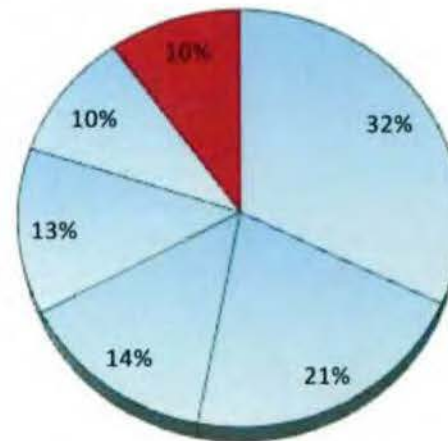
Categorized Compromises

- Intelligence and EOD Analysis
- CF Tactical and Operational Intent
- CF Capabilities and Vulnerabilities
- CF Unit Specifics
- Networks and Names w/ IEDs
- INS Capabilities and Vulnerabilities

Insurgent Response

- Improve OPSEC
- Improve Targeting Effort
- Improve IED Construction
- Exploit CF limitations of CF SOP
- Effectively Target Local Nationals
- Migrate IED Best Practices

(S//REL) 10% (4k) of the 44k possible compromises involve reported insurgent capabilities and vulnerabilities.



- Intelligence and EOD Analysis
- CF Tactical and Operational Intent, TTPs
- CF Capabilities and Vulnerabilities
- Specifics Regarding CF Unit, SOP and Equipment
- Persons and Networks Named and Associated with IEDs
- INS Capabilities and Vulnerabilities

(S//REL) "Best Practices" will migrate across Iraq, to OEF and worldwide.

(S//REL) These slides categorize the possible compromises. The categories are determined by an assessment of the human read of a statistically relevant sample of the data set. Trends noted are assessed to be statistically relevant to the entire data set. Certainty is 97% +/- 3%.



(U) Way-Ahead



- (U//~~FOUO~~) CENTCOM should conduct Risk Assessment / Risk Mitigation regarding high severity infractions. In particular, records that exposed cooperation by Local Nationals should be reviewed to determine if protective measures are needed.
- (U//~~FOUO~~) Future assessments should be completed with a combination of subjective and objective methods. The larger the data set, the more necessary it is for ORSA to objectively guide the subjective process.
- (U//~~FOUO~~) Inferences to "Special Programs" were not taken into account in this effort. As part of the Way-Ahead, Red Team suggests the customer works with ORSA on search criteria so that any compromises of Special Programs can be identified.
- (U//~~FOUO~~) There are ~20k records that could not be assessed one way or the other due to the fact that that as provided by the customer, there were no populated summary fields. Future effort may be needed to assess these as a separate task should the summary fields be repopulated.



(U) COIC Points of Contact



Red Team

- (b)(6) Lead for RFS 69307
 - (b)(6)
- (b)(6) Analyst
 - (b)(6)
- (b)(6) Analyst
 - (b)(6)
- (b)(6) Analyst
 - (b)(6)

ORSA

- (b)(6)

OSAAC

- (b)(6) Team Lead
 - (b)(6)
- (b)(6) Cultural Analyst
 - (b)(6)

Oversight

- (b)(6) General Oversight (Red Team Lead)
 - (b)(6)
- (b)(6) Technical Oversight
 - (b)(6)

Operations Lab Team

- (b)(6)

17-LR-0074 (Leopold)/DIA/REFERRAL/018



Attack the Network – Defeat the Device – Train the Force



Joint IED Defeat Organization Counter IED Operations Integration Center

Classified By: Multiple Sources
Reason: 1.4 (a), (e) and (g)
Declassify on: MR
Prepared by: (b)(6)



RFS 63095
DST Red Team Analysis of WikiLeaks

Published on: 08 SEP 2010
Information Cutoff Date: 07 SEP 2010

Prepared by: COIC MID
COIC Reston (COIC DST)



This Slide is **UNCLASSIFIED** When Separated from the Rest of the Presentation



(U) Agenda / Product Overview



Agenda

- (U) The WikiLeaks Assessment Team
- (U) Executive Summary
- (U) Overall Methodology
- (U) Key Findings
- (U) DST Methodology
- (U) ORSA Methodology
- (U) Way-Ahead
- (U) Points of Contact

Product Overview

- (U) Requestor (b)(6) Deputy CCJ3 CENTCOM
 - Unit: CENTCOM
 - Phone: (b)(6)
 - (b)(6)
- (U//~~FOUO~~) What was requested:
 - Request a DST Red Team Analysis of the level of compromise regarding IED related WikiLeaks.
- (U//~~FOUO~~) What was provided:
 - DST assessments based on a complete read of the 3970 records.
 - An ORSA determination based on computational linguistics.
 - This PowerPoint Presentation presents the key findings derived from the study of the released records.
 - The primary response to the RFS is in the form of a Microsoft Excel Spreadsheet (embedded below) that lists in great detail all of the possible compromises found in the 3970 released records that were provided by CENTCOM.
 - A supplementary briefing by OSAAC with analysis of the societal reaction to the released records is also provided and is embedded in this document. This briefing is provided as an addendum to this presentation.



Data and Data Reduction



OSAAC Presentation

17-LR-0074 (Leopold)/DIA/REFERRAL/020



(U) The WikiLeaks Assessment Team



DST

(Directed Studies Team)

(U) The COIC Directed Studies Team (DST) is a "Red Team" charged with conducting threat emulation at the tactical and operational level. As such, the DST is responsible for independently reviewing the full range of analytical issues related to the counter-IED fight, with an approach that provokes thought and offers alternative viewpoints. DST has Intelligence, Operations and Academic expertise.

ORSA

(Operational Research & Statistical Analysis)

(U) Provide commanders and their staffs with analytically derived, empirically supported basis for decisions regarding options to affect operational application of resources in C-IED efforts. Discover and implement innovative approaches, leveraging a wide array of skills and knowledge, to solve hard problems and enhance methodologies relating to data analysis and decision support.

OSAAC

(Open Source Analysis Augmentation Center)

(U) OSAAC provides a cultural context to the economic, political, social and "threat" layer of the overall intelligence picture.

(U) OSAAC products cite and distinguish reliability of sources using footnotes which are found on the notes pages of each of the OSAAC slides.



(U) Executive Summary



(U//~~FOUO~~) Purpose:

- Determine the pertinent information from 3970 TF Paladin reports that were released on WikiLeaks.com which may lead to the compromise of tactics, techniques and procedures (TTPs) used by our Coalition Forces while conducting exploitation of IED events.

(U//~~FOUO~~) Key Findings:

- DST and ORSA each found ~20% of the 3970 released reports to be compromises . ~4% (183 released reports) of the compromises were determined to be significant.
- The impact of the compromises is not affected by the location to which the released report pertains. Insurgents in RC North and West can make full use of compromised Friendly Force TTPs in RC East and RC South.
- Compromised reports will likely significantly aid in the migration and improvement of Insurgent TTPs.
- Insurgents will likely change their TTPs to account for the effectiveness of Friendly Force Close Air Support (CAS) and Unmanned Aerial Vehicles (UAV) that are used in response to an IED event.
- Insurgents will likely increase intimidation of local nationals in locations where the released reports specify local national cooperation with friendly forces. Also, in incidents where individuals (local populace or government officials) are mentioned by name, insurgents will likely develop assassination plans.
- OSAAC assesses that the Afghan government will likely use the WikiLeaks issue to both condemn the leak and affirm their position on several topics.
- OSAAC determines that insurgents are strongly denying any support from the Pakistan government as evidenced in the released WikiLeaks reports.



DST

- (U) Directed Studies determines through an analytical methodology whether, and to what extent, there is compromise with a particular record.
- (U) DST determines whether a released report is a likely compromise.
- (U) DST determined the severity of the compromise
 - **High Severity:** Infers methods or means of collection or codifies the coalition understanding of the insurgents' relationship to other countries.
 - **Medium Severity:** Tactical procedures that may be observed and possibly countered by insurgents.
 - **Low Severity:** Tactical procedures that are easily observed and cannot be easily countered by insurgents.
- (U) Directed Studies provides context for both the DST and ORSA findings.

(U) Methodology

ORSA



- (U) ORSA attacks the same problem using an iterative, automated process.
- (U) Techniques from computational linguistics were applied to label records with categories.
- (U) The initial list of categories was derived from partial results of the DST process.
- (U) Records that received no label were studied for patterns that led to additional categories being identified and the process started over.
- (U) DST analysts determined the severity level for each category and those levels were assigned by the computerized process based on the category of the record.

- (U) The DST/ORSA divergence is explained by:
 - The ORSA process used a computer to label records with a specified list of possible labels. The DST process used the judgment of human analysts to assign categories that they thought were appropriate.
 - The ORSA process marked all records using the same process. In the DST process, the analysts changed the marking process as they went along because a) they interpreted the data differently after seeing more records and b) stopped marking records in a category after that category had been marked repeatedly.



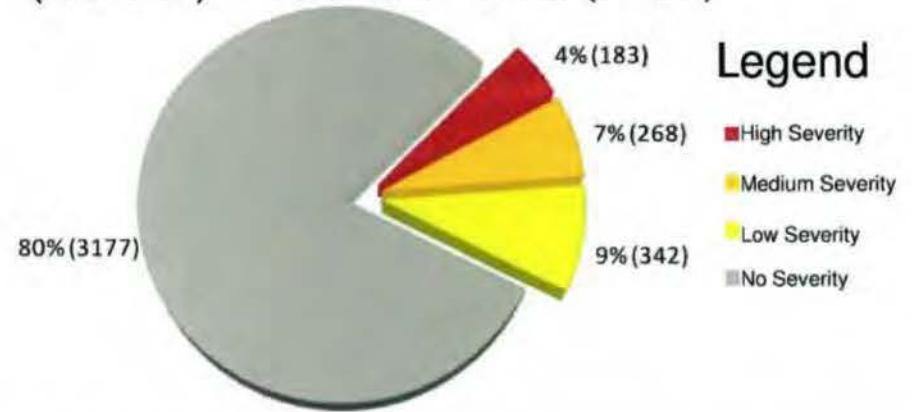
(S//REL) Key Findings

(U) **High Severity:** Infers methods or means of collection or codifies the coalition understanding of the insurgents' relationship to other countries.

(U) **Medium Severity:** Tactical procedures that may be observed and possibly countered by insurgents.

(U) **Low Severity:** Tactical procedures that are easily observed and cannot be easily countered by insurgents.

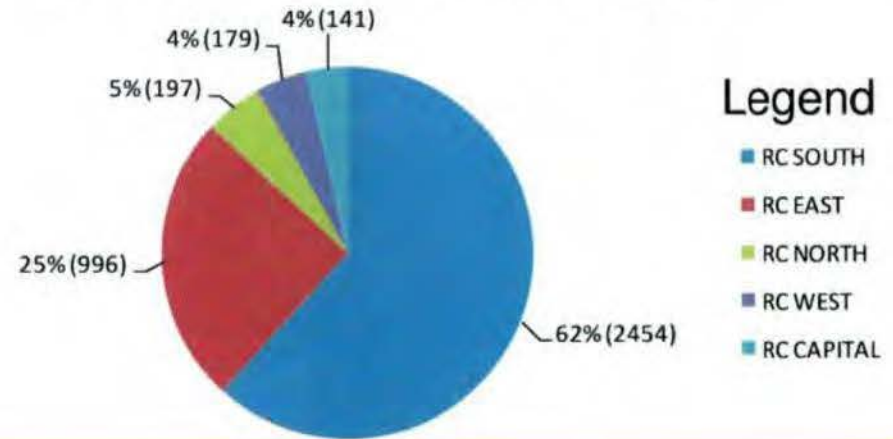
(S//REL) Percent of Total (3970)



(U//FOUO) DST/ORSA Determined that ~20% (793 reports) of the 3,970 records were potential compromises of TTPs. ~4% (183 reports) of the compromised records are considered high severity.

(U//FOUO) DST Determined that the vast majority of the released records pertain to RC East and RC South 3450 reports (~87%).

(S//REL) Percent of Total (3970)



Analyst Comments: (b)(1), Sec. 1.4(a)

(b)(1), Sec. 1.4(a)

17-LR-0074 (Leopold)/DIA/REFERRAL/024



(~~S//REL~~) Key Findings (cont')



(U) High Severity: Infers methods or means of collection or codifies the coalition understanding of the insurgents' relationship to other countries.

(U) Medium Severity: Tactical procedures that may be observed and possibly countered by insurgents.

(U) Low Severity: Tactical procedures that are easily observed and cannot be easily countered by insurgents.

High Severity TTPs

- ISR use and capabilities
- Local National cooperation with FF
- Communications intercept capability
- Analytical capabilities
- Tactical Limitations
- Use and capability of Ground Penetrating Radar (GPR)

INS Response

- Compensate for ISR capabilities
- More effectively intimidate LNs
- Improve OPSEC
- Use cover names and locations
- Exploit tactical limitations
- Use secondary devices

(U/~~FOUO~~) DST/ORSA determined potential insurgent responses for 6 categories of high severity possible compromises. From the release of these reports, the insurgent will likely be able to discern (to some degree) the effectiveness of friendly forces ISR, the level of LN support in particular areas, IED analytical capabilities, tactical limitations of friendly forces, tactical communication collection methods, and the use and capability of Ground Penetrating Radar.



(S//REL) Key Findings (cont')

High Severity TTPs

ISR Use and Capabilities

- Local National cooperation with FF
- Communications intercept capability
- Analytical capabilities
- Tactical Limitations
- Use and capability of GPR



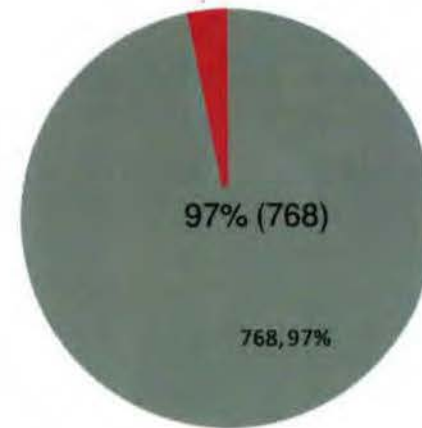
INS Response

Compensate for ISR Capabilities

- More effectively intimidate LNs
- Improve OPSEC
- Use cover names and locations
- Exploit tactical limitations
- Use secondary devices



(S//REL) 3% (25) out of the 793 possible compromises involve ISR use and capability.



(U//FOUO) Insurgents will likely use the information in the released records to better understand the role, general capabilities and limitations of ISR.

(U//FOUO) Insurgents will likely attempt to evade or deceive ISR in future attacks.



(S//REL) Key Findings (cont')

High Severity TTPs

- ISR use and capabilities
- Local National Cooperation with FF
- Communications intercept capability
- Analytical capabilities
- Tactical Limitations
- Use and capability of GPR

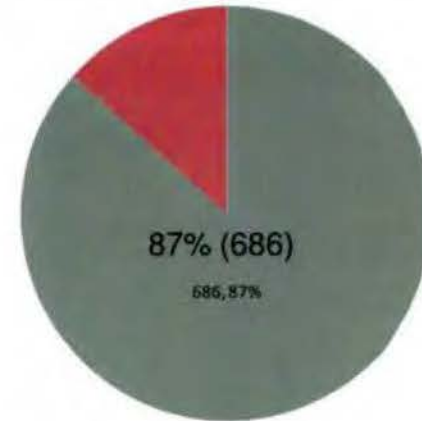


INS Response

- Compensate for ISR capabilities
- More Effectively Intimidate LNs
- Improve OPSEC
- Use cover names and locations
- Exploit tactical limitations
- Use secondary devices



(S//REL) 13% (107) out of the 793 possible compromises involve local national cooperation.



(U//FOUO) Insurgents will likely target more effectively LNs in areas that the released reports show high levels of LN cooperation.

(U//FOUO) Insurgents will likely inform LNs that if they cooperate with CF, it will not be kept secret, as evidenced by "WikiLeaks."

Analyst Comments (b)(1), Sec. 1.4(a)

(b)(1), Sec. 1.4(a)



(S//REL) Key Findings (cont')

High Severity TTPs

- ISR use and capabilities
- Local National cooperation with FF
- Communications Intercept Capability
- Analytical capabilities
- Tactical Limitations
- Use and capability of GPR

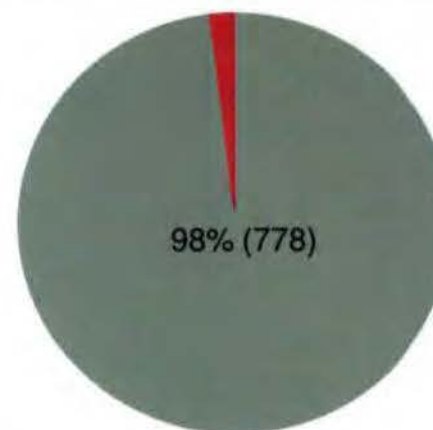


INS Response

- Compensate for ISR capabilities
- More effectively intimidate LNs
- Improve OPSEC
- Use cover names and locations
- Exploit tactical limitations
- Use secondary devices



(S//REL) 2% (15) out of the 793 possible compromises involving communications and intercept capability.



(U//FOUO) Insurgents will likely improve their OPSEC by incorporating frequency shifts in their tactical communications.

(U//FOUO) Insurgents will likely improve their deception planning with false indicators of ambush over ICOM radio and the development of code words.



(S//REL) Key Findings (cont')

High Severity TTPs

- ISR use and capabilities
- Local National cooperation with FF
- Communications intercept capability
- Analytical Capabilities
- Tactical Limitations
- Use and capability of GPR

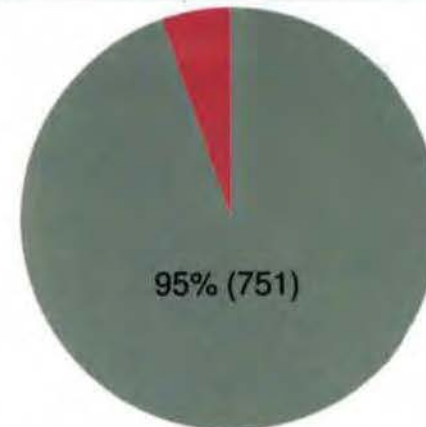


INS Response

- Compensate for ISR capabilities
- More effectively intimidate LNs
- Improve OPSEC
- Use Cover Names and Locations
- Exploit tactical limitations
- Use secondary devices



(S//REL) 5% (42) out of the 793 possible compromises involve analytical techniques.



(U//FOUO) Insurgents will likely develop new cover names and cover locations.

(U//FOUO) Insurgents will likely develop countermeasures to protect against friendly force analytic capabilities.

(U//FOUO) In response to the released records, insurgents will likely develop new IEDs that appear to be UXOs but are actually timed IEDs. (ANP stores some UXOs for a time prior to bringing them to CF for analysis.)



(S//REL) Key Findings (cont')

High Severity TTPs

- ISR use and capabilities
- Local National cooperation with FF
- Communications intercept capability
- Analytical capabilities
- Tactical Limitations
- Use and capability of GPR

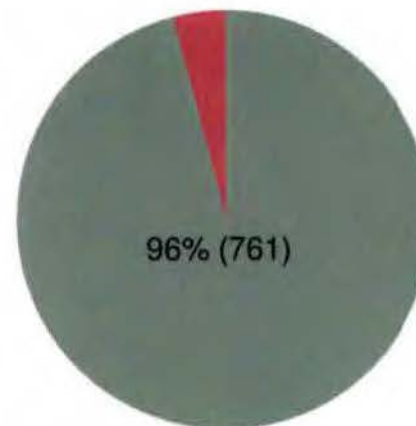


INS Response

- Compensate for ISR capabilities
- More effectively intimidate LNs
- Improve OPSEC
- Use cover names and locations
- Exploit Tactical Limitations
- Use secondary devices



(S//REL) 4% (32) out of the 793 possible compromises involve tactical limitations.



(U//FOUO) Insurgents will likely exploit limitations FF has with regard to weather, terrain and the presence of civilians when Close Air Support is needed.



(~~S//REL~~) Key Findings (cont')

High Severity TTPs

- ISR use and capabilities
- Local National cooperation with FF
- Communications intercept capability
- Analytical capabilities
- Tactical Limitations
- Use and Capability of GPR

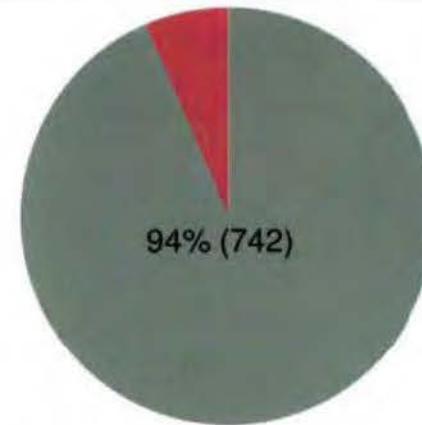


INS Response

- Compensate for ISR capabilities
- More effectively intimidate LNs
- Improve OPSEC
- Use cover names and locations
- Exploit tactical limitations
- Use Secondary Devices



(~~S//REL~~) 6% (51) out of the 793 possible compromises involve the use of metal detectors or GPR.



(U//~~FOUO~~) Insurgents will likely use secondary and tertiary devices to overcome the effectiveness of metal detectors and GPR.

(U//~~FOUO~~) Insurgents will likely use more low metal content IEDs in order to defeat the effectiveness of metal detectors.



(U) Way-Ahead



- (U) Risk Assessment / Risk Mitigation should be completed regarding the infractions determined to be high severity. In particular, records that exposed cooperation by local nationals should be reviewed to determine if protective measures are needed.
- (U//~~FOUO~~) Future assessments on perhaps larger data sets should be done with a combination of subjective and objective methods. The larger the data set, the more necessary it is for ORSA to objectively guide the subjective process.
- (U) Inferences to "Special Programs" were not taken into account in this effort as none of the parties involved in the effort are read on to the relevant programs. As part of the way-ahead, DST suggests the customer works with ORSA on search criteria so that any compromises of special programs can be identified.
 - (U) Recommend a Special Programs review of the findings in this document and the embedded excel spreadsheet.
- (U) Recommend a SIGINT assessment of IED facilitators mentioning the released reports.
- (U) Recommend an analysis of the strategic and political impact of these released reports.



(U) DST Methodology



- (U) The COIC Directed Studies Team (DST) is a “Red Team” charged with conducting threat emulation at the tactical and operational level. As such, the DST is responsible for independently reviewing the full range of analytical issues related to the counter-IED fight.
- (U) Charged with assessing the level of compromise regarding 3970 TF Paladin classified records that were released in an open and unclassified manner, Directed Studies has teamed with ORSA.
- (U) Directed Studies determines through an analytical methodology whether, and to what extent, there is a compromise with a particular record.
- (U) ORSA attacks the same problem set but with a computational methodology.
- (U//~~FOUO~~) In the end, there are two categories of compromise that are presented.
 - Those that are selected by both DST and ORSA and are determined by DST to be high severity:
 - **High Severity:** Infers methods or means of collection or codifies the coalition understanding of the insurgents’ relationship to other countries
 - **Medium Severity:** Tactical procedures that may be observed and possibly countered by insurgents.
 - **Low Severity:** Tactical procedures that are easily observed and cannot be easily countered by insurgents.
 - Those that are not selected by ORSA, but DST determines to be high severity.
- (U) Directed Studies provides context for both the DST and ORSA findings.
- (U) Comments or questions are welcome and may be directed to any of the team members listed on the POC slide.



(U) ORSA Methodology



- (U) Computational linguistics techniques were applied to the records to determine which events were relevant to the current study.
- (U) DST had human analysts read each record. When they had processed approximately 300 of the records, ORSA used the partial DST results to determine an initial set of categories to be used in labeling the compromised CIDNE records.
- (U) In the initial labeling, some records received no label. They did not belong in any of the categories. Text mining techniques were applied to the unlabeled documents to suggest additional categories. These additional categories were reviewed and selected ones were added to the labeling program.
- (U) The process of labeling, searching for new categories and then relabeling with additional categories was continued until no new categories were added.
- (U//~~FOUO~~) This process substitutes computer processing for human reading of every record. Although every effort was made to produce an accurate, high-quality product, incomplete and inconsistent reporting together with the inherent weaknesses of computer processing means that a few reports may have been mischaracterized. The number of such mischaracterizations is a small portion of all of the data and will not significantly change the conclusions.



(U//FOUO) COIC Points of Contact



DST

- (b)(6) Team Lead
 - (b)(6)
- (b)(6) Analyst
 - (b)(6)
- (b)(6) Analyst
 - (b)(6)
- (b)(6) Analyst
 - (b)(6)
- (b)(6) Analyst
 - (b)(6)

ORSA

- (b)(6)

OSAAC

- (b)(6) Team Lead
 - (b)(6)
- (b)(6) Senior OSINT Analyst
 - (b)(6)
- (b)(6) Cultural Advisor
 - (b)(6)

Afghanistan Operations Lab Team

- (b)(6)

17-LR-0074 (Leopold)/DIA/REFERRAL/035



- (U) Secretary of Defense tasked DIA to lead a comprehensive DoD review of documents posted to WikiLeaks website on July 25, 2010, to include any related data that may have been provided to WikiLeaks, but yet to be posted or released to the public. The SECDEF designated the IRTF as the single DoD organization with authority and responsibility to conduct the DoD review regarding this unauthorized disclosure of DoD information.

(b)(3):10 U.S.C. § 424,(b)(3):50 U.S.C. § 3024(i),(b)(5)

~~SECRET~~

(b)(3):10 USC 424

INFO MEMO

~~S~~10-0217/IRTF

20 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

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

Derived from: ~~SECRET~~

Declassify on: ~~SECRET~~

~~SECRET~~

(b)(3):10 USC 424

~~SECRET~~

(U) Data Characterization

(b)(1),(b)(3):10 USC 424, Sec. 1.4(b), Sec. 1.4(c)



Prepared by: (b)(3):10 USC 424,(b)(6)

Reviewed by:



Derived from: ~~Multiple Sources~~
Declassify on: ~~20XX~~

~~SECRET~~

~~SECRET~~

(b)(3):10 USC 424

INFO MEMO

10-0229/IRTF

20 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

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

(U) Smuggling and Illegal Crossings

(b)(1),(b)(3):10 USC 424,Sec. 1.4(b),Sec. 1.4(c)

Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

~~SECRET~~

(b)(3):10 USC 424

~~SECRET~~

(b)(3):10 USC 424

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

[Redacted content]

(U) Harassment of Border Forces

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

[Redacted content]

Derived from: ~~SECRET~~
Declassify on: ~~SECRET~~

~~SECRET~~

(b)(3):10 USC 424

~~SECRET~~

(b)(3):10 USC 424

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

(U) Iraqi Border Forces Response to Harassment

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

(U) Cross-Border Operations

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

Derived from: ~~Multiple~~
Declassify on: ~~FOUO~~

~~SECRET~~

(b)(3):10 USC 424

(b)(3):10 USC 424

(b)(1),(b)(3):10 USC 424,Sec. 1.4(b),Sec. 1.4(c)

(U) Politically-Sensitive Incidents

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

Prepared by: (b)(3):10 USC 424,(b)(6)
Reviewed by:

Derived from: ~~SECRET~~
Declassify on: ~~SECRET~~

(b)(3):10 USC 424

INFO MEMO

10-0318/IRTF

14 December 2010

TO: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

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

(U) Media Treatment

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

- (U) Leading centrist daily *Le Soir* noted on 30 November 2010 the leaks mostly highlight the “solid and orthodox work of the [traditional] press,” which has already revealed most of the secrets in the cables.²
- (U) Popular daily *Le Derniere Heure* on 9 December 2010 said of the following topics concerning Belgium that were revealed in the leaked cables, all had been

Derived from: ~~SECRET//NOFORN~~
Declassify on: ~~SECRET//NOFORN~~

thoroughly covered by traditional media already:³

- (U) U.S. pressure on Belgium to accept Guantanamo detainees
- (U) The presence of nuclear weapons in Belgium
- (U) European Union (EU) President (and former Belgian Prime Minister) Van Rompuy's pessimism on Afghanistan and climate change negotiations
- (U) Belgian internal political debates

(U) Official Reaction

(U) Belgian officials have downplayed the importance of the disclosures in public, condemning the act of leaking the cables while stressing that they contain few important disclosures.

- (U) Foreign Minister Vanackere, specifically referencing negotiations over Guantanamo detainees, said on 29 November 2010 "a great many things which are now being presented as leaks were actually already known."⁴
- (U) An advisor to Prime Minister Leterme wrote in a 30 November 2010 op-ed that the content of the leaked cables is not surprising and will not affect U.S. relations with other countries, while criticizing the WikiLeaks organization for being motivated "more by the desire to do harm than to fight injustice."⁵
- (U) Vanackere on 12 December 2010 claimed another foreign minister had refused to answer a question "for fear of seeing a report of the conversation on the Internet."⁶

(U) Potential Loss of Diplomatic Contacts

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

Derived from: ~~multiple sources~~
Declassify on: ~~FOUO~~

The last 4 pages are withheld in full and are not included.

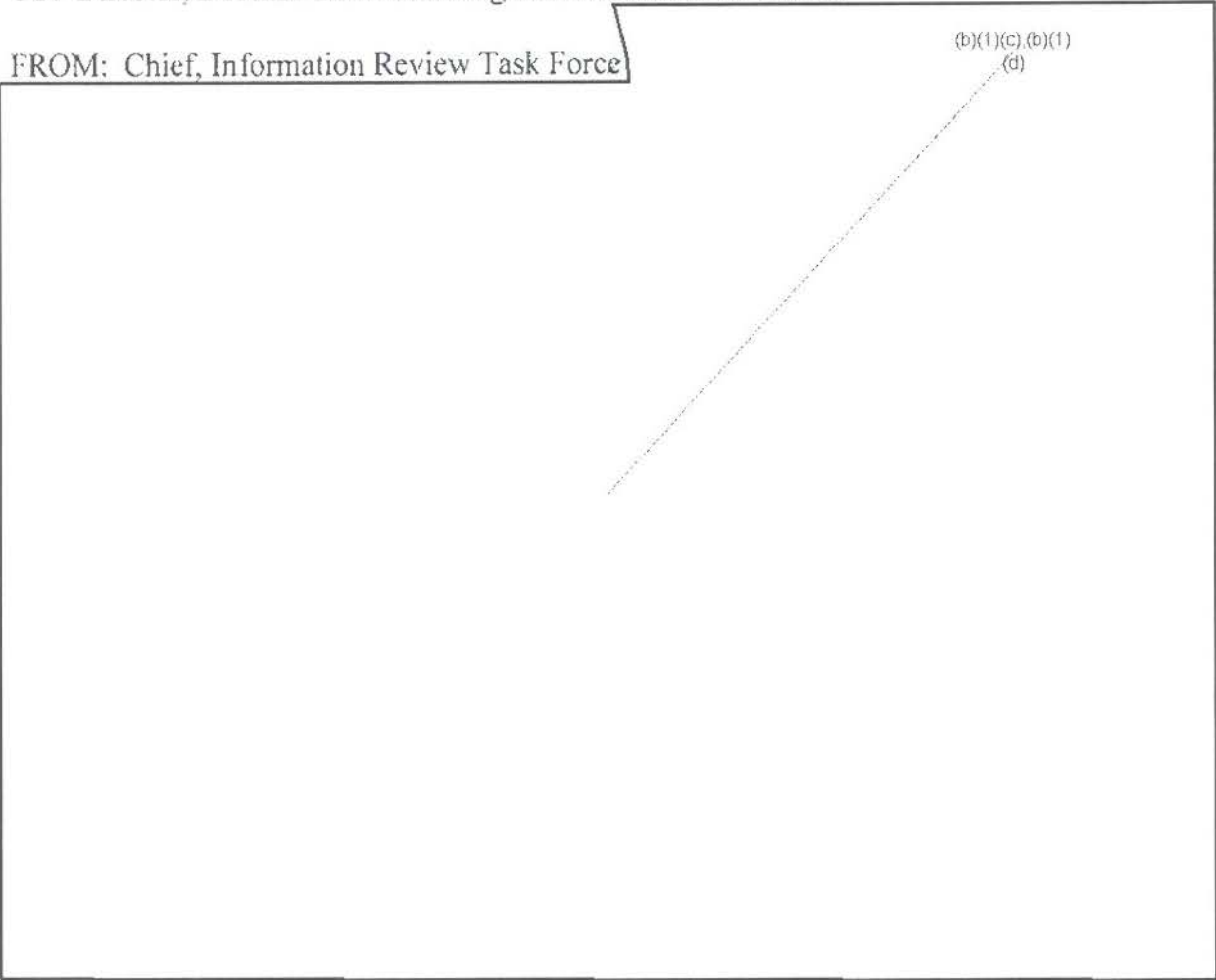
INFO MEMO

11-0384/IRTF

8 February 2011

TO: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force



- (U) According to an open source report dated 16 December 2010, President Colom reacted to the leaked documents by saying that some of the divulged information is inaccurate, [redacted] (b)(3):10 USC 424,(b)(3):50 USC 3024(i)

- (U) According to an open source report dated 14 December 2010, Guatemalan officials are avoiding commenting on the cables divulged by Wikileaks, stating that they will wait until they can see what information the cables contain.²


Derived from [redacted]
Declassify on: [redacted]

The Honorable John Ensign
United States Senate
Washington, DC 20510

Dear Senator Ensign:

(U) This letter responds to your December 10, 2010 request to the Director of National Intelligence for information regarding the impact of unauthorized disclosures of classified information by Wikileaks.

(b)(1),(b)(3):50 U.S.C. § 3024(i),(b)(5),Sec. 1.4(c),Sec. 1.4(d)



~~SECRET//NOFORN~~

(b)(1),(b)(3):50 U.S.C. § 3024(i),(b)(5),Sec. 1.4(c),Sec. 1.4(d)

(U) I appreciate the interest and concern shown by you and other Members regarding unauthorized disclosures of sensitive and classified information. Keeping such information secure is of vital importance to the Department and the U.S. Government, and I look forward to working with you in addressing the many challenges we face.

Michael G. Vickers
Acting

~~SECRET//NOFORN~~

18-LR-0001 (Leopold/DIA/REFERRAL/005)

#584

From: (b)(5),(b)(6),(b)(3):10 USC 424
To:
Cc:
Subject:
Date: Thursday, April 28, 2011 12:54:58 PM
Attachments: (b)(3):10 USC 424;(b)(3):50 USC 3024(i)

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(5),(b)(6),(b)(3):10 USC 424;(b)(3):50 USC 3024(i)

From:
Sent: Thursday, April 28, 2011 11:56 AM
To: (b)(5),(b)(6),(b)(3):10 USC 424
Cc:
Subject:

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(5),(b)(6),(b)(3):10 USC 424;(b)(3):50 USC 3024(i)

The unveiling of WikiLeaks in Nicaragua

1,432 U.S. diplomatic cables, of which 48 are secret and confidential 638 *A media partnership between the Nation, Confidential, This Week and El Nuevo Diario *An exercise of journalistic independence and public accountability, without any economic interests

LA NACIÓN

Starting tomorrow, we will begin to publish the diplomatic cables from the U.S. Embassy on Nicaragua, leaked by WikiLeaks, a media partnership between the nation of Costa Rica, CR and This Week, which has joined El Nuevo Diario. This diplomatic cables of 1,432 mostly originated in the United States Embassy in Managua from January 2006 to February 26, 2010. These cables are part of the package of more than 251,000 documents, written from 280 U.S.

EL NUEVO DIARIO

The complete collection of U.S. diplomatic cables on Nicaragua, which remained in power and totaling 1,432 WikiLeaks documents are now available to readers of CR and El Nuevo Diario, Nicaragua, and the newspaper La Nación, Costa Rica, as a result of a partnership and unprecedented publishing collaboration between the media of both countries.

The vast majority of diplomatic cables on Nicaragua, a total of 1,398 documents- for the years 2006-2010, period 2006 general elections in

The maze of cables

From 23 to 27 March in marathon sessions of reading, analysis and screening, the news teams of the Nation and Confidential comprised of seven writers, read the first package of diplomatic cables released weeks ago. In a second session from 12 to 16 April, worked a second batch of documents released by WikiLeaks, to complete the series of 1,432 official texts. In the original version in English of each wire was added a headline and a summary of a paragraph in Spanish, for easy

Jointly identified 16 specific issues that are of public interest in Nicaragua and Costa Rica. These subjects investigated, along with the cables intact, original will be published weekly in the pages of The Nation, Costa Rica, and CR and El Nuevo Diario, from Monday 25 April.

Also, the websites of The Nation (www.nacion.com /research) of Confidential (www.confidencial.com.ni) will be releasing each and every one of the wires 1,432 and block deliveries to the interest of Nicaraguan general, academics, specialists, etc.

In agreement with WikiLeaks Nation, whose commitment now extends to CR and This Week, and through them to El Nuevo Diario, did not mediate any kind of financial outlay.

The figures on Nicaragua Cables

1,432: Number of cables supplied by WikiLeaks to the Nation related to Nicaragua.

12/12/1986 to 26/02/2010: Period covering diplomatic reports on Nicaragua.

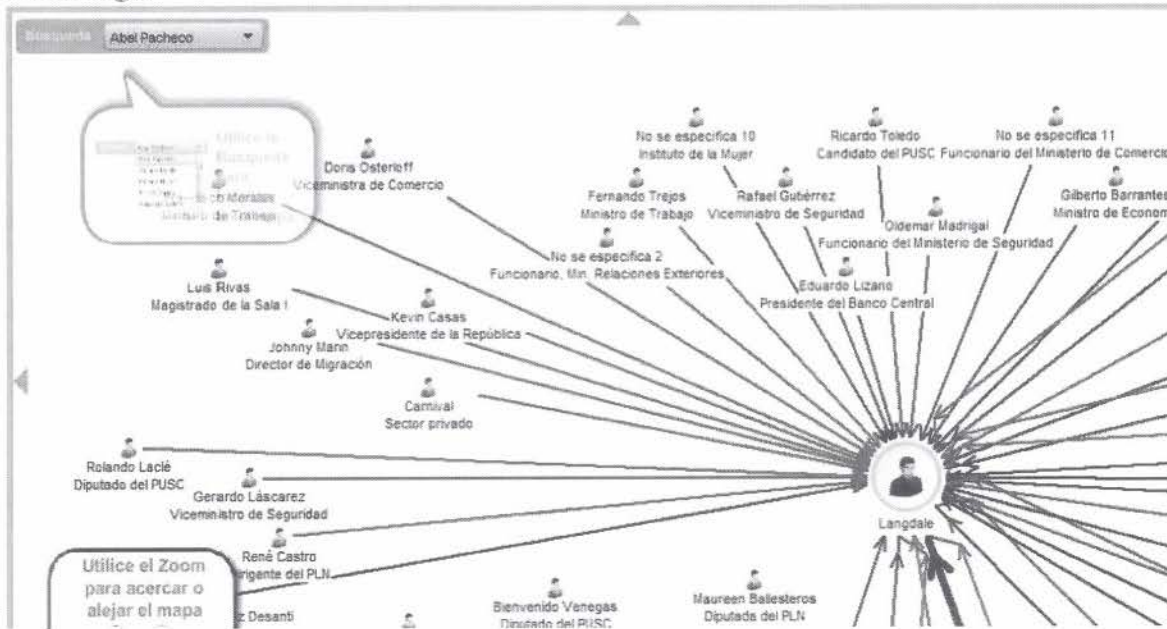
Rating: This diplomatic documents were classified by the Department of State: 48 secrets, 638 and 746 declassified confidential.

By year: In 2006, generated the largest number, 348 cables, followed by 2007, 336, 2008 with 334, with 329 in 2009, 2010, to 51, 2005 with 26, 2004 with six, and 1986 and 1988 with one each.

Las fuentes de la Embajada

■ Estas son las fuentes que utilizaron los diplomáticos estadounidenses para redactar los cables que contienen información más sensible, de acuerdo a un estudio de los 827 despachos efectuado por La Nación. Para facilitar la lectura del gráfico, se omitieron las fuentes que compartieron información importante o que solo hicieron análisis.

Simbología



CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(5);(b)(6);(b)(3):10 USC 424

Date: Thursday, August 04, 2011 12:56:57 PM

CLASSIFICATION: ~~SECRET~~ (b)(3) 50 USC 3024(i) ~~NOFORN~~

(b)(1);(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

Update on Cables in the Public Domain

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

(U) Journalists continue to exploit the leaked cables as a reference archive when breaking news events occur around the globe. Early-to-mid July press reporting highlights included media use of leaked cables to cast blame on the U.S. government for pressuring Cyprus in 2009 to seize and secure the illegal shipment of cargo from Iran to Syria that recently exploded in Cyprus, and subsequently to fault the Cypriot government for not taking advantage of training offered by the UN that might have prevented the disaster. The Cypriot Naval Chief is among the dead, and several senior Cypriot defense officials have since tendered their resignations. In the wake of the shooting tragedy in Norway in late July, media outlets seized on cables that discussed Norway's attitudes toward terrorism and preparedness for a terrorist event.

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

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

(b)(1);(b)(5);(b)(3):10 USC 424;Sec. 1.4(c);Sec. 1.4(d);(b)(3):50 USC 3024(i)

Update on the Assange Memoir

The Assange memoir, already overdue, now appears to be on hold indefinitely.

Timeline:

28 March 2011 - Heather Brooke (*The Guardian*) tweeted hearing on the literary grapevine that Julian Assange's memoir had been pushed back to June. (Twitter – newsbrooke)

15 April 2011 – WikiLeaks Versus the World: My Story was scheduled for release April 7, but failed to make the deadline – Canongate told *The Standard*: "Publishing dates change all the time." No revised date for the book's release was given. (echonews.com)

6 July 2011 - *The Guardian* reported a million-pound book deal by Assange to write his memoirs had collapsed after the WikiLeaks founder became unhappy with the process. He is thought to have told publishing sources the book could give ammunition to US prosecutors, whom he fears may seek his extradition on terrorist charges relating to WikiLeaks disclosures. Publishers are waiting to comment until after a decision is reached in the UK High Court hearings of 12 and 13 July.

Update on the UK High Court extradition appeal hearings 12 and 13 July 2011

Still no ruling following Assange's 12-13 July extradition hearing.

The two-day hearing dealt with Assange's application to overturn a lower court's rejection in February of defense arguments that he would have an unfair trial in Sweden. Lawyer Mark Summers closed the defense's case on Wednesday by reiterating arguments that the European arrest warrant issued by Sweden was invalid because Assange is only wanted for questions and has not been charged. The reality of the case is also that no decision to prosecute or charge has been made. The preliminary investigation remains open. (AFP)

If Assange's High Court appeal is unsuccessful, he could take his case to the Supreme Court, the highest court in the land. (The Guardian – 12 July 2011)

DERIVED FROM: ~~MC~~
DECLASSIFY ON: ~~25X1~~
DATE OF SOURCE: ~~20110803~~

CLASSIFICATION: ~~SECRET~~ (b)(3);50 USC 3024 (i) ~~NOFORN~~

#595

From: (b)(6),(b)(3):10 USC 424,(b)(3):50 USC 3024(i)
To:
Cc:
Subject:
Date: Tuesday, July 19, 2011 3:53:20 PM
Attachments: (b)(3):50 USC 3024(i)

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(5),(b)(6),(b)(3):10 USC 424,(b)(3):50 USC 3024(i)

From: [redacted]
Sent: Tuesday, July 19, 2011 12:04 PM
To: [redacted]
Cc: (b)(6),(b)(3):10 USC 424,(b)(3):50 USC 3024(i)
Subject: [redacted]

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

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

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

(U) *Russkiy Reporter* online magazine (*Russian Reporter*, <http://rusrep.ru>) started reporting on the Georgia cables on 29 November 2010 named "The War with Georgia." (*Russian Reporter*, <http://rusrep.ru>)

(U) The *Russkiy Reporter* received 117 cables from WikiLeaks that were not published elsewhere. Origins for cables published in the *Russian Reporter* on the Russia-Georgia conflict in August 2008 cited at www.xs4all.nl/~aebr/wl/rusrep/georgia.html:

:
TBILISI USNATO USUNNEWYORK STATE BEIJING
YEREVAN BUDAPEST ANKARA COPENHAGEN OSLO
BERLIN VILNIUS OTTAWA

WARSAW THEHAGUE REYKJAVIK LISBON PRAGUE TOKYO
JAKARTA RIGA TALLINN STOCKHOLM ATHENS
BRATISLAVA PARIS

ROME BAKU BRUSSELS HELSINKI LONDON
MOSCOW LJUBLJANA MADRID KYIV TELAVIV CARACAS

(b)(5);(b)(6);(b)(3):10 USC 424;(b)(3):50 USC 3024(i)

(b)(6),(b)(3):10 USC 424

CLASSIFICATION: UNCLASSIFIED/~~FOUO~~

REGRADE UNCLASSIFIED W/O ATTACHMENTS.

DERIVED FROM: ~~██████████~~

DECLASSIFY ON: ~~20360718~~

DATE OF SOURCE: ~~20110719~~

CLASSIFICATION: ~~SECRET/NOFORN~~

#597

From: (b)(6),(b)(3):10 USC 424;(b)(3):50 USC 3024(i)
To:
Subject:
Date: Saturday, December 18, 2010 4:35:18 PM

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(5)

From: (b)(6),(b)(3):10 USC 424;(b)(3):50 USC 3024(i)
Sent: Friday, December 17, 2010 8:15 AM
To:
Cc:
Subject:

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(5),(b)(6),(b)(3):10 USC 424;(b)(3):50 USC 3024(i)

WikiLeaks Staff Cited on Infighting, Internal Operation of Whistleblower Site (U//~~FOUO~~)

EUP20101216024001 Rotterdam NRC Handelsblad Online in Dutch 15 Dec 10 (U//~~FOUO~~)

[Report by Leonie van Nierop: "The WikiLeaks Youngsters Are Idealistic, They Want To Manipulate Systems" (U//~~FOUO~~)

[OSC Translated Text]

Reykjavik, 15 December -- A relatively large number of former employees of the core group running WikiLeaks live in Reykjavik. They are only too pleased to talk about the whistleblowing website. "I don't like to play James Bond."

At the Kormaks og Skjaldar beer house in the capital Reykjavik there is a lot of talk about WikiLeaks. The talk is mainly about the criminal charges against the Australian

founder Julian Assange for sex offenses. To be precise ; About the question of whether the Swedish women involved are hysterical and jealous lesbian feminists or are under the influence of the CIA.

There are also criticisms of WikiLeaks. Because the foundation that supports the soldier Bradley who is suspected of making the leaks is said not to have received a single cent of the money that WikiLeaks collected for him. Because evil tongues claim that the media have to pay large sums of money to gain access to the quarter of a million US diplomatic cables, just a fraction of which are published. Because chaos has allegedly broken out internally following Assange's arrest last week in London. Because the organization that advocates openness itself remains a mystery.

Such malicious talk is being spread not least of all by people who have left WikiLeaks in recent years. Although on the Internet they say that they have no comment to make about Assange or WikiLeaks, they are only too willing to talk, and openly. Also the Icelanders, which make up a relatively large proportion of the small core that runs the whistleblowing site, are easier to reach than is generally believed. Three former members of the team and three current members spoke in Reykjavik about who they are and how the organization operates. To protect their safety, names have been omitted.

The unverifiable "facts" they provide: The permanent inner core consists of -- in addition to Assange and at least three Icelanders -- a Brit and an Australian university employee. The only two or three hackers who are familiar with the entire web infrastructure take great care to remain anonymous. And although the organization runs largely on trust, there is a high rate of turnover about the associates. Of the nine people who worked for WikiLeaks in March at least five have left.

Internet activist Smari McCarthy (26) is one of the few former employees who left in the last year without having a row. He still has contacts with Wikileaks, has been able to see all the cables and fully supports their circulation. Other aspects he is less enthusiastic about. Such as having to constantly change telephone number for fear of the intelligence services. "Some get a kick out of it but I don't like playing at James Bond."

He followed the traditional career path of a hacker. As a youngster -- the kind of youngster who finds pleasure in taking a toaster apart -- he was given a computer on his twelfth birthday. He soon discovered he could improve it and discovered similar souls in chatrooms with whom he talked technicalities. McCarthy: "It was only later that I heard about the bigger problems in the world, also offline. We slowly became politicized." In 2001 he attended his first hackers congress in Amsterdam, about self-determination on the web. Nine years later he helped Assange produce the video showing US soldiers shooting dead civilians and journalists in Baghdad.

McCarthy describes himself as "a hacker in the positive sense of the word." A hacker is not somebody who breaks into computers to steal, but somebody who is interested in "manipulating the system." And precisely this interest in a higher mission, absolute freedom of information, is something that McCarthy finds is now lacking on

WikiLeaks. "They seem to be interested in quick scoops not in changing the system."

The legal case in Sweden also bothers hm. "Through his insinuations that the charges are politically motivated, Assange has become a martyr. But that is playing into the hands of the United States. All the attention focusing on him is not focusing on the diplomatic cables."

There is not the romantic image of Assange as the vilified man prepared to take on the rest of the world. He is also seen as a paranoid and self-obsessed autocrat. Former employees say that all decisions had to pass through him, which is difficult when somebody is on the run or in jail. That is possibly why the German foundation Wau Holland, which manages a part of the funds, has not yet transferred any money to support Bradley Manning.

Since Assange's arrest Kristinn Hrafnsson has been the WikiLeaks spokesperson out of London. The Icelandic investigative journalist travelled to Iraq at the beginning of the year to produce the video. Last weekend he was briefly in Reykjavik. He denies that the media pay for the information. He attributes the rumor to the "excessive attacks" on WikiLeaks. But he says little else. He will not say what is contained in the locked file that WikiLeaks is advising everybody to download in the event of Wikileaks going under, or at what point the key to unlock it will be released. "We are still a long way from that moment. And we hope that it never comes to that."

According to WikiLeaks there are still hundreds of volunteers for its cause. For example 25-year-old Herbert Snorrason. When, in the summer of 2009, Wikileaks published an explosive piece about an Icelandic bank, he asked WikiLeaks in a chatroom for some technical details. He continued to hang out there. When a year later the chatroom was flooded out, following the release of around 90,000 documents about the war in Afghanistan, Snorrason himself started to moderate and to answer questions. WikiLeaks was happy to let him continue. Since then he has helped with about 40 other volunteers to remove personnel details from 15,000 of these documents.

Snorrason's activities for WikiLeaks ended when in a chatroom conversation with Assange he defended Daniel Domscheit-Berg (known at the time as Daniel Schmitt). This 32-year-old German left in September after conflict with Assange, who Domscheit-Berg claimed was dictatorial in his behavior and only interested in dramatic revelations. When Snorrason complained, Assange wrote "piss off." And that was it for Snorrason.

His revenge is sweet. Soon he will be launching a rival whistleblowing website with Domscheit-Berg: [OpenLeaks](#). The founders have high hopes for it. WikiLeaks wishes it all the best. Because on one thing friend and foe are agreed: This information revolution is unstoppable.

[Description of Source: Rotterdam NRC Handelsblad Online in Dutch -- Website of prestigious left-of-center newspaper; URL: <http://www.nrc.nl>]

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

#629

The next 4 pages are withheld
in full and are not included.

~~SECRET//NOFORN~~

INFORMATION REVIEW TASK FORCE
SUMMARY REPORT

(b)(3):10 USC 424;(b)(3):50 USC 3024(f)

30 March 2011

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

Information Review Task Force
Defense Counterintelligence and Human Intelligence Center
Defense Intelligence Agency

Derived From: ~~Multiple Sources~~
Declassify on: ~~OSI~~

~~SECRET//NOFORN~~

The next 28 pages are withheld in full and are not included.

~~SECRET//NOFORN~~

(b)(3):10 USC 424;(b)(3):50 USC 3024(i);(b)(5)

(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.

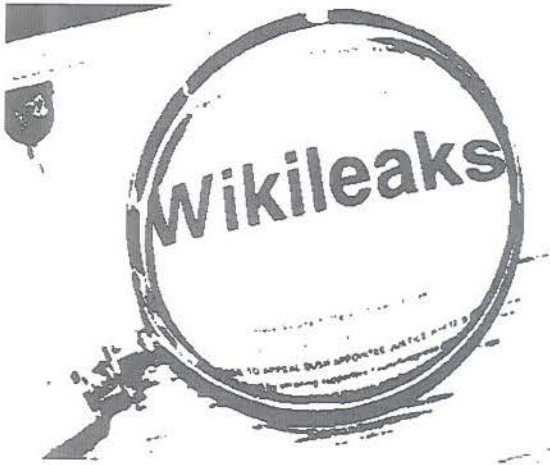
(b)(3):10 USC 424

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

~~SECRET//NOFORN~~

The remaining 5 pages are withheld in full and are not included.

APPENDIX B – General Background Information on WikiLeaks (U)



(U) WikiLeaks is a publicly accessible Internet website that hosts 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.

"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.

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

⁷ (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.

#632

The next 21 pages are withheld in full and are not included.

~~SECRET//NOFORN~~

Information Review Task Force Summary Report:

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

21 December 2010



*Information Review Task Force
Defense Counterintelligence and Human Intelligence Center
Defense Intelligence Agency*

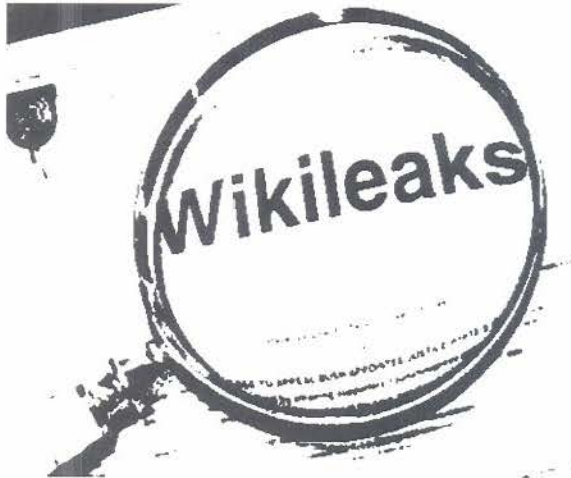
Derived From: ~~DoDI C-5240-8~~

~~Reason 1.4(c)~~

Declassify on: ~~21 December 2035~~

~~SECRET//NOFORN~~

APPENDIX A – GENERAL BACKGROUND INFORMATION ON WIKILEAKS (U)



(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 way for people with damning, potentially helpful, or just plain embarrassing information to make it public without providing any linkage back to the source who leaked or disclosed the information.

"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.

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

⁶ (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.

#034

The next page is withheld in full and is not included.

UNCLASSIFIED

Information Review Task Force WikiLeaks National Defense and Security Impact Brief (U)



IRTF Brief to
Offices of the Attorney General and Deputy Attorney General
2 February 2011

This briefing is classified
~~TOP SECRET~~ (b)(3); 50 USC 3024 (f) ~~NF~~

Derived from: ~~Multiple Sources~~
Declassify on: ~~20060106~~



CELEBRATING OUR LEGACY
FORGING OUR FUTURE

UNCLASSIFIED



What is WikiLeaks Doing?

According to Assange:

- **(U//~~FOUO~~) Harm the US War Effort:** *“The most dangerous men are those who are in charge of war. And they need to be stopped.” “I enjoy helping people who are vulnerable. And I enjoy crushing bastards. So it is enjoyable work.”*
- **(U//~~FOUO~~) Expose Sources:** *“We are not obligated to protect other people’s sources,” including sources of “spy organizations or militaries.” ...the Afghan public “should know about” people who have been involved in “genuinely traitorous” acts.*



PHOTOGRAPH BY KI PRICE

YANITYFAIR.COM



QUESTIONS

(b)(3):10 USC 424





Backup Slides

(b)(3):10 USC 424





More Media Outlets Gain Access to Unreleased Cables

- (U) WikiLeaks-approved cable transfer
 - (U) **La Nación**— Costa Rican daily newspaper - received 827 cables from Assange in late-February
 - (U) **El Pais**— Uruguayan daily newspaper - received approximately 345 cables from Assange in late-February

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

- (U) Cable transfers outside WikiLeaks' control
 - (U) **15 Minutes**- a free Lithuanian daily newspaper - gained access an unspecified number of cables, likely via **Aftenposten**

50th

713

The next page is withheld in full and is not included.

(b)(3):10 USC 424;(b)(5);(b)(6)

From:
To:
Cc:
Subject:
Date:

Thursday, July 14, 2011 2:17:13 PM

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(1);(b)(3):10 USC 424;(b)(6);Sec. 1.4(c);Sec. 1.4(d)

From:

Sent: Thursday, July 14, 2011 2:11 PM

To:

Cc:

(b)(3):10 USC 424;(b)(5);(b)(6)

Subject:

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(1);(b)(5);Sec. 1.4(c);Sec. 1.4(d)

From:

Sent: Thursday, July 14, 2011 2:07 PM

To:

Cc:

(b)(3):10 USC 424;(b)(6)

Subject:

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(1);(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

Update on the Assange Memoir

The Assange memoir, already overdue, now appears to be on hold indefinitely.

Timeline:

28 March 2011 - Heather Brooke (*The Guardian*) tweeted that she heard on the literary grapevine that the Julian Assange memoir had been pushed back to June. (Twitter – newsbrooke)

15 April 2011 – WikiLeaks Versus the World: My Story was due to be released April 7, but failed to make the deadline – Canongate told *The Standard*: "Publishing dates change all the time." No revised date for the book's release was given. (echonews.com)

6 July 2011 - *The Guardian* reported that the million pound book deal by Assange to write his memoirs had collapsed after the WikiLeaks founder became unhappy with the process. He is thought to have told publishing sources that the book, ..., could give ammunition to US prosecutors, whom he fears may seek his extradition on terrorist charges relating to WikiLeaks disclosures. Publishers are waiting to comment until after the UK high court hearings 12 and 13 July.

Update on the UK High Court extradition appeal hearings 12 and 13 July 2011

The two-day hearing was dealing with Assange's application to overturn a lower court's rejection in February of defence arguments that he would have an unfair trial in Sweden. Lawyer Mark Summers closed the defence's case on Wednesday by reiterating arguments that the European arrest warrant issued by Sweden was invalid because he is only wanted for questions and has not been charged. The reality of the case is also that no decision to prosecute or charge has been made. The preliminary investigation remains open. (AFP)

If Assange's High Court appeal is unsuccessful, he could take his case to the Supreme Court, the highest court in the land. (The Guardian – 12 July 2011)

It is estimated that a ruling will not be immediate. Assange was reserved and unusually quiet and his lawyers were guarded in their statements. (UK Huffington Post)

CLASSIFICATION: ~~SECRET//NOFORN~~

DERIVED FROM: ~~xxx~~

DECLASSIFY ON: ~~20360712~~

DATE OF SOURCE: ~~20110714~~

CLASSIFICATION: ~~SECRET//NOFORN~~

DERIVED FROM: ~~xxx~~

DECLASSIFY ON: ~~20360712~~

DATE OF SOURCE: ~~20110714~~

CLASSIFICATION: ~~SECRET//NOFORN~~

#714

From: (b)(3):10 USC 424;(b)(6)
To:
Cc:
Subject: RE: More Wikileaks News - 9 Feb 2011
Date: Thursday, February 10, 2011 6:42:04 PM
Attachments: [image001.png](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image006.png](#)

CLASSIFICATION: UNCLASSIFIED

Thank you

(b)(3):10 USC 424;(b)(6)

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From: (b)(3):10 USC 424;(b)(6)
Sent: Thursday, February 10, 2011 6:27 PM
To: (b)(3):10 USC 424;(b)(6)
Cc:
Subject: FW: More Wikileaks News - 9 Feb 2011

CLASSIFICATION: UNCLASSIFIED

(b)(3):10
USC 424

(b)(3):10 USC 424;(b)(3):50 USC 3024
(i),(b)(6)

See below. If so, it's all over the net

(b)(3):10 USC 424;(b)(6)

From: (b)(3):10 USC 424;(b)(6)
Sent: Wednesday, February 09, 2011 3:39 PM
To: (b)(3):10 USC 424;(b)(6)
Subject: More Wikileaks News - 9 Feb 2011

CLASSIFICATION: UNCLASSIFIED

WIRED

Anonymous Hacks Security Firm Investigating It; Releases E-mail



This domain has been seized by Anonymous under section #14 of the rules of the Internet.

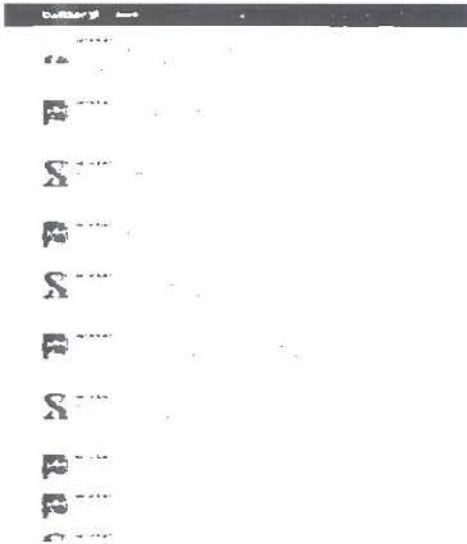
A U.S. security firm that claimed to have uncovered the real identity of Anonymous members responsible for a recent spate of web site attacks became a victim of Anonymous itself, when members of the online vigilante group breached the company's network and stole more than 60,000 internal e-mails.

The group posted the e-mail spool Sunday on the Pirate Bay torrent site for anyone to download and sift through.

HBGary Federal, which does classified work for the U.S. federal government among other security work, claimed it had been working with the FBI to unmask hackers behind recent denial-of-service attacks against PayPal, Visa, MasterCard and Amazon. Members of Anonymous — a loosely structured group of internet troublemakers — had organized the mass attacks after the companies suspended accounts used by WikiLeaks to receive donations and host documents. More recently, members of the group directed denial-of-service attacks against government web sites in Tunisia and Egypt.

Last month, the FBI announced it had executed more than 40 search warrants against people suspected of participating in the WikiLeaks-related attacks. British police also arrested five men in relation to the attacks.

The hack against HBGary Federal occurred after the Financial Times published a story on Saturday quoting Aaron Barr, CEO of the company. Barr said his company's researchers had uncovered clues to the real identities of top members of Anonymous by monitoring chat rooms and Facebook groups they frequented. Barr identified a co-founder of the group, who goes by the name Q, and said he planned to give some of the information to the FBI. He also planned to present his findings at a security conference in San Francisco next week.



On Sunday, Anonymous ridiculed the company's research skills and the accuracy of its data in a press release posted at Daily Kos, mocking the company's "infiltration of our entirely secret IRC server anonops.ru and in particular our ultra-classified channels #opegypt, #optunisia, and, of course, #reporters, which itself is the most secret of all."

In addition to the sudden disappearance of Anonymous leader Q, Anonymous co-founder Justin Bieber also disappeared just before his top-secret mission to Eritrea to offer physical succour to the rebels, suggesting that Mubarak is in our base, eating our Cheetos, likely with military support authorized by Hill Dawg.

The group then hacked into the HBGary Federal web site and e-mail servers, and replaced the web site content with a lengthy message taunting the security firm for failing to protect its own network and for trying to gain attention by marketing its research on Anonymous.

"Your recent claims of 'infiltrating' Anonymous amuse us, and so do your attempts at using Anonymous as a means to garner press attention for yourself. How's this for attention?," the message reads. "You've tried to bite at the Anonymous hand, and now the Anonymous hand is bitch-slapping you in the face."

```
From: Greg England <greg@hbgary.com> [mailto:greg@hbgary.com]
To: Justin Bieber <jbeber@anonops.ru>
Subject: [mailto:jbeber@anonops.ru]

Hi, in Europe and need to ssh into the server. Can you drop ssh up
firewall and allow ssh through port 22022 or something like that?
and if not your password is j1158210s14k148 or did we change it?
83x-004 $ $
Thanks

From: Justin Bieber <jbeber@anonops.ru> [mailto:jbeber@anonops.ru]
To: Greg England <greg@hbgary.com>
Subject: [mailto:jbeber@anonops.ru]

Hi, do you have public ip? or should i just drop port
and if so why. The network team access allowed.

From: Greg England <greg@hbgary.com> [mailto:greg@hbgary.com]
To: Justin Bieber <jbeber@anonops.ru>
Subject: [mailto:jbeber@anonops.ru]

Hi, I don't have the public ip with me at the moment because I have
for a small writing and I'm in a rush
if anything just have my password (a change it) and give me public
ip and I'll ssh in and reset it for you.

From: Justin Bieber <jbeber@anonops.ru> [mailto:jbeber@anonops.ru]
To: Greg England <greg@hbgary.com>
Subject: [mailto:jbeber@anonops.ru]

Hi,
I have couple guys, I will ssh into other server, ssh keys are 1152
... a little later.

both 128 ssh hbgum@hbg 4 181 141 p 4152
[authentication access prohibited]
hbgum@hbg 14 181 141 x password
[hbgum@hbg hbgum@hbg]
hbgum@hbg hbgum@hbg
11:22:28 up 20 days, 1:42:11, user load: 0.00, 0.00, 0.00
```

The hackers then posted a file purporting to contain the research that Barr had collected on Anonymous members as well as more than 50,000 e-mails in Barr's account. The group claimed to have financial details for the company and threatened to erase content on the company servers.

The group also hijacked Barr's Twitter account, sending out tweets as Barr, including a home address and Social

Security number purporting to belong to him.

In addition to the HBGary site, the hackers gained root access to Rootkit.com, an online forum dedicated to analyzing and developing stealthy "rootkit" malware technology. The forum was founded by Greg Hoglund, CEO of HBGary, a separate security firm that owns about 15 percent of HBGary Federal. They seized Hoglund's e-mail account and then posed as him in order to manipulate a Rootkit.com administrator named Jussi Jaakonaho into giving them root access to Rootkit.

Hoglund, Barr and Hoglund's wife Penny, president of HBGary, tried to negotiate with the hackers via phone and chats to get the company's data taken down, stating that Hoglund's e-mails shouldn't be exposed because he has little to do with HBGary Federal and that disclosure of some of the data would cost his company millions of dollars. The group ultimately agreed to remove links to the published e-mails for this reason, according to an online post from an Anonymous member.

Hoglund declined to comment on the hack.

REUTERS

WikiLeaks Bank Of America Documents Could Be A Snore, Founder Suggests

LONDON: The bombshell that WikiLeaks founder Julian Assange has said could "take down a bank or two" may in fact be something of a dud.

Assange has said privately he does not know if his cache of internal Bank of America (BAC.N) data, whose public release he has suggested might be imminent, contains any big news or scandal, according to three people familiar with the WikiLeaks leader's private discussions about the material.

They said that Assange said it consists of e-mails from the hard-drive of a Bank of America executive's computer and that the latest messages are dated sometime in 2006.

The sources said that Assange privately acknowledged the material was not self-explanatory and that he personally was unable to make much sense of it. Assange indicated it would require a substantial amount of effort by financial experts to determine whether any of the material was newsworthy, according to the sources.

Assange's private characterizations of the Bank of America material as being dated and difficult to interpret contrasts with inflammatory public statements he has made -- some as recently as last month -- touting the significance of bank-related materials WikiLeaks has been planning to publish.

A person who works with Assange did not respond to an emailed request for comment.

In an interview in November with Forbes, Assange said WikiLeaks planned early in 2011 to release "either tens or hundreds of thousands of documents depending on how you define it" from a cache of material the website had received from an unnamed American bank. Assange said the material would highlight "some flagrant violations, unethical practices" and added that it could "take down a bank or two."

In the Forbes interview, Assange wouldn't identify which U.S. bank the material came from. In an interview last month with U.S. television program "60 Minutes," Assange again declined to identify which bank his cache of data came from, claiming to the CBS newsmagazine: "There'll be a process of elimination if we denied some and admitted others... I think it's great. We have all these banks squirming, thinking maybe it's them."

But in an interview with Computerworld magazine in October, 2009, he said "We are sitting on 5GB from Bank of America, one of the executive's hard drives."

The contrast between the schadenfreude with which he has talked about the bank documentation in public and

the caution with which he has described the material in private may provide fresh ammunition to opponents of Assange, who have accused him of hyping revelations and promoting conspiracy theories for personal and political gain. His critics include former WikiLeaks collaborators, who allege Assange has sought to dominate WikiLeaks by fostering a cult of personality.

Assange and WikiLeaks have become international media phenomena because he has delivered on some of his claims -- particularly through WikiLeaks' acquisition and publication of thousands of classified U.S. government reports about diplomatic machinations and the wars in Iraq and Afghanistan.

WikiLeaks critics have also accused Assange of exaggerating the importance of the leaked official documents, and some internal U.S. government assessments of the impact of WikiLeaks' publication of American government secrets have suggested that long-term damage to U.S. interests and foreign policy are likely to be limited.

Some former WikiLeaks collaborators who split away from the website due to what they regarded as Assange's erratic and imperious behavior said that over the last year, he had lost interest in publishing financial secrets which had flowed into the website and was much more enthusiastic about publishing material which would irritate or damage the U.S. government.

Last month, Assange appeared at a London press conference where Rudolf Elmer, former head of a private Swiss bank's operations in the Cayman Islands, handed over what purported to be two discs containing documentation of alleged offshore tax abuses by wealthy business people. The day after the press conference, Elmer pleaded guilty in a Zurich court to violating Swiss laws on bank secrecy, and was released without a custodial sentence.

Hours after the court hearing, Elmer's house was raided by Swiss authorities and he was taken away and detained.

(Editing by Claudia Parsons and Jim Impoco)

<http://www.deathandtaxesmag.com>

FBI's Twitter Probe Into WikiLeaks Supporter Challenged by ACLU and EFF

By DJ Pangburn Wednesday, February 09, 2011

Last month, Twitter accounts of WikiLeaks supporters were subpoenaed by the FBI and Twitter was hit with a gag order. Twitter fought and won the right to inform their users of the subpoena. Now the ACLU and EFF have stepped in.



Birgitta Jonsdottir is a one-time WikiLeaks supporter and current member of the Icelandic parliament, but that did not stop the FBI from subpoenaing her Twitter account.

According to the Electronic Frontier Foundation's website:

"The Electronic Frontier Foundation (EFF) and the American Civil Liberties Union represent Birgitta Jonsdottir, a member of the Icelandic Parliament, in response to the efforts by the U.S. Department of Justice to seek information and records about her online activities as part of the investigation into Wikileaks."

The case is called In the Matter of the 2703(d) Order Relating to Twitter Accounts: Wikileaks, Rop_G, IOERROR; and BirgittaJ.

On January 26th, the EFF and ACLU filed two motions in federal court. The first seeks to unseal still-secret records of the subpoena of Twitter accounts, as well as all other businesses who received similar subpoenas.

The second motion "seeks to overturn the court Order issued on December 14 requiring Twitter to hand over private records about some of its users, including Ms. Jonsdottir, Mr. Gonggrijp and Mr. Appelbaum."

The motions were unsealed yesterday, February 8th.

This is an important cause that EFF and the ACLU have taken up, since it is not a crime first of all to support an organization like WikiLeaks, which deals in publishing free information in much the same way as the New York Times did with Daniel Ellsberg's "Pentagon Papers." Which, as we all know, were important cases in the right to publish information relating to government secrets.

(b)(3):10 USC 424;(b)(6)

CLASSIFICATION: UNCLASSIFIED

CLASSIFICATION: UNCLASSIFIED

CLASSIFICATION: UNCLASSIFIED

#720

The remaining 3 pages are withheld in full and are not included.

(b)(3):10 USC 424;(b)(5);(b)(6)

Date: Friday, January 28, 2011 2:26:05 PM
Attachments: NYT Magazine.doc

CLASSIFICATION: ~~SECRET//NOFORN~~

I'm still waiting on the Newsweek article to be moved up...but here's the quote...

Newsweek Online, 09 Sep 2010

[Bureau of investigative Journalism editor Ian] *Overington says that media organizations participating in the [Iraq War] project will be making financial contributions to 'help meet production costs'*

NYT Magazine, 27 Jan 2010:

Much later, some American news outlets reported that they were offered last-minute access to WikiLeaks documents if they signed contracts with financial penalties for early disclosure. The Times was never asked to sign anything or to pay anything. For WikiLeaks, at least in this first big venture, exposure was its own reward.

From:

Sent: Friday, January 28, 2011 11:23 AM

To:

(b)(3):10 USC 424;(b)(5);(b)(6)

Cc:

Subject:

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(1);(b)(3):10 USC 424;(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

#730

From: (b)(3):10 USC 424;(b)(6)
To:
Subject: RE: IRTF Update -- 1700, 23 Oct 2010
Date: Monday, October 25, 2010 12:09:50 PM

CLASSIFICATION: ~~SECRET~~

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

From: (b)(3):10 USC 424;(b)(6)
Sent: Monday, October 25, 2010 11:48 AM
To:
Subject: RE: IRTF Update -- 1700, 23 Oct 2010

CLASSIFICATION: ~~SECRET~~

(b)(1);(b)(3):10 USC 424;(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From: (b)(3):10 USC 424;(b)(6)
Sent: Monday, October 25, 2010 9:27 AM
To:
Subject: RE: IRTF Update -- 1700, 23 Oct 2010

CLASSIFICATION: ~~SECRET~~

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

(b)(1);(b)(3):10 USC 424;(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

From: [REDACTED]

Sent: Monday, October 25, 2010 6:52 AM

To: [REDACTED] (b)(3):10 USC 424;(b)(6)

Subject: FW: IRTF Update -- 1700, 23 Oct 2010

CLASSIFICATION: ~~SECRET~~

FYSA

(b)(3):10 USC 424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From: [REDACTED]

Sent: Saturday, October 23, 2010 4:32 PM

To: [REDACTED]

Cc: [REDACTED]

(b)(3):10 USC 424;(b)(6)

Subject: IRTF Update -- 1700, 23 Oct 2010

CLASSIFICATION: ~~SECRET~~

IRTF Update -- 1700, 23 Oct 2010

(b)(1);(b)(3):10 USC 424;(b)(3):50 USC 3024(f);(b)(5);Sec. 1.4(c);Sec. 1.4(d)

(b)(1),(b)(3):10 USC 424;(b)(5):Sec. 1 4(c);Sec. 1 4(d)

(U) Reporting Trends --

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

(U) The issue of civilian casualties also generally follows two themes – U.S. escalation of force and defensive measures killed hundreds of Iraqis (Guardian – *Civilians Gunned Down at Checkpoints*; Al Jazeera – *Death at a Checkpoint*) and U.S. airstrikes killed a number of Iraqi civilians (Der Spiegel – *Hellfire from the Sky*; Al Jazeera – ‘Crazy Horse’ and *Collateral Damage*). The escalation of force articles generally take a personal tone and highlight the killing of women and children. Most of the U.S. airstrike articles tie in the previously-released “Collateral Murder” video and reference an incident where insurgents allegedly tried to surrender before being killed by U.S. Forces.

(U) Major media outlets also highlighted the negative role Iran has played in the Iraq war (New York Times – *Leaked Reports Detail Iran’s Aid for Iraqi Militias*; Guardian – *Iran Accused of Plotting Attack on Green Zone*; Al Jazeera – *Iran’s ‘Involvement’*). All of these reports document the Islamic Revolutionary Guard Corps-Quds Force (IRGC-QF) and Lebanese Hizballah role in supporting Shia militant activity in Iraq. The New York Times article makes a point of highlighting that U.S.-Iran tensions did not subside following the change in U.S. administration. While all articles draw connections between Iran and some of the more prominent Shia militias (Jaysh al-Mahdi, Badr Corps, Khataib Hizballah) the Al Jazeera article draws some erroneous conclusions linking Iran to cult-like group (Soldiers of Heaven).

(U) Emerging media themes include the role of private security contractors (New York Times – *Growing Use of Contractors Added to Chaos*) and enduring Arab-Kurd tensions (New York Times – *Tensions Remain High Along Kurdish-Arab Line*). Two Al Jazeera articles (*Faith Held Hostage by Violence*; *How Suicide Bombings Shattered Iraq*) highlight violence against Iraq’s religious minorities.

(U) Release Characterization --

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

(b)(1);(b)(3):10 USC 424;(b)(3):50 USC 3024(i);(b)(5);Sec. 1.4(c);Sec. 1.4(d)

(U) IRTF will continue to monitor press reporting and characterize topics in comparison to IRTF expected releases. Our next update will be released Sunday morning.

(b)(3):10 USC 424;(b)(6)

DERIVED FROM: ~~44S~~
DECLASSIFY ON: ~~20351023~~
DATE OF SOURCE: ~~20101023~~

CLASSIFICATION: ~~SECRET~~

DERIVED FROM: ~~44S~~
DECLASSIFY ON: ~~20351023~~
DATE OF SOURCE: ~~20101023~~

CLASSIFICATION: ~~SECRET~~

DERIVED FROM: ~~44S~~
DECLASSIFY ON: ~~20351023~~
DATE OF SOURCE: ~~20101023~~

CLASSIFICATION: ~~SECRET~~

DERIVED FROM: ~~44S~~
DECLASSIFY ON: ~~20351023~~
DATE OF SOURCE: ~~20101023~~

CLASSIFICATION: ~~SECRET~~

DERIVED FROM: ~~44S~~
DECLASSIFY ON: ~~20351023~~
DATE OF SOURCE: ~~20101023~~

CLASSIFICATION: ~~SECRET~~

DERIVED FROM: ~~TOP SECRET~~
DECLASSIFY ON: ~~20351029~~
DATE OF SOURCE: ~~20101023~~

CLASSIFICATION: ~~SECRET~~

#731

From: (b)(3):10 USC 424;(b)(6)
To:
Cc:
Subject: RE: Russia and China Next Wikileaks Targets?
Date: Tuesday, October 26, 2010 2:57:21 PM

CLASSIFICATION: ~~SECRET//NOFORN~~

Thanks

From: [Redacted]
Sent: Tuesday, October 26, 2010 2:06 PM
To: [Redacted]
(b)(3):10 USC 424;(b)(6)
Cc: [Redacted]
Subject: RE: Russia and China Next Wikileaks Targets?

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(1);(b)(3):10 USC 424;(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

From: [Redacted] (b)(3):10 USC 424;(b)(6)
Sent: Tuesday, October 26, 2010 1:36 PM
To: [Redacted]

Subject: Russia and China Next Wikileaks Targets?

CLASSIFICATION: UNCLASSIFIED

FYI

Wikileaks to post Russian, Chinese files
MOSCOW, Oct 26, 2010 (UPI via COMTEX) —

Wikileaks, the Web site that published U.S. Defense Department documents, is getting ready to release secret files from Russia and China, a site spokesman said.

Wikileaks official Kristinn Hrafnsson told the Russian newspaper Kommersant the subjects of the disclosures were the "despotic regimes" in China, Russia and central Eurasia, RIA Novosti reported Tuesday.

"Russians are going to find out a lot of interesting facts about their country," Kristinn said.

Wikileaks last week published some 400,000 secret U.S. military files concerning the Iraq war and also released secret documents on the war in Afghanistan earlier this year. Among other things, the Iraqi-related released documents allege that Iraqi forces beat, burned or otherwise mistreated detainees transferred to their custody by U.S. forces.

The Christian Science Monitor

By Fred Weir, Correspondent / October 26, 2010
Moscow

Wikileaks ready to drop a bombshell on Russia. But will Russians get to read about it?

Wikileaks is about to release documents on Russia, but the tightly-controlled Russian media is unlikely to report them the way Western media attacked the documents about Afghanistan and Iraq

Founder of the Wikileaks website Julian Assange arrives for a press conference on October 23, 2010 during a press conference at the Park Plaza hotel in central London to release previously secret files on the Iraq war. Assange has told Izvestia Wikileaks will release information on Russia soon.

The Kremlin had better brace itself for a coming wave of WikiLeaks disclosures about Russia, the website's founder, Julian Assange, told a leading Moscow newspaper Tuesday.

"We have [compromising materials] about Russia, about your government and businessmen," Mr. Assange told the pro-government daily Izvestia. "But not as much as we'd like... We will publish these materials soon."

He then dropped a hint that's likely to be nervously parsed in Russia's corridors of power: "We are helped by the Americans, who pass on a lot of material about Russia," to WikiLeaks, he said.

Russian security experts say there probably won't be anything comparable to the huge archives of US military secrets from the wars in Afghanistan and Iraq that the website has recently published. 'A lot of interesting facts' about Russia

Assange and another WikiLeaks spokesperson, **Kristinn Hrafnsson**, who talked to the daily **Kommersant Tuesday, refused to provide details. "Russians are going to find out a lot of interesting facts about their country," Ms. Hrafnsson told Kommersant, adding that WikiLeaks would soon be targeting "despotic regimes in China, Russia, and Central Asia" in a series of fresh document dumps.**

"If they are going to disclose details of secret bank accounts and offshore businesses of the Russian elite, then the effect will be shocking," says Stanislav Belkovsky, president of the Kremlin-connected Institute of National Strategy. "Most Russians believe that political leaders and others have siphoned off billions of dollars into foreign accounts, but proof of something like that would be dynamite."

Will Russia see it in the media?

But nobody should expect the tightly-controlled Russian media to report on any WikiLeaks revelations about Russia in the thorough manner that Western media have analyzed the huge troves of documents about Afghanistan and Iraq, says Sergei Strokan, foreign affairs columnist with Kommersant.

"You can expect minimal coverage, without any dangerous details, from major Russian news organizations," he says. "Of course there are independent print publications, and the Internet, where it might get picked up and discussed. But there will be no national discussion, no wider repercussions. This is not a country where media disclosures can lead to political changes."

In fact, a US-based website recently published a huge trove that purported to be secret operational documents of Russia's FSB security service, and no one in Russia even noticed, says Andrei Soldatov, editor of Agentura.ru, an online journal that reports on the secret services.

"Unlike what happens in the US, no Russian journalists even mentioned these materials, which included reports of FSB operations in Ukraine, Turkmenistan, and other countries," says Mr. Soldatov. "No reporters asked the FSB any questions; there was no independent process that might have determined the validity of the documents, or what significance they might have for the Russian public. Nothing at all."

The documents, stamped "top secret," were posted last June on Lubyankapravda.com, a website hosted in the US and registered in Egypt, and mysteriously taken down three weeks later. Visitors now find only a message saying the site is "under construction."

An English translation of Soldatov's article about the episode can be found here. (Pulled - See following)

Mr. Strokan says it's not surprising that "American sources" might be ready to dish up Russian secrets for publication on WikiLeaks.

"It's a whole new world of kompromat [a Russian expression meaning 'compromising materials'] out there," he says. "There are political interests all over the world watching this, and it's dawning on them that WikiLeaks is a powerful new tool for wielding influence or undermining a competitor."

"We're going to see a lot more of this."

Leaks: American and Russian approaches

Andrei Soldatov

The documents published on WikiLeaks may, of course, inflict some damage on American interests in Afghanistan (relations with a couple of generals from Pakistani intelligence are definitely going to be spoiled). At the same time, the leak cannot be said to substantially change our notion of how the war is

being waged in Afghanistan. The task forces tactic is well known from Iraq, the wide use of drones to take out Taliban leaders is no secret at all, and both British and American journalists have written volumes about the ambiguous position, to put it mildly, of Pakistan's ISI (Inter-Services Intelligence).

The publication of these documents is a special instance for completely different reasons. Thousands and thousands of field reports and reports from commanders of small army subdivisions have for the first time fallen into the public sphere, and this has given the public and the expert community access to that information, access to which only a limited circle of people once had. In this case, the significance of the leak is not just in the content of the reports and dispatches. This is a new stage in detailing the picture we are dealing with. It is as if we have gone from 800:600 resolution to modern monitors.

Of course, the country's political situation can also be analyzed based on the arrangement of deerskin caps on the Mausoleum, but the analysis will be somewhat more precise if there are documents in the public space: first laws, then generals' orders, and now lieutenants' dispatches as well. With each new level of detail it becomes increasingly difficult for the military and special services to distort the picture of what is happening. It is no longer enough to say that our subdivisions were not in the location where civilians died for some reason; it will have to be explained where specifically each platoon was operating on that day; moreover, journalists will know the number and name of the commander of each of them.

It is curious that while the Russian media were writing about the American scandal, predicting the coalition's imminent demise, quite unremarked was another episode bearing a direct relation to Russia -- another leak.

That leak involved the FSB (Federal Security Service) documents, orders and reports stamped top secret, that were published at lubyanskaypravda.com this June. Not only was this the first case of a leak of FSB documents to the Internet over the last ten years (there was one episode when the Georgian special services published the "tally sheet" of a local politician, but the scan of this document looked dubious enough that it attracted almost no attention). Moreover, if in the WikiLeaks case the authors of the dispatches were the junior command, then included on lubyanskaypravda.com were reports prepared by the special services' leadership, including the top man.

If the documents on WikiLeaks clarify certain issues on the war in Afghanistan, the key problem for the United States, then the FSB documents are primarily reports from the FSB's department of Operations Information (DOI), and simply FSB intelligence, about operations in Ukraine, Turkmenistan, and several other former Soviet republics dating to the mid-2000s. The documents not only clarify what exactly FSB has been doing in these countries but even reveals the lack of coordination among the Russian special services. For example, one of the reports talks about a Ukrainian document forged by the FSB that was obtained by the SVR (Foreign Intelligence Service) and reported to the Kremlin as genuine.

It is no accident that I am not quoting details from these documents. The point is that there is one big difference between these documents and the WikiLeaks collection. Unlike the American reports, the FSB correspondence, **although it was put out on the Internet, never did land in the public sphere. The documents were not republished by Russian newspapers, and the site itself was shut down a couple of weeks after the release. The leak interested only Armenian journalists, who on their basis rushed to accuse one of the directors of the local special services of working for Moscow.**

A paradoxical situation arose as a result. Not having fallen into the public sphere, the FSB documents did not become the subject of discussion, which means there was no attempt to verify their authenticity (and it is for this reason that I do not think it proper to quote them in more detail). There were no official inquiries made to the FSB and presidential administration, there were no press conferences with justifications or refutations, and journalists did not verify them based on their own sources. **Consequently, these documents cannot be quoted, and it is as if they do not exist.**

The US Senate just passed a law protecting journalists and authors publishing in the States from lawsuits for slander in other countries (primarily in London), and human rights activists have welcomed this law, partly because it guarantees the legal immunity of website owners who host in the United States from lawsuits from countries with repressive regimes. Certainly this is a positive step but it is hardly going to

significantly improve the situation with free speech and access to information.

At the least, this did not happen in the case of the FSB document leaks. The website lubyanskayaprawda.com was hosted in the United States, and the domain was registered in Egypt; however, it was the inattention of the traditional print press in Russia that kept these documents from being introduced into the public sphere.

Published in Yezhednevnyy Zhurnal 2.08.2010

CLASSIFICATION: UNCLASSIFIED

DERIVED FROM: [REDACTED]

DECLASSIFY ON: [REDACTED]

DATE OF SOURCE: 20101026

CLASSIFICATION: ~~SECRET//NOFORN~~

DERIVED FROM: [REDACTED]

DECLASSIFY ON: [REDACTED]

DATE OF SOURCE: 20101026

CLASSIFICATION: ~~SECRET//NOFORN~~

#736

From: (b)(3):10 USC 424;(b)(6)
To:
Cc:
Subject: RE: Syria: WikiLeaks IDs four who helped finance or hide monies for Syrian regime
Date: Tuesday, August 09, 2011 2:45:39 PM

CLASSIFICATION: UNCLASSIFIED

Thanks

(b)(3):10 USC 424;(b)(6)

From: [Redacted]
Sent: Tuesday, August 09, 2011 2:43 PM
To: [Redacted] (b)(3):10 USC 424;(b)(6)
Cc: [Redacted]
Subject: Syria: WikiLeaks IDs four who helped finance or hide monies for Syrian regime

CLASSIFICATION: UNCLASSIFIED

See following.

(b)(3):10 USC 424;(b)(6)

WikiLeaks IDs four said to have helped Syrian regime
Published: Aug. 9, 2011 at 2:01 PM

BRUSSELS, Aug. 9 (UPI) -- Newly leaked U.S. cables from WikiLeaks identify four men said to have helped finance the Syrian regime or hide money for it.

EUobserver reports the diplomatic notes, dating from 2006 to 2009 and published by WikiLeaks, focus on actions against Syrian President Bashar Assad because of his suspected role in the assassination of pro-Western politician Rafik Hariri in

Lebanon in 2005.

None of the men has been targeted by the punitive measures against Syria by the European Union, which is preparing for additional action this week. **The release of the names comes as the EU and United States prepare to apply diplomatic pressure at a United Nations Security Council meeting on Syria Wednesday.**

In a communique Friday, the White House said leaders of France, Germany and the United States condemned "Assad's continued use of indiscriminate violence against the Syrian people."

The WikiLeaks dispatches identify Fawas Akhras, Morthada Dandashi, Nabil Kuzbari and Zuhair Sahloul.

Akhras, a London-based cardiologist, "is suspected of being another avenue used by Assad to stash funds abroad," a U.S. diplomat's 2008 cable states.

Sahloul, "the most important black-market money changer in Syria," helped stabilize the Syrian pound during a crash in 2005 and, according to an acquaintance, "could move \$10 million anywhere in the world in 24 hours," the cable says.

Kuzbari, a Vienna-based businessman, is said to have helped hide funds for Rami Makhoul, the regime's main financier, and move regime assets abroad.

And according to another cable, Makhoul "deposited significant sums under Dandashi's name in the Damascus branch of the Lebanese Byblos Bank."

© 2011 United Press International, Inc. All Rights Reserved. Any reproduction, republication, redistribution and/or modification of any UPI content is expressly prohibited without UPI's prior written consent.

Read more: http://www.upi.com/Top_News/World-News/2011/08/09/WikiLeaks-IDs-four-said-to-have-helped-Syrian-regime/UPI-87761312912879/#ixzz1UYa7kUH4

CLASSIFICATION: UNCLASSIFIED

CLASSIFICATION: UNCLASSIFIED

#745

From: (b)(3):10 USC 424;(b)(6)
To:
Subject: RE: WikiLeaks claims that it has had its funding blocked
Date: Wednesday, October 20, 2010 6:56:08 AM

CLASSIFICATION: UNCLASSIFIED

(b)(3):10 USC 424;(b)(3):50 USC 3024(i);(b)(6)
meeting on Friday or Monday, nobody knew anything about it.

From: (b)(3):10 USC 424;(b)(6)
Sent: Wednesday, October 20, 2010 6:54 AM
To:
Subject: RE: WikiLeaks claims that it has had its funding blocked

CLASSIFICATION: UNCLASSIFIED

(b)(3):10 USC 424;(b)(6)
This is very interesting. Do we have any more information about (b)(3):50 USC 3024(i) though I'm not surprised that there's such (b)(3):50 USC 3024(i) this is the first I read about it. Does anyone in IRTF have more background (b)(3):50 USC 3024(i) I did not see any reference (b)(3):50 USC 3024(i)
(b)(3):10 USC 424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From:
Sent: Thursday, October 14, 2010 4:42 PM
To: (b)(3):10 USC 424;(b)(6)
Cc:
Subject: FW: WikiLeaks claims that it has had its funding blocked

CLASSIFICATION: UNCLASSIFIED

The Guardian newspaper in the U.K. published the attached article today. Julian Assange is

asserting that Wikileaks' funding has been blocked since 13 Aug. Moneybookers, a British-registered internet payment company that collects WikiLeaks donations, emailed the organization to say it had closed down its account because it had been put on an official US watchlist and on an Australian government blacklist.

We do not know whether or not this will affect the planned release of media articles based upon (b)(3);50 USC 3024(i) reports on 18 Oct. It may help explain why the Wikileaks main server/website has been down for "system engineering" since 28 Sep.

(b)(3);10 USC 424;(b)(5);(b)(6)

CLASSIFICATION: UNCLASSIFIED

CLASSIFICATION: UNCLASSIFIED

CLASSIFICATION: UNCLASSIFIED

#753

~~SECRET~~

(b)(3):10 USC 424

INFO MEMO

~~S~~-10-0237/IRTF

20 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT: (U) Review of Compromised Baghdad Airstrike Video

(b)(1);(b)(3)-10 USC 424;(b)(5);Sec. 1.4(c);Sec. 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 12 July 2007 from rocket propelled grenades (RPGs) and small arms

Derived from: ~~Multiple Sources~~
Declassify on: ~~SECRET~~

~~SECRET~~

(b)(3):10 USC 424

SECRET//REL USA, FVEY

fire. Air Weapons Teams (AWT) 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.

(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 air crews 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 a 5 April 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

Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

SECRET//

(b)(3):10 USC 424

~~SECRET~~

(b)(3):10 USC 424

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 5 April 2010, USCENTCOM released two separate 15-6 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 BDE 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.

(b)(3):10 USC 424;(b)(6)

Derived from: ~~multiple sources~~
Declassify on: ~~2010~~

~~SECRET~~

(b)(3):10 USC 424



Australia Network News

Provided by the ABC Asia Pacific News Centre

Pages 1 and 3-12 are withheld in full and are not included.

WikiLeaks founder Julian Assange is at risk of being assassinated over the release of secret US documents and will remain in hiding for his own security, according to the website's spokesman.

Spokesman Kristinn Hrafnsson said the Australian's safety was at stake after US politicians called for him to face treason charges and an adviser to Canadian prime minister Stephen Harper reportedly said he should be killed.

"We have had threats from governments and commentators, some of them totally preposterous, even calls for the assassination of Julian Assange," Mr Hrafnsson said during a debate at the Frontline Club in London.



QUESTIONS / GUIDANCE

(b)(3):10 USC 424

50th



#762

UK Guardian on Assange and Potential US Charges

- The Guardian: *"...extradition to the US is safe and fair: we should not allow high-profile cases like Julian Assange's to prejudice us against a due process that has full legal safeguards."*
- *There are rigorous standards of evidence, full rights of defence, a well-trained and scrupulous judiciary, an advanced appeals system up to the state and us supreme courts (depending on the nature of the offence) and full transparency.*

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

30th

AnonOps Communications

We are fighters for internet freedom.

[Home](#) [Wikileaks: The Movie](#)

A Warning Message to the Algerian Government

To the Algerian government, we, Anonymous, the people, announce that we will not tolerate acts of violence towards Algerian citizens. What is happening is unacceptable. The starving Algerian people are oppressed by a corrupt government, unable to even voice their anger.

We, Anonymous, the people, demand that the Algerian government stop any and all acts of suppression against its own citizens. The infiltration of disruptive policemen in the demonstration is not within the rights of a state and will not hide the unadorned truth of the dishonourable acts committed by this political regime. We will be paying close attention to the sequence of events in the march scheduled for the Saturday, January 22. It is a crying shame that the protests are not allowed. For each casualty of the repression, the Algerian government will pay a hundredfold, for,

WE DO NOT FORGET HUMAN RIGHTS VIOLATIONS;

WE DO NOT FORGIVE INJUSTICE!



Anonymous says it is preparing operations to hack key Internet sites and portals of the Algerian Government. On its website, the hactivists are promising "for each victim of the repression, the Algerian Government will pay 100 times."



Intro

GlobalLeaks is a project to create a worldwide distributed **Leak Amplification Network** supporting whistleblowers all around the world

The final goal is to reach a network of independent organizations running **GlobalLeaks Amplification Routers** allowing anonymous submission of sensitive material to media (journalists, bloggers, activists, unions) at local/regional level

GlobalLeaks wants to

- **Build** an easy to use software platform
- **Plan** an attack resistant leaking methodology
- **Crowd source** editing/publishing to media in a totally distributed way
- **Create** regional or language specific leak amplification routers that anyone can setup and use to join the network. Each router will maintain it's lists of trusted journalists, bloggers, activists, nqp
- **Reduce, evaluate, and minimize** responsibility
- **Guarantee** the leakers and the nodes anonymity
- **Delegate** the leaks review process to experts in the relative fields
- **Educate** people on how to minimize the risks

We propose a possible model, methodology and hope to be able (we or someone else) to successfully get it up. We are open to receive criticisms and suggestions but most important volunteers support! Spreading Leaks has been showed how helpful is for the democracy (remember: power in the hand of the humanity), and a replicable methodology will make the leaking possible also where non skilled technical people live

Please post your comments in the various sections of the website, we will incorporate your questions, concepts or fixes into the document.

Although they are better described in the other sections of the website, here is a quick look at some schemas that better clarify our concept and what we would like to achieve

UNCLASSIFIED//~~FOUO~~

Wikileaks vs GlobalLeaks: How GlobalLeaks differs from WikiLeaks

Site

Intro

Key points

- Decentralization
- Localized leaking
- Responsibility
- Leak Amplification
- Leaking anonymity
- WikiLeaks comparison

Architecture

- Infrastructure
- Software
 - Research in progress
 - Specifications
- Running a node
- GlobalLeaks network

Submission process

- Leak Amplification Process
- About us
- Get involved!

Events

Blogroll

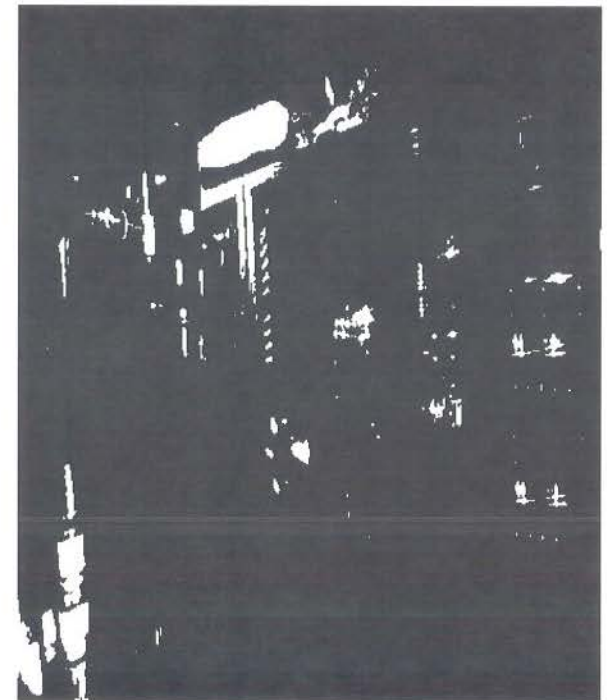
- BalkanLeaks
- BrusselsLeaks
- IndoLeaks
- OpenLeaks
- TimLeaks
- WikiLeaks



#763

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

- Bahnhof, the Swedish ISP and host of WikiLeaks, is moving to encrypt all customer traffic
- This will make detailed logging of customer activities impossible
- The change comes with Switzerland's implementation of the European Data Retention Directive
 - The Directive forces ISPs to store customers logs and provide it to authorities investigating alleged copyright infringement
- Bahnhof will not know what WikiLeaks and other clients are doing



50th



#764

How WikiLeaks Just Set Back Democracy in Zimbabwe

- ~~(U//FOUO)~~ *It's difficult to see this as anything but a major setback for democracy in Zimbabwe. Even if Tsvangirai is not charged with treason, the opponents to democratic reforms have won a significant victory. First, popular support for Tsvangirai and the MDC will suffer due to Mugabe's inevitable smear campaign, including the attorney general's "investigation." Second, the Prime Minister might be forced to take positions in opposition to the international community to avoid accusation of being a foreign corroborator. Third, Zimbabwe's fragile coalition government could collapse completely. Whatever happens, democratic reforms in Zimbabwe are far less likely now than before the leak.*



Morgan Tsvangirai
Zimbabwean opposition leader

the Atlantic

Source: The Atlantic, 28 Dec 2010



#765

Twitter Subpoena

- Julian Assange
- Bradley Manning
- Birgitta Jonsdottir; WikiLeaks volunteer, Icelandic parliament member
- Rop Gonggrijp; Dutch hacker and activist
- USPER; U.S. representative of WikiLeaks



Birgitta Jonsdottir
Icelandic Parliament Member

Source: WIRED, Threat Level Blog
January 7, 2011

“According to the subpoena, the government is seeking the customer’s full contact details (phone numbers and addresses), account payment method if any (credit card and bank account number), IP addresses used to access the account, connection records (“records of session times and durations”) and data transfer information, such as the size of data file sent to someone else and the destination IP. The latter suggests this is a boilerplate request that was likely submitted to other service providers, such as ISPs, social networking sites and e-mail providers, such as Facebook and Google.”



Twitter Subpoena/Legal Update

- According to a statement by WikiLeaks it was legal action by Twitter that brought about the order to unseal the subpoena.
- Assange, Jonsdottir and USPER have indicated they will contest the subpoena
- Julian Assange in court Tuesday for extradition hearing on Swedish Charges

Sources:
WIRED, Threat Level Blog, Jan 7, 2011
Sydney Harold, Jan 10, 2011

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

WikiLeaks was never mentioned by name and greatest concern appeared to be about Jonsdottir's ability to travel.



7666

Assange and the Al-Jazeera Interview

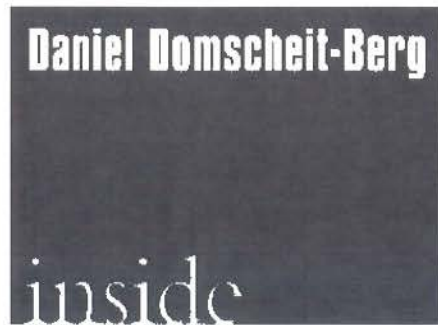
- (U//~~FOUO~~) The one month period during which some major newspapers, like the Guardian, El-Pais, and Le Monde, had the exclusive rights to publish the documents is about to end.
 - "...after that we will publish the documents all over the world. Even the small parties concerned will have their documents."
 - The pace of publishing will increased, and more media outlets will be involved in the process
- (U//~~FOUO~~) Majority of Israeli-related documents not published; about 3700; going to be extremely controversial
 - major world newspapers published what they considered to be important, "not what we consider to be important;" will take four to six months depending on resources
 - "You will see more information about Arab countries and Israel, and this will be published gradually over the next six months."

50th



#767

Daniel Schmitt book to be released



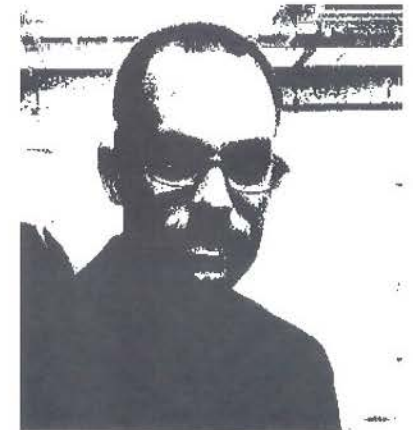
Daniel Domscheit-Berg AKA Daniel Schmitt

Expose titled:
Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website

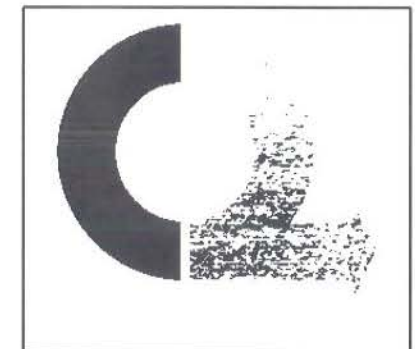
Release Date: 15 February 2011

Likely a catalyst for Openleaks.org launch

Preorder currently available through Amazon



amazon.com



Openleaks.org

50th

Expect media to publicize Domscheit-Berg's book closer to release date; emphasis on new website, inner workings of WikiLeaks, and fall out with Julian Assange



#769

Where are the Russia Cables?

- (U) Novaya Gazeta – Russian opposition newspaper which obtained Russia-related cables from Assange – has published only 2 stories so far
 - (U) Reportedly acquired cables in late Dec 2010 amid much hype about what would be exposed
 - (U) Paper owned by former President Gorbachev and recently elected district legislator Alexander Lebedev
- (U) Statements by Assange and Novaya Gazeta spokesmen suggest money was paid for the publication rights to these cables
- (U) Article questions whether money was actually paid to keep cables out of the public eye

50th



QUESTIONS / GUIDANCE

50th

#786

(b)(3);10 USC 424;(b)(6)

Date: Tuesday, August 30, 2011 4:15:49 PM

CLASSIFICATION: ~~SECRET//NOFORN~~

Good afternoon

(U) We've finally seen a lull in the cable releases – a mere 1,000 new cables have been posted since Friday evening. The latest cable releases include (b)(3);10 USC 424,(b)(3),50 USC 3024(i) and WikiLeaks was quick to note that these releases did include some classified cables (apparently in response to criticism that last week's massive push was overwhelmingly unclassified).

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



#790

WikiLeaks and the DoD CI Insider Threat Program



21 June 2011

Classified by: ~~Multiple Sources~~
Declassify on: ~~AZS~~

This briefing overall classification:

~~SECRET//NOFORN~~



Agenda



- (U) WikiLeaks Update

- (U) XXXXX

- (U) XXXXX



WikiLeaks Update





#791

Defense CI and HUMINT Center (DCIC)

WikiLeaks and the DoD CI Insider Threat Program



(b)(3):10 USC 424;(b)(6)

23 June 2011

Classified by: ~~Multiple Sources~~
Declassify on: ~~XZS~~

This briefing overall classification:

~~SECRET//NOFORN~~



Agenda

- WikiLeaks
- Defense Insider Threat Trend Update
- DCHC Support to the Enterprise



WikiLeaks Update



PHOTOGRAPH BY KI PRICE VANITYFAIR.COM



WikiLeaks Permanently Changes the Disclosure Game

- WikiLeaks was NOT a one-time phenomenon. It represents a 21st Century reality.
- WikiLeaks has been the most covered news story worldwide since 9.11.
- WikiLeaks' stated goals of creating a much more open society by revealing government secrets and "wrong-doing" are regarded positively by large sectors of the world's population, even if members of the public do not condone the group's methods.
- WikiLeaks' success has spawned thousands of mirror sites, imitators and spin-offs.
- Envious of this success, large media organizations, such as the Wall Street Journal and Al Jazeera, have established their own 'leak' portals.



THE WALL STREET
JOURNAL.



QUESTIONS?



#793

Will Pressure on Assange Prompt a Release?

▪ (U) Julian Assange's 'Jewish conspiracy' comments continue to cause controversy; Lawyers claim distortion

▪ (U) British publication quotes Assange as saying the report on Shamir part of a "Jewish" conspiracy Source: UK Guardian

▪ (U) WikiLeaks statement: *"Israel Shamir has never worked or Volunteered for WikiLeaks, in any manner, whatsoever."* Source: twitlonger.com

▪ (U) Daniel Domscheit-Berg said Assange sought out Shamir to collaborate on the WikiLeaks project; that Assange described Shamir's writings as *"compelling..."* Source: Weekly Standard Online

▪ (U) WikiLeaks Slams Spielberg Movie Project Source: Forbes Online

▪ (U) Assange's legal issues

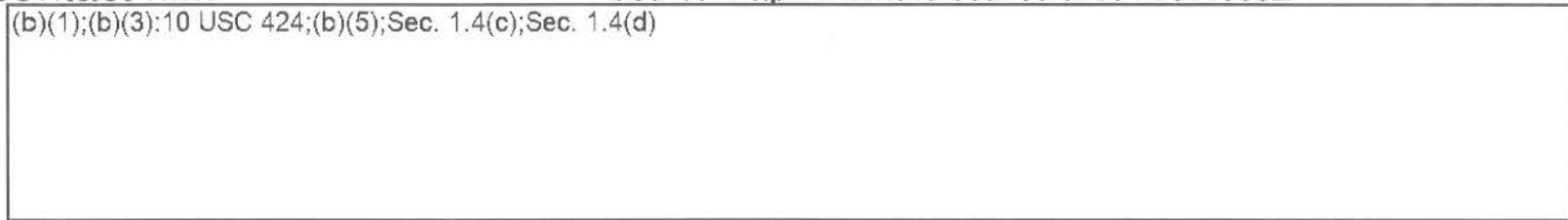
▪ (U) Extradition appeal filed

▪ (U) Swedish lawyer alleged to have purposefully given faulty information about how many times Swedish prosecutors tried to contact him Source: <http://www.thelocal.se/32354/20110302/>



Israel Shamir and Assange

(b)(1);(b)(3);10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)



50th

CELEBRATING OUR LEGACY
FORGING OUR FUTURE



Would GTMO Be Next?

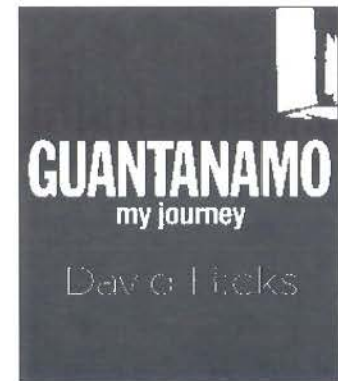
- (U) Australian David Hicks's account of his arrest and incarceration at GTMO released 1 Mar

Source: The West Australian

- (U) Spain to Investigate Torture Allegations at Guantanamo

- (U) Audiencia Nacional gave the green light on Friday to the investigation of a complaint filed by a Moroccan with Spanish residency

Source: Prensa Latina



(b)(1);(b)(3):10 USC 424;(b)(3):50 USC 3024(i);(b)(5);Sec. 1.4(c);Sec. 1.4(d)



22 Additional Charges Preferred Against PFC Bradley E. Manning

- (U//~~FOUO~~) Aiding the enemy in violation of Article 104, Uniformed Code of Military Justice (UCMJ)
- (U//~~FOUO~~) 16 Specifications under Article 134, UCMJ:
 - (U//~~FOUO~~) Wrongfully causing intelligence to be published on the internet knowing that it will be accessed by the enemy (One Specification)
 - (U//~~FOUO~~) Theft of Public Property or Records, in violation of 18 United States Code (U.S.C.) 641 (Five Specifications)
 - (U//~~FOUO~~) Transmitting Defense Information, in violation of 18 U.S.C. 793(e) (Eight Specifications)
 - (U//~~FOUO~~) Fraud and Related Activity in Connection with Computers in violation of 18 U.S.C. 1030(a)(1) (Two Specifications)
- (U//~~FOUO~~) Five specifications in violation of Article 92, UCMJ, for violating Army Regulations 25-2 "Information Assurance" and 380-5 "Department of the Army Information Security Program."
 - (U//~~FOUO~~) Prosecution will not recommend the death penalty to the Convening Authority
 - (U//~~FOUO~~) Trial proceedings have been delayed since July 12, 2010, pending the results of a defense requested inquiry into Manning's mental capacity and responsibility pursuant to Rule for Courts-Martial (R.C.M.) 706.





(b)(3):10 USC 424;(b)(3):50 USC 3024(i);(b)(5)

- (U) Future production will be handled on an ad-hoc basis to respond to RFIs, to support senior travel/counterpart visits, or as deemed necessary based on significant related events.

bth

Pages 2-4 are withheld
in full and are not
included.

UNCLASSIFIED

#795

Information Review Task Force



WikiLeaks Disclosure of Afghan Data (U)

(b)(3);10 USC 424;(b)(6)

20 October 2010

THIS BRIEF IS CLASSIFIED
~~SECRET~~

Derived from: ~~Multiple Sources~~
Declassify on: ~~2005-10-20~~

Current as of: 27Sep 2010 (0800 EST)

UNCLASSIFIED



Information Review Task Force (IRTF)

Mission: review impact of unauthorized disclosures of classified information posted to WikiLeaks website and any associated materials

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

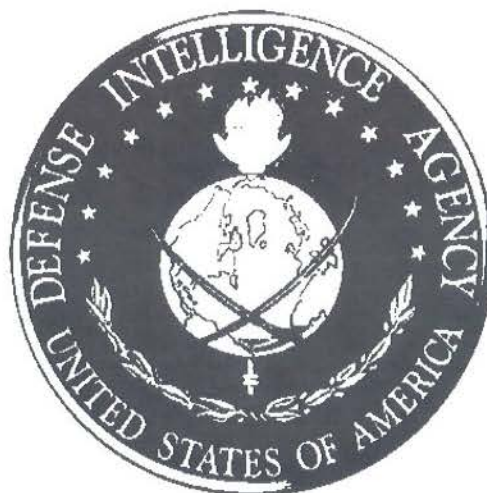


QUESTIONS



#796

WikiLeaks Impact



(b)(3):10 USC 424;(b)(6)

18 July 2011

Derived from: ~~Multiple Sources~~
Declassify on: ~~20260718~~

This briefing is classified
~~TOP SECRET~~ ~~NOFORN~~ (b)(3):50
USC 3024

UNCLASSIFIED



CELEBRATING OUR LEGACY
FORGING OUR FUTURE



Agenda



- (U) Compromised USG Data Sets
- (U) WikiLeaks' Mission and Modus Operandi
- (U) WikiLeaks Impact in South Asia
- (U) Potential Future Impact
- (U) Where to Access WikiLeaks Data

50th



QUESTIONS

50th

CELEBRATING OUR LEGACY
FORGING OUR FUTURE



#798

WikiLeaks Joins Forces With Billionaire Lebedev

- Novaya Gazeta
 - Moscow newspaper controlled by former Soviet leader Mikhail Gorbachev and billionaire Alexander Lebedev
 - Says it is joining forces with WikiLeaks to expose corruption in Russia
 - The weekly newspaper is known in an industry dominated by state-run companies for its critical reports of the Kremlin and investigative coverage of Russian affairs.

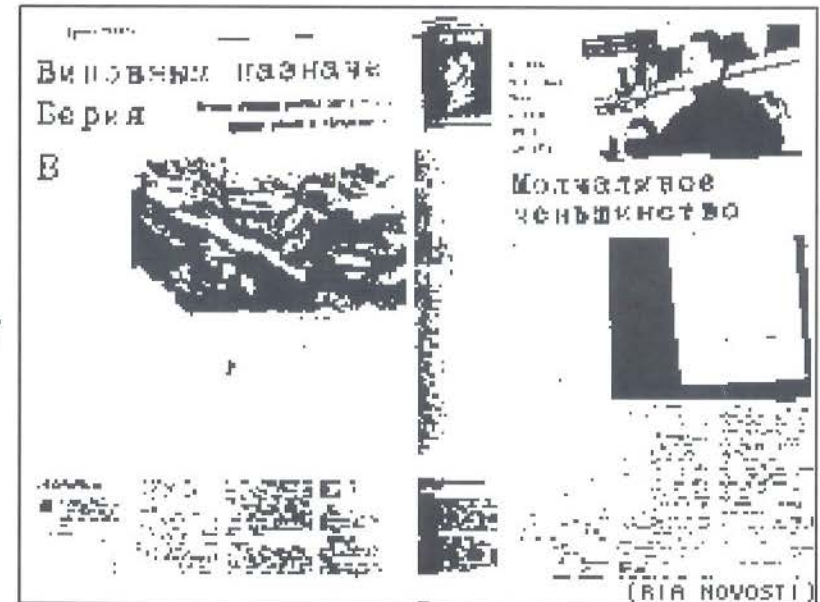


50th



WikiLeaks Joins Forces With Billionaire Lebedev

- Novaya Gazeta reports receiving unlimited access to the WikiLeaks database, which has a "wide range" of materials reportedly including:
 - Documents about the murder of reporter Anna Politkovskaya's murder in 2006
 - Information about Russian politicians' ties to organized crime
- Newspaper says it will start releasing materials next month

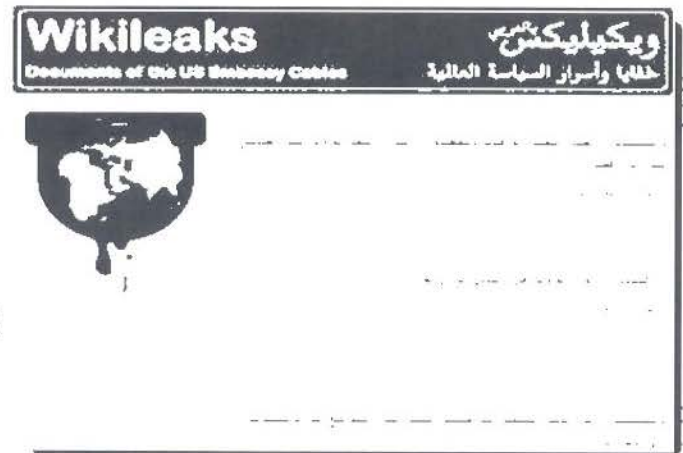


“Assange said that Russians will soon find out a lot about their country and he wasn’t bluffing,” Novaya Gazeta said. “Our collaboration will expose corruption at the top tiers of political power. No one is protected from the truth.”



Jordanian News Sites Translate, Republish WikiLeaks Cables

- Two Jordanian news websites have launched a project to translate WikiLeaks cables issues from the American Embassy in Amman and cables related to Jordan.
 - AmmanNet.net and 7iber.com began this week posting translations of full translations of these cables.



- A special page was created online for this purpose with two categories: cables originated from the US Embassy in Amman, and cables related to Jordan and the Arab region.
 - The page continuously provides unofficial translations of the leaks released on the WikiLeaks website, with a link to the original document in English.

Source: Press





Pages 6-8 are withheld in full and are not included.

Spread of NCD?

- Oslo-based Aftenposten claims they, along with Swedish outlet *Svenska Dagbladet*, gained unrestricted access to all 251,287 cables
 - It also claims it allows them to dodge WikiLeaks' current strategy of drip-feeding the cables to preferred partners The New York Times, The Guardian, Der Spiegel and El Pais. (b)(3):10 USC 424
- Aftenposten news editor Ole Erik Almlid says: "We're free to do what we want with these documents ... We're free to publish the documents or not publish the documents, we can publish on the internet or on paper. We are handling these documents just like all other journalistic material to which we have gained access."
- Around 20 Aftenposten journalists are sifting through the file dump.
 - Articles will be written in Norwegian, which may restrict their immediate impact in the English-speaking media world



#804

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: [redacted]
Date: Monday, August 08, 2011 11:00 AM
Attachments: [redacted].ppt

CLASSIFICATION: [redacted]

(b)(1);(b)(3);10 USC 424;(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

From: [redacted]
Sent: Monday, August 08, 2011 11:00 AM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

CLASSIFICATION: UNCLASSIFIED

(b)(3);10 USC 424;(b)(1);(b)(3);50 USC 3024(i);(b)(5);(b)(6);Sec. 1.4(c);Sec. 1.4(d)

Researchers: Anonymous and LulzSec Need to Focus their Chaos

By Kim Zetter, Email Author
August 6, 2011 | 10:44 pm <http://www.wired.com/threatlevel/>

LAS VEGAS — The online vigilante groups Anonymous and LulzSec are weakening their cause with scattershot attacks and need to get more intelligent and focused, according to a panel of computer security experts at the DefCon hacker conference in Las Vegas.

"We have an opportunity to not just cause chaos, but to cause organized chaos," said Josh Corman, research director at the analyst firm 451 Group, who said the groups are burying their message in noisy denial-of-service and SQL attacks. "I'm suggesting the actions in pursuit of their own goal compromise their goal. There's a way to render more specific what they want to accomplish."

The loosely affiliated groups have launched controversial denial-of-service attacks on PayPal and MasterCard, after the money services stopped processing donations for WikiLeaks, as well as PBS.com after they took issue with a PBS documentary about alleged WikiLeaks source Bradley Manning. They've also masterminded hacks of government contractors, and participated in hacks of Sony.

But Corman said the groups would be better off focusing their energy on more significant things like taking down child-exploitation sites.

"That's something we can all get behind," Corman said.

Another panelist, unimpressed with Anonymous's recent hack of defense contractor ManTech International, said the groups should focus on finding evidence of corrupt governments and exposing things like the Collateral Murder video that WikiLeaks published in 2010, which showed an Army gunship opening fire on a group of civilians in Iraq.

"If you're going to do this, then find the real dirt," said the panelist, who initially appeared on stage in disguise, wearing sunglasses and a scarf to cover his head and the lower half of his face. After audience members called for him to reveal himself, he removed the disguise and identified himself as security blogger Krypt3ia.

The disguise highlighted the fact that many security people fear speaking out publicly against Anonymous and LulzSec after Anonymous hacked the network of HBGary Federal and exposed thousands of emails from the company's then-CEO Aaron Barr. Anonymous targeted the company after Barr was quoted in a news article asserting that he knew the identities of some Anonymous members and would be providing the information to the FBI.

Barr and his company faced intense scrutiny after his exposed emails revealed that they were involved in a shady undercover operation to discredit WikiLeaks and some of the people who support the group. Barr was eventually fired, in an effort by the company to distance itself from the controversial plan.

Barr was scheduled to appear on the DefCon panel but withdrew after HBGary threatened to sue him and his current employer if he spoke about the hack and his former company's anti-WikiLeaks project.

Comran said that in the company's effort to suppress discussion of the issue, it had "put a big target on themselves."

"I've had people come up to me saying 'guess who my next target is? HB Gary,' he said.

The provocative panel, moderated by Paul Roberts, editor of the ThreatPost security blog, also included Jericho, a founding member of Attrition.org, a computer security site that specializes in investigating and exposing industry frauds.

The panel discussion touched on the ethics of Bar's activities, but focused primarily on the activities of Anonymous and LulzSec.

Krypteia accused the groups of not having real goals but of simply wanting "to smash things" and then coming up with a cause by the hacks afterward to defend their actions. He noted that due to the nebulous nature of Anonymous and LulzSec that allows any hacker to claim he's a member of the groups, **corporate spies and nation-state actors can now hide their activities under the umbrella of Anonymous to draw suspicion away from them.**

Jericho called on the community to "build a better Anonymous" to create one that wouldn't cause as much collateral damage from its actions and could have a beneficial effect on the security industry. He suggested that Anonymous and LulzSec might have a role to play in improving computer security by hacking companies that fail to secure their systems despite repeated warnings that they're vulnerable.

If companies "don't do the security they need to do "why not force them to get it," he said. "You're not learning your lessons, so maybe it is time for Anonymous or LulzSec to come in ... and wake them up."

Another fair target he said would be companies that sue researchers who uncover vulnerabilities in their systems or products. Sony, which has experienced ongoing hacks over the last months, was initially hacked over the company's choice to sue SonyPlaystation 3 linker George Hotz.



<http://news.softpedia.com/news/LulzSec-Leader-Sabu-and-The-Jester-Challenge-Each-Other-at-DEFCON-215589.shtml>

CLASSIFICATION: UNCLASSIFIED [REDACTED]

REGRADE: UNCLASSIFIED W/O ATTACHMENTS.

DERIVED FROM: [REDACTED]

DECLASSIFY ON: [REDACTED]

DATE OF SOURCE: [REDACTED]

CLASSIFICATION: [REDACTED]

#960

From:

To:

Cc:

[Redacted]

(b)(3):10 USC 424;(b)(6)

Subject:

RE: WikiLeaks

Date:

Wednesday, September 01, 2010 12:47:35 PM

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(3):10 USC 424,(b)(3):50 USC 3024(i),(b)(5),(b)(6)

[Redacted]

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From:

Sent: Wednesday, September 01, 2010 11:12 AM

To:

Cc:

Subject: WikiLeaks

[Redacted]

(b)(3):10 USC 424;(b)(6)

Classification: UNCLASSIFIED

(b)(3):10 USC 424

Greetings (b)(3):10 USC 424 I've been tasked to be the lead for [Redacted] understanding issues and actions that have been taken relating to [Redacted] WikiLeaks. I remember the initial scrub we did when I was in DC and that [Redacted] for action; however, I can't find any data pertaining to such actions. [Redacted]

(b)(3):10 USC 424;(b)(3):50 USC 3024 (i),(b)(5),(b)(6)

Regards,

(b)(3):10 USC 424;(b)(6)

(b)(6)

Classification: UNCLASSIFIED

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~



#976

The Man Who Spilled the Secrets

- (U//~~FOUO~~) 01 Nov meeting between Assange and Guardian Editor – Assange threatens to sue the paper
- (U//~~FOUO~~) A disgruntled WikiLeaks volunteer had leaked the last big segment of the documents to the Guardian
- (U//~~FOUO~~) The paper was released from its previous agreement with Assange—that The Guardian would publish its stories only when Assange gave his permission.
- (U//~~FOUO~~) *Enraged that he had lost control, Assange unleashed his threat, arguing that he owned the information and had a financial interest in how and when it was released.*



Source: Vanity Fair Online
February 2011

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c)



#979

Information Review Task Force (IRTF)

More Media Outlets Gain Access to Unreleased NCD Cables

- (U) WikiLeaks-approved cable transfer
 - (U) **Le Temps** – French-language newspaper in Switzerland – obtained 5,814 cables from or mentioning Switzerland. **Le Temps** shared cables with **Neue Zürcher Zeitung**
 - (U) **Neue Zürcher Zeitung** – German-language newspaper in Switzerland – received access to cables with **Le Temps**
 - (U) **YLE** – Finnish state-owned public broadcasting – received approximately 1,000 cables related to Finland
 - (U) **La Jornada** – Mexican daily newspaper – received approximately 3,000 cables related to Mexico
 - (U) **El Comercio** – Peruvian daily newspaper – received cables related to Peru and Bolivia
- (U) Cable transfers outside WikiLeaks' control
 - (U) **20 Minutos** - free Spanish daily newspaper - gained access to Spain cables through **Aftenposten**. **20 Minutos** is owned by **Schibsted Media**, who also own **Aftenposten**. **Schibsted** owns similar free daily newspapers in France, Switzerland and Russia
 - (U) **Helsingin Sanomat** received access to Finland cables from **Aftenposten**

50th

#982

(U) WikiLeaks Impact



(b)(3):10 USC 424;(b)(6)

16 August 2011

This briefing is classified

~~TOP SECRET~~

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

UNCLASSIFIED//~~FOUO~~



(U) Agenda

- (U) Compromised Data Sets
- (U) WikiLeaks' Modus Operandi
- (U) WikiLeaks Impact Examples
- (U) Potential Future Impact
- (U) How Did We Get Here?
- (U) WikiLeaks Status/POCs



QUESTIONS



(b)(1);(b)(3):10 USC 424 Sec. 1.4(c);Sec. 1.4(b)

#989



Pages 1-6 are withheld in full and are not included.

Information Review Task Force (IRTF)

WikiLeaks Operational Status

▪ (U) Internet Service Providers



- (U) Bahnhof in Stockholm, Sweden – two servers host WikiLeaks data - resources only – no control over content or management of traffic (Collateral Murder video hosted by Bahnhof.de)

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



- (U) eDot in Zoetermeer, Netherlands – wikileaks.nl

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

- (U) OVH based in Roubaix, France – hosts part of WikiLeaks

SOURCE: ZDNet France 3 Dec 10



- (U) Swiss Pirate Party – wikileaks.ch (points to OVH)
 - International Pirate Party - computer activists - provide servers and network capacities

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



1961 2011
CELEBRATING OUR LEGACY
FORGING OUR FUTURE



WikiLeaks Operational Status

- (U/~~FOUO~~) First week in December 2010 – WikiLeaks.org inaccessible (DDoS)
 - (U/~~FOUO~~) Activated servers wikileaks.de, .fr, .nl, and .ch – with 100 in reserve
SOURCE: *Paris les echos.fr* in French 09 Dec 10 (U/~~FOUO~~)
- (U) Two or three hackers are familiar with entire web infrastructure
 - (U) High rate of turnover of associates - permanent inner core - in addition to Assange and at least three Icelanders - a Brit and an Australian university employee

(b)(3) 50 USC 3024(i)
- (U) Disaffected WikiLeaks volunteers took site's software-based secure-submission platform
 - (U) Group took backlog of previously submitted, leaked material
 - (U) Software was intellectual property of one of departing volunteers
 - (U) Group intends to return material unused and unpublished when WL shows technical ability to keep data/sources safe

UNCLASSIFIED//~~FOUO~~

SOURCE: Domscheit-Berg interview, Wired online 10 Feb 11





WikiLeaks Operational Status

- (U) Assange: For 2011-- will publish more telegrams on countries and more than 100 organizations
 - (U) Need other publications
 - (U) Will expand our structure

SOURCE: Assange interview, *O Estado de S Paulo* 23 Dec 2010

- (U) Jonsdottir: They had to find a way to screen all volunteers who wanted to work with them in order to find out how far they could let them go. Now, WikiLeaks reminds me of a small company that is growing, but its founder does not want to let other people participate in the management. This may destroy the company in the end.

SOURCE: Interview with Icelandic MP Birgitta Jonsdottir, *Bratislava Sme* Online in Slovak 9 Mar 11





Open Source WikiLeaks Reporting

- (U) Twitter Must Turn Over Records In WikiLeaks Case
 - Government attorneys requested the identification of screen names, IP addresses and account activity relating to the three people in question (1 US, 2 Icelandic)
 - Twitter will not hand over the data until the defendants' lawyers have had a chance to appeal the decision
 - Appeals are planned based on alleged violations of the First Amendment



SOURCE: Information Week

#932

DoD Unclassified Talking Points Related to the Compromise of Classified Information by a Former National Security Agency (NSA) Contractor

1. A former NSA contractor downloaded nearly 1.7 million files from Intelligence Community (IC) systems. This is the single greatest quantitative potential compromise of secrets in U.S. history.
2. Much of the information compromised has the potential to gravely impact the National Security of the United States, to include the Department of Defense and its capabilities.
3. While most of the reporting to date in the press has centered on NSA's acquisition of foreign intelligence to protect the lives of our citizens and allies, the files cover sensitive topics well beyond the NSA collection. Disclosure of this information in the press and to adversaries has the potential to put Defense personnel in harm's way and jeopardize the success of DoD operations.
4. These unauthorized disclosures have tipped off our adversaries to intelligence sources and methods and negatively impacted our Allies who partner with us to fight terrorism, cyber crime, human and narcotics trafficking, and the proliferation of weapons of mass destruction. Such international cooperation involving the pooling of information, technology, and expertise is critical to preserve our security and that of our allies.
5. An Information Review Task Force 2 (IRTF-2) of the Department of Defense, led by the Defense Intelligence Agency and working in coordination with elements of the Intelligence Community, is conducting an assessment of the impact to the Department of Defense from the compromise of this information.

Sent to Hill 1/8

9477

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)

(U//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.

(U//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.

(U//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:

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

OSD 09134-10



UNCLASSIFIED//FOR OFFICIAL USE ONLY

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 USD(I) 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~~

INFO MEMO

10-0234/IRTF

1 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1),(b)(3);50 USC 3024(i),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

[Redacted content]

Derived from: [Redacted]
Declassify on: 25X1

~~SECRET~~

The next page is withheld in full and not included.

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

(U) Data Characterization

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

(U) Local Government/Municipality Corruption

(b)(1),(b)(3),10 USC 424,Sec. 1.4(b),Sec. 1.4(c)

(U) Oil/Power Industry Corruption

Derived from: ~~████████████████████~~
Declassify on: ~~██████~~

(b)(1),(b)(3):10 USC 424,Sec. 1.4(b),Sec. 1.4(c)



(U) Sons of Iraq Malfeasance

(b)(1),(b)(3):10 USC 424,Sec. 1.4(b),Sec. 1.4(c)



Derived from: ~~██████████~~
Declassify on: ~~SECRET~~

~~SECRET~~

Prepared by:
Reviewed by:

(b)(3), 10 USC 424, (b)(6)

Derived from: ~~SECRET~~
Declassify on: ~~SECRET~~

~~SECRET~~

The remaining 4 pages are withheld in full and not included.

INFO MEMO

10-XXXX/IRTF

2 February 2011

TO: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

[Redacted content]

(b)(1),(b)(3):10 USC 424,(b)(3) 50 USC 3024(i),(b)(5),Sec. 1.4(c),Sec. 1.4(d)

- (U) According to an open source report dated 16 December 2010, President Colom reacted to the leaked documents by saying that some of the divulged information is inaccurate,

[Redacted]

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

- (U) According to an open source report dated 14 December 2010, Guatemalan officials are avoiding commenting on the cables divulged by Wikileaks, stating that they will wait until they can see what information the cables contain.²

Derived from: ~~Multiple Sources~~

Declassify on: ~~25X1~~

The remaining 3 pages are withheld in full and are not included.

INFO MEMO

10-00XX/IRTF

5 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT: (b)(3) 50 USC 3024(f)

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

(U) Data Characterization

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

INFO MEMO

10-00XX/IRTF

7 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT

(b)(1),(b)(5) Sec. 1.4(c)

Derived from: ~~SECRET//NOFORN~~
Declassify on: ~~SECRET//NOFORN~~

The remaining 2 pages are withheld in full and are not included.

(b)(1),(b)(5),Sec. 1.4(c)

(U) Data Characterization

(b)(1),(b)(3);10 USC 424,Sec. 1.4(b),Sec. 1.4(c)

Derived from: ~~SECRET//NOFORN~~
Declassify on: ~~SECRET//NOFORN~~

INFO MEMO

~~S~~10-00XX/IRTF

07 September 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

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

(b)(1), Sec. 1.4(b), Sec. 1.4(c)

Derived from: ~~SECRET//NOFORN~~
Declassify on: ~~SECRET//NOFORN~~

(U) Data Characterization

(b)(1),(b)(3):10 USC 424,Sec. 1.4(b),Sec. 1.4(c)



Prepared by:
Reviewed by:

(b)(3):10 USC 424,(b)(6)

The next page is withheld in full and not included.

INFO MEMO

S-10-XXXX/IRTF

8 February 2011

TO: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1),(b)(5),Sec. 1.4(c),Sec. 1.4(d)

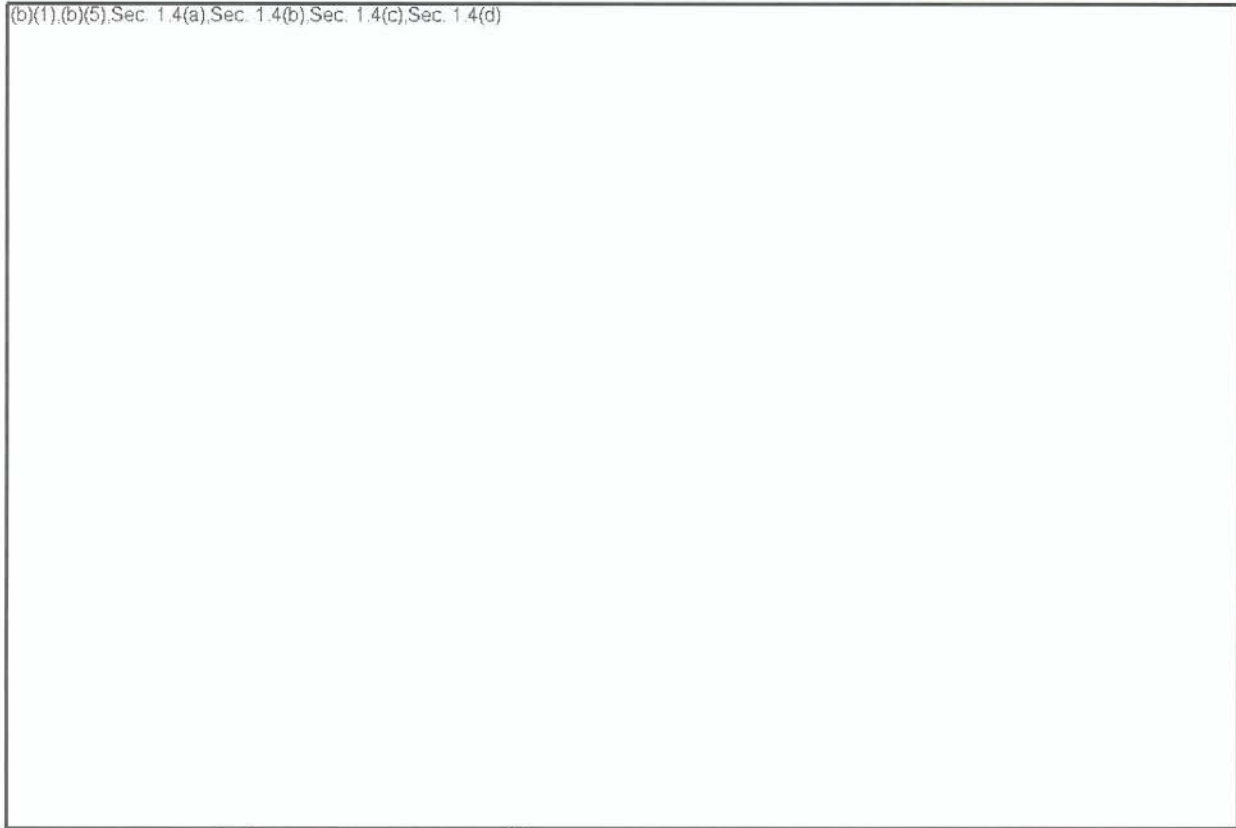
(b)(1),(b)(3);50 USC 3024(f),Sec. 1.4(b),Sec. 1.4(c),Sec. 1.4(d)

(U) Sensitive, candid commentary.

Derived from: ~~Multiple Sources~~

Declassify on: ~~FOUO~~

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



(U) Expected media treatment

(U) Australian media has thus far focused on Rudd's comments on China and Afghanistan, U.S. criticism of Rudd, and leadership views on North Korea and Iran. Foreign Minister Rudd publicly responded in December that he did not "give a damn" about criticism of him in the cables. A number of Australian news outlets have also used leaked cables for press reports related to Indonesia including troubled Papua province, the Indonesian Army Special Forces, and human rights abuses, as well as articles highlighting Singaporean criticism of regional neighbors.

(b)(1),(b)(5),Sec. 1.4(c),Sec. 1.4(d)



Drafted by:

Reviewed by:

(b)(3);10 USC 424,(b)(6)

INFO MEMO

~~S~~11-xxxx/IRTF

9 February 2011

TO: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1),(b)(3);10 USC 424,(b)(3);50 USC 3024(i),(b)(5);Sec. 1.4(b);Sec. 1.4(c);Sec. 1.4(d)

Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

The last page is withheld in full and not included.

~~SECRET//NOFORN~~

(b)(1),(b)(3):10 USC 424,(b)(3) 50 USC 3024(i),(b)(5),(b)(6),Sec. 1.4(b),Sec. 1.4(c),Sec. 1.4(d)

(U) Expected media treatment

(U) Thus far, Timorese media have not reported extensively on Wikileaks disclosures. We expect domestic and regional media would focus on negative commentary about Timorese leaders, shortfalls in the military and police, and the 2006 crisis.

Drafted by:

Reviewed by:

(b)(1),(b)(3):10 USC 424,(b)(3) 50 USC 3024(i),(b)(6),Sec. 1.4(c),Sec. 1.4(d)

~~SECRET//NOFORN~~

INFO MEMO

~~S~~XXXXXX-10

14 December 2010

SUBJECT:

(b)(1),(b)(5),Sec. 1.4(c),Sec. 1.4(d)

(U) Media treatment

(b)(1),(b)(5),Sec. 1.4(c),Sec. 1.4(d)

- (U) Leading centrist daily *Le Soir* noted 30 November the leaks mostly highlight the “solid and orthodox work of the [traditional] press,” which has already revealed most of the secrets in the cables.²
- (U) Popular daily *Le Derniere Heure* on 9 December said of the following topics concerning Belgium that were revealed in the leaked cables, all had been thoroughly covered by traditional media already:³

The last 3 pages are withheld in full and not included.

- (U) U.S. pressure on Belgian to accept Guantanamo detainees
- (U) The presence of nuclear weapons in Belgium
- (U) EU President (and former Belgian Prime Minister) Van Rompuy's pessimism on Afghanistan and climate change negotiations
- (U) Belgian internal political debates

(U) Official Reaction

(U) Belgian officials have downplayed the importance of the disclosures in public, condemning the act of leaking the cables while stressing that they contain few important disclosures.

- (U) Foreign Minister Vanackere, specifically referencing negotiations over Guantanamo detainees, said on 29 November "a great many things which are now being presented as leaks were actually already known."⁴
- (U) An advisor to Prime Minister Leterme wrote in a 30 November op-ed that the content of the leaked cables are not surprising and will not affect U.S. relations with other countries, while criticizing the Wikileaks organization for being motivated "more by the desire to do harm than to fight injustice."⁵
- (U) Vanackere on 12 December claimed another foreign minister had refused to answer a question "for fear of seeing a report of the conversation on the Internet."⁶

~~(C)~~ Potential loss of diplomatic contacts

(b)(1),(b)(5),Sec. 1.4(c),Sec. 1.4(d)

INFO MEMO

10-XXXX/IRTF

19 September 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1),(b)(3);50 USC 3024(i),Sec. 1.4(b),Sec. 1.4(c)

[Redacted content]

(U) Background

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

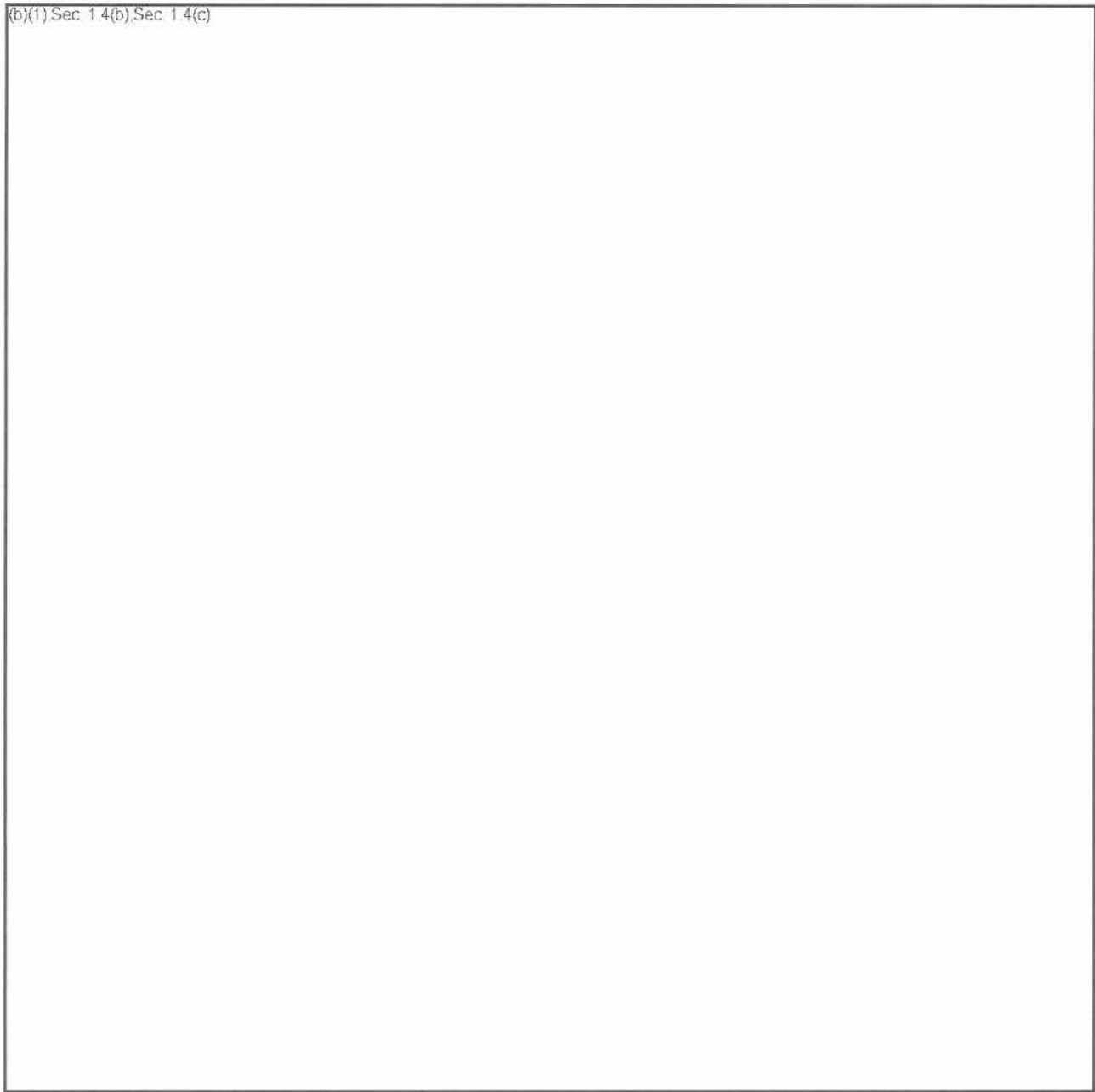
[Redacted content]

Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

The next page is withheld in full and is not included.

(U) Impact

(b)(1) Sec. 1.4(b), Sec. 1.4(c)



(U) Data Characterization

Derived from: ~~multiple sources~~
Declassify on: ~~2025~~

(b)(1),(b)(3):10 USC 424, Sec. 1 4(b), Sec. 1 4(c)

Prepared by: (b)(3):10 USC 2305 (g),(b)(6)
Reviewed by:

Derived from: ~~SECRET//NOFORN~~
Declassify on: ~~SECRET//NOFORN~~

~~SECRET~~

INFO MEMO

10-000X/IRTF

22 August 2010

FOR: DIRECTOR, DEFENSE INTELLIGENCE AGENCY

THROUGH: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1)Sec. 1.4(b)Sec. 1.4(c)

~~SECRET~~

~~SECRET~~

Reviewed by:

(b)(3);10 USC 424,(b)(6)

~~SECRET~~

INFO MEMO

~~S~~ 10-00XX/IRTF

24 September 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT

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

(b)(1), Sec. 1.4(b), Sec. 1.4(c)

[Redacted content]

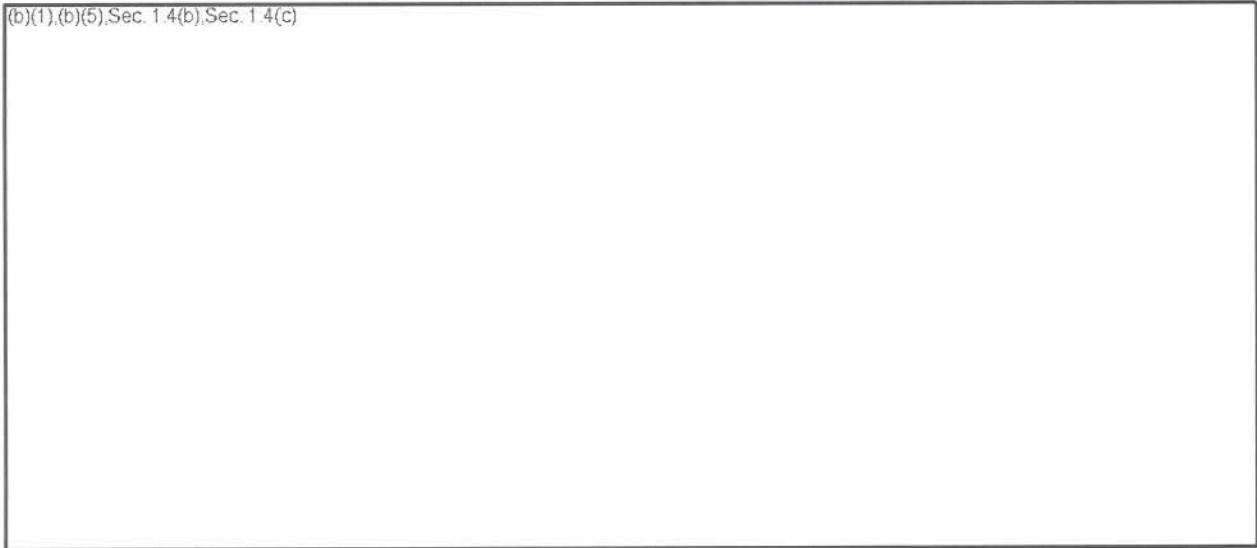
Smuggling and Illegal Crossings

(b)(1), Sec. 1.4(b), Sec. 1.4(c)

[Redacted content]

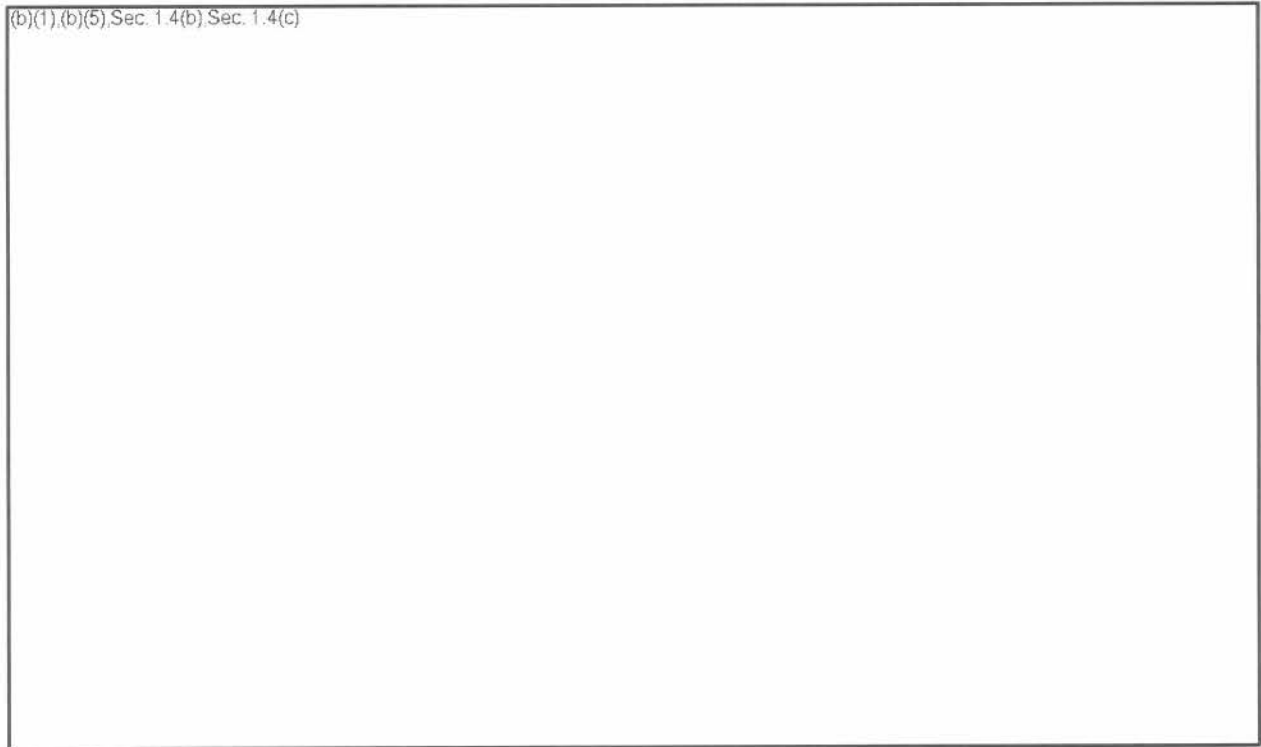
Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)



Harassment of Border Forces

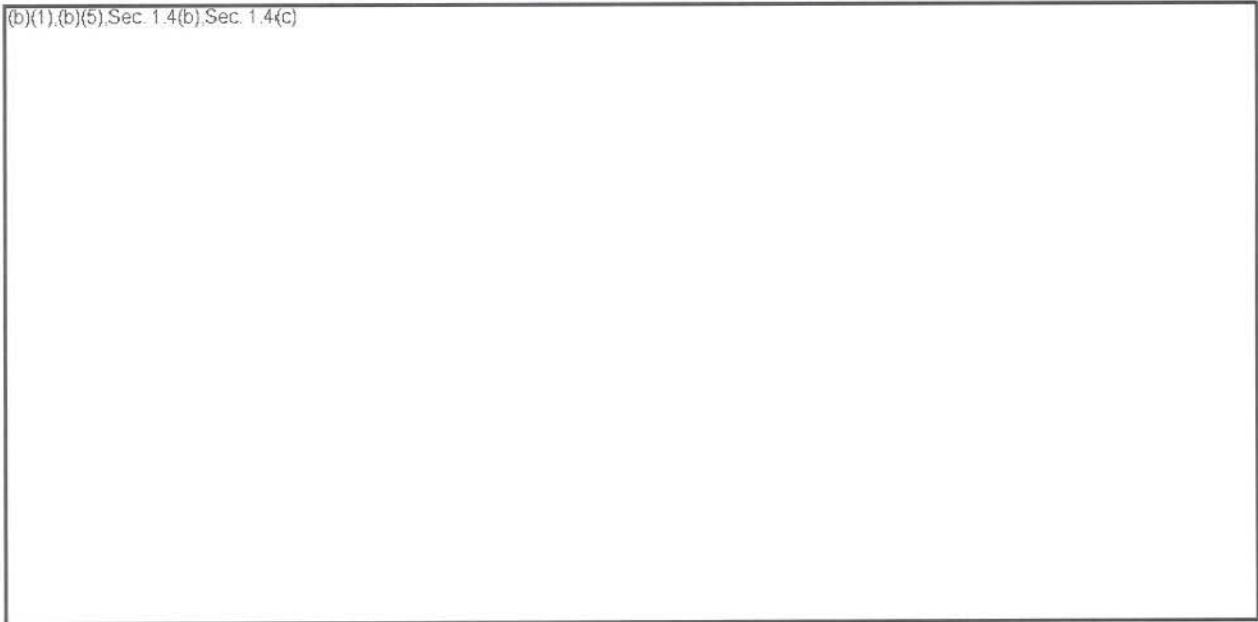
(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)



Iraqi Border Forces Response to Harassment

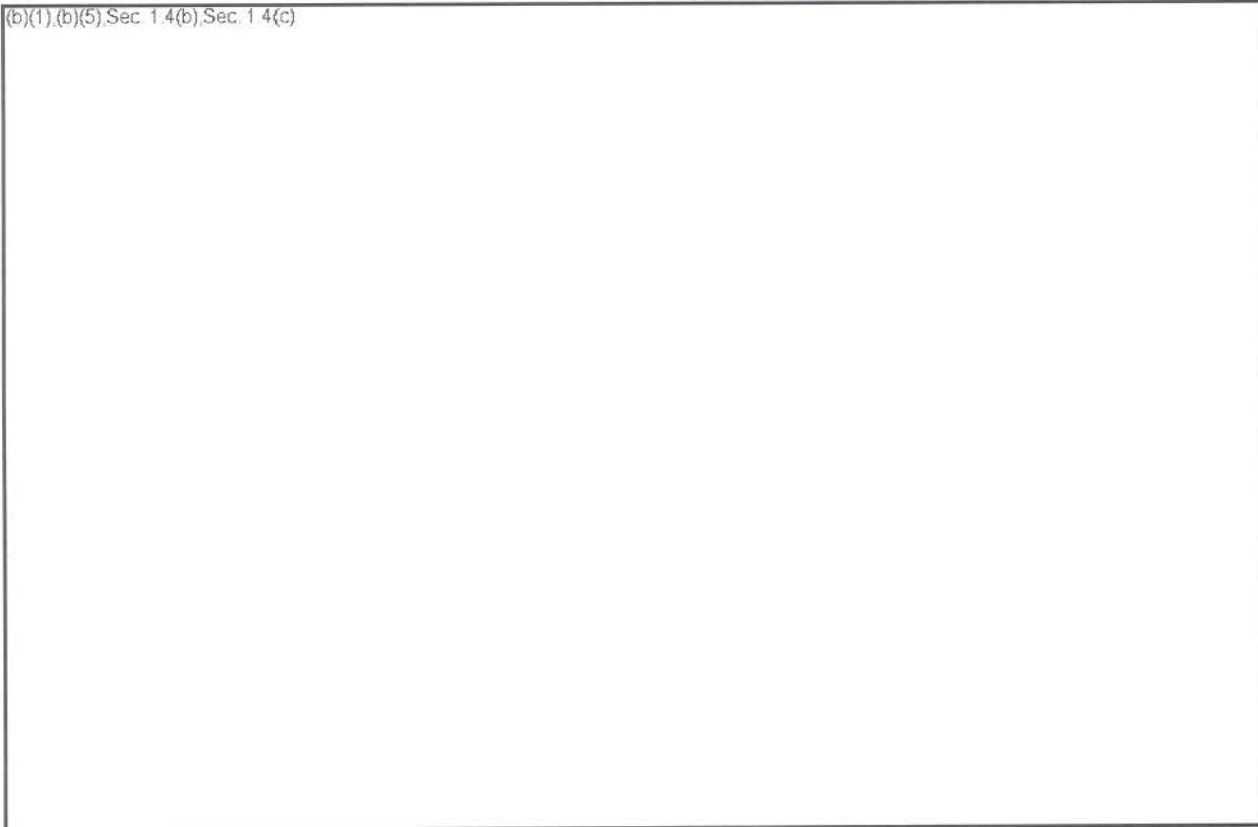
Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)



Cross-Border Operations

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)



Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

Politically-Sensitive Incidents

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

Prepared by: (b)(3);10 USC 424,(b)(6)
Reviewed by:

Derived from: ~~Multiple Sources~~
Declassify on: ~~25X1~~

~~SECRET//NOFORN~~

INFO MEMO

10-00XX/IRTF

27 September 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT (b)(3):50 USC 3024(f)

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

(U) Background

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

(U) Summary

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

Derived from: [redacted]
Declassify on: [redacted]

~~SECRET//NOFORN~~

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

(U) Impact

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

Prepared by: (b)(3);10 USC 424,(b)(6)
Reviewed by:

INFO MEMO

10-XXXX/IRTF Draft

29 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1),(b)(3):10 USC 424,(b)(3) 50 USC 3024(i),Sec. 1.4(c),Sec. 1.4(d)

(U) Characterization of the CIDNE-A Data

(b)(1),(b)(3):50 USC 3024(i),Sec. 1.4(b),Sec. 1.4(c)

Derived From: ~~Multiple Sources~~
Declassify On: ~~20350816~~

~~SECRET~~

(b)(3):10 USC 424

- (U//~~FOUO~~) Threat reports are immediate, uncorroborated reporting on enemy activities. As time is of the essence when potential threats are identified, speed is more important than fact checking. This reporting is information in its rawest form and not “statements of fact” as the media is likely to report it.

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

~~SECRET~~

(b)(3):10 USC 424

~~SECRET~~

(b)(3):10 USC 424

(b)(1),(b)(3):10 USC 424, Sec. 1.4(b), Sec. 1.4(c)

(U) Prepared by:

(b)(3):10 USC 424

~~SECRET~~

(b)(3):10 USC 424

INFO MEMO

~~S~~ 10-0XXX/IRTF

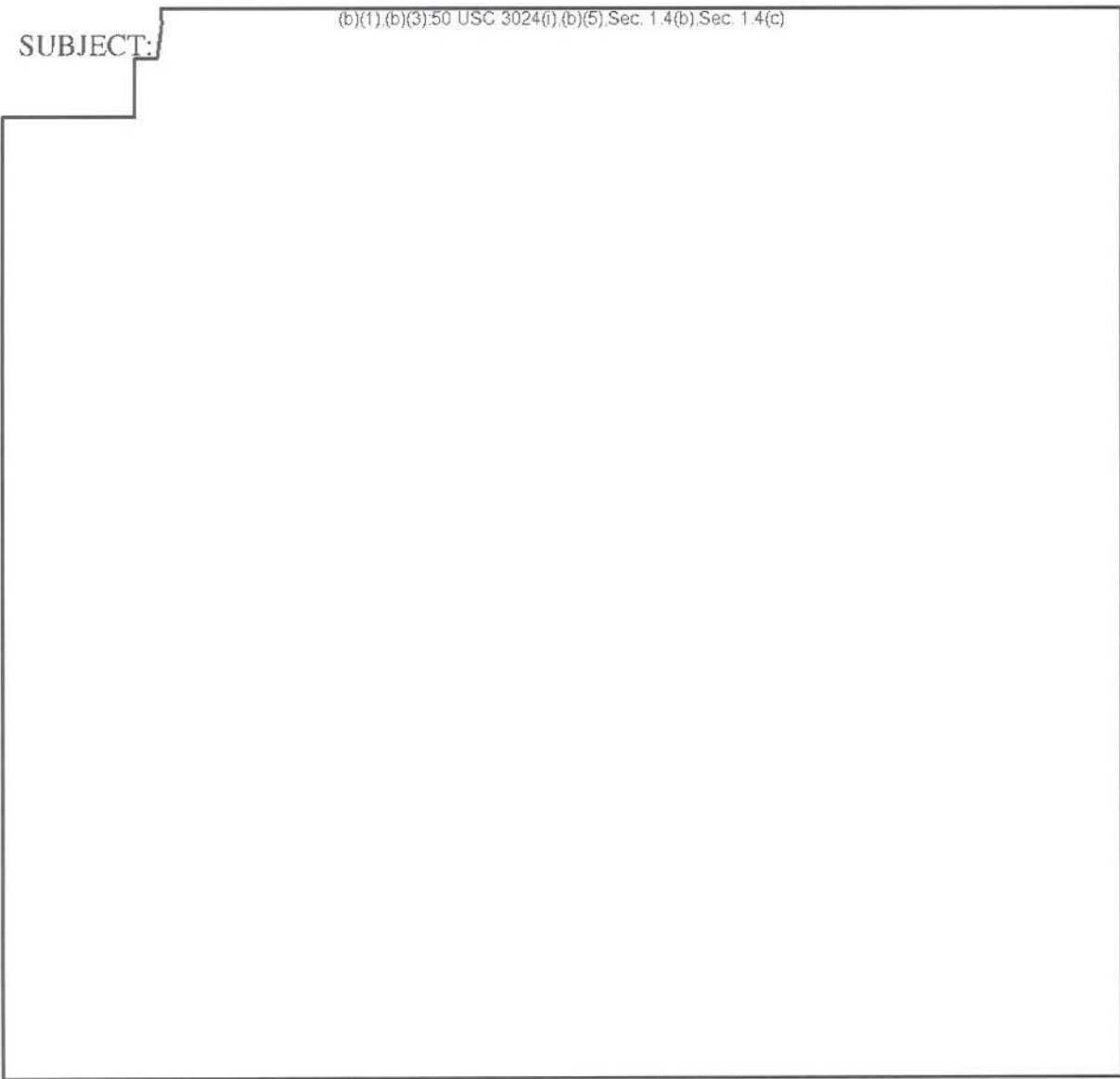
29 September 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1),(b)(3) 50 USC 3024(i),(b)(5) Sec. 1.4(b), Sec. 1.4(c)



Derived from: ~~multiple sources~~
Declassify on: ~~OSMA~~

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

(U) Data Characterization

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

(U) Vehicle Accidents

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

(U) Escalation of Force Resulting in Civilian Deaths

(b)(1),Sec. 1.4(b),Sec. 1.4(c)

Derived from: ~~██████████~~
Declassify on: ~~██████████~~

(b)(1), Sec. 1.4(b), Sec. 1.4(c)

(U) Iraqi PSC Incidents

(b)(1), (b)(3), 10 USC 424, (b)(6), Sec. 1.4(b), Sec. 1.4(c)

Derived from: ~~██████████~~
Declassify on: ~~██████████~~

INFO MEMO

10-00XX/IRTF

29 September 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT

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

(b)(1), Sec. 1.4(c), Sec. 1.4(d)

(U) Background

(b)(1), Sec. 1.4(b), Sec. 1.4(c)

¹ The Fourth Geneva Convention for the protection of civilian persons in time of war; Article 4 defines who is a Protected person: Persons protected by the Convention are those who, at a given moment and in any manner whatsoever, find themselves, in case of a conflict or occupation, in the hands of a Party to the conflict or Occupying Power of which they are not nationals.

Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

(b)(1), Sec. 1.4(b), Sec. 1.4(c)



(U) Summary

(b)(1), Sec. 1.4(b), Sec. 1.4(c)



(U) Impact

(b)(1), (b)(5), Sec. 1.4(b), Sec. 1.4(c)



Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)



Prepared by:
Reviewed by:

(b)(3);10 USC 424,(b)(6)

² On 16 July 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.

Derived from: ~~Source~~
Declassify on: ~~Source~~

The last 2 pages are withheld in full and not included.

INFO MEMO

XXXXXX-10

30 December 2010

SUBJECT:

(b)(1),Sec. 1.4(c),Sec. 1.4(d)

(U) Media treatment

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

(U) Official Reaction

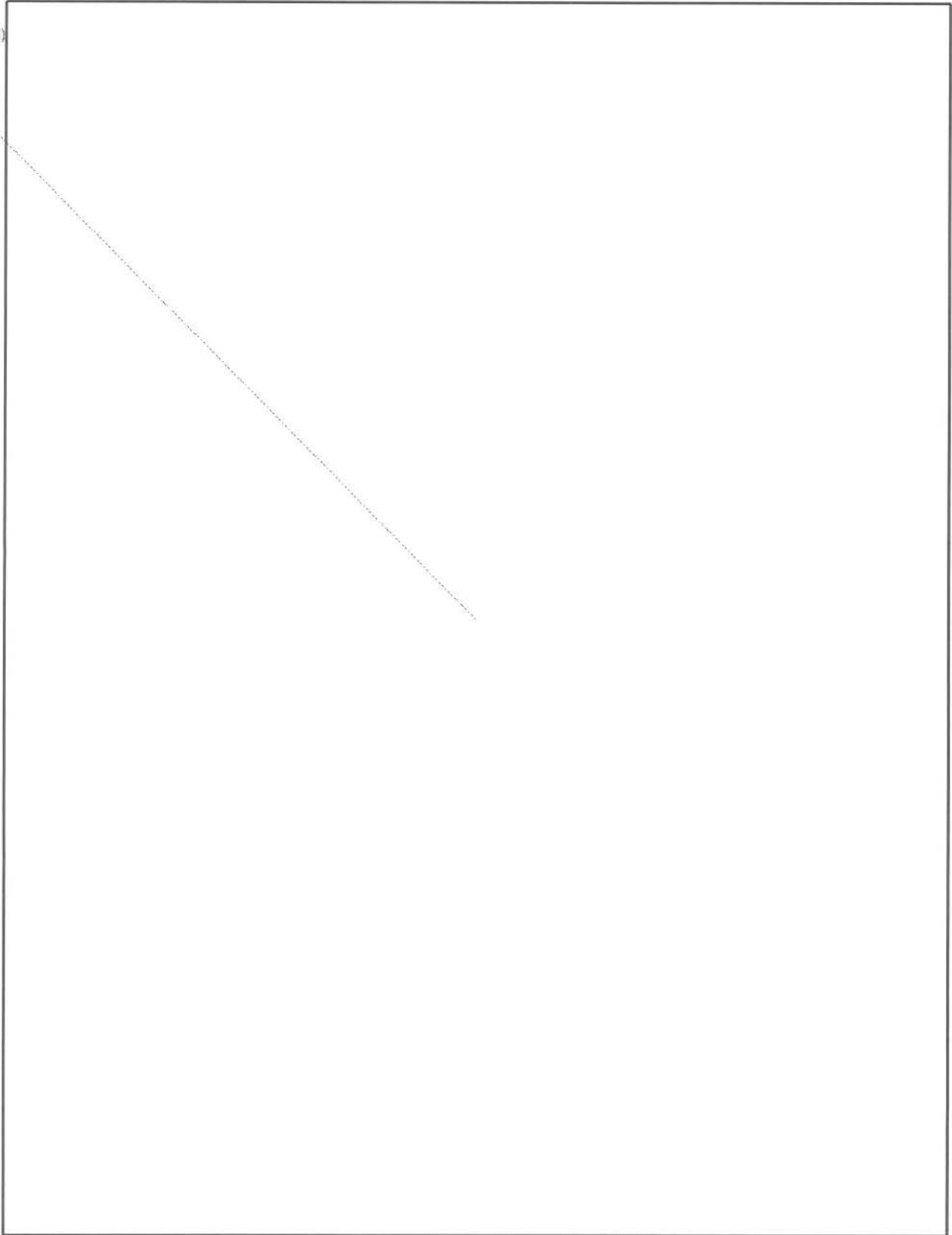
(U) A foreign ministry spokesman said the leaks would not harm Bulgaria's relations with the U.S. and served only the interest of those looking to weaken transatlantic ties. ² However, former Foreign Minister Ivo Kalfin decried the collection of personal information, including credit card numbers, of Bulgarian politicians as inappropriate, but observed the United States would only collect such information if it felt Bulgaria was important. ³

(b)(1),(b)(3);10 USC 424 (b)(6) Sec. 1.4(c),Sec. 1.4(d)

From:
To:
Subject:
Date:

Thursday, December 02, 2010 1:26:00 PM

(b)(1),(b)(3);10
USC 424 (b)
(3); 50 USC
3024(i),(b)
(6),Sec. 1.4
(c),Sec. 1.4(d)



(b)(1),(b)(3):10 USC 424,(b)(3):50 USC 3024(f),(b)(6),Sec. 1.4(c),Sec. 1.4(d)

CLASSIFICATION: ~~SECRET//NOFORN~~

Alcon,

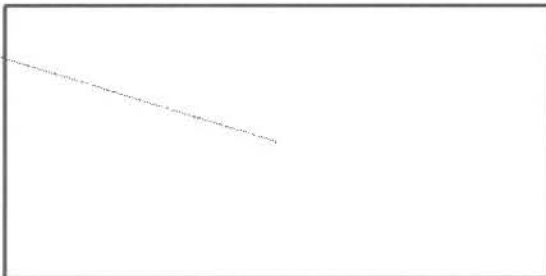
Please provide line in/line out comments on the attached word doc containing the portions of the latest CJCS Wikileaks slide, by **NLT 1400 TODAY**.

(b)(1),Sec. 1.4(c),Sec. 1.4(d)

Please send all comments to the Cc line.

Thanks,

(b)(3):10 USC 424,(b)(6)



(b)(3):10 USC
424,(b)(6)



DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~25X1~~
DATE OF SOURCE: ~~20101202~~

CLASSIFICATION: ~~SECRET//NOFORN~~

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~25X1~~
DATE OF SOURCE: ~~20101202~~

CLASSIFICATION: ~~SECRET//NOFORN~~

#849

U.S. DEPARTMENT OF DEFENSE
OFFICE OF LEGISLATIVE AFFAIRS

December 23, 2010

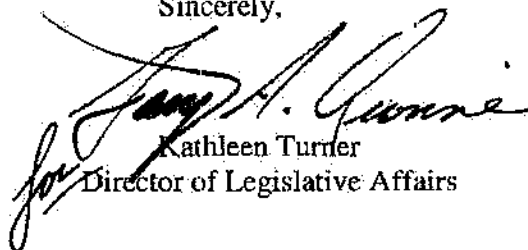
The Honorable John Ensign
United States Senate
Washington, D.C. 20510

Dear Senator Ensign:

Thank you for your 10 December 2010 letter on the SHIELD Act, S. 4004, and the impacts of WikiLeaks' unauthorized disclosures of classified information. The Office of the Director of National Intelligence has referred your letter to the Department of Defense as they are the most appropriate agency to answer your questions. The Defense Intelligence Agency is leading the WikiLeaks Information Review Task Force (IRTF) under the direction of Brigadier General Robert Carr. The Congressional Activities Office of the Under Secretary of Defense for Intelligence will ensure you receive a timely response, and they can be contacted at (703) 697-6644.

We appreciate your continued support on issues concerning national security and the Intelligence Community. If you have any questions, please contact me on (703) 275-2473.

Sincerely,



Kathleen Turner
Director of Legislative Affairs

869

UNCLASSIFIED//~~FOUO~~

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL COUNTERINTELLIGENCE EXECUTIVE
WASHINGTON, DC 20505

NCIX-017-11

MEMORANDUM FOR: LTG Ronald L. Burgess, Jr.
Director, Defense Intelligence Agency

SUBJECT: (U) [REDACTED] (b)(3)
[REDACTED] (b)(3)

(U//~~FOUO~~) [REDACTED] (b)(3)
[REDACTED] (b)(3)

(b)(3):10 USC
424;(b)(6)

(U//~~FOUO~~) [REDACTED] (b)(3)
(DIA) [REDACTED] (b)(3)

[REDACTED] (b)(3)

(U//~~FOUO~~) [REDACTED] (b)(3)
[REDACTED] (b)(3)

(U) STATUTORY AUTHORITY:

In accordance with its statutory responsibility, as provided for at 50 USC 402c(e)(4), the National Counterintelligence Executive (NCIX) leads and coordinates comprehensive government-wide assessments of the damage resulting from unauthorized disclosures.

(b)(3):10
USC 424

(DIA) [REDACTED]

[REDACTED] (b)(3)

(b)(3):10
USC 424

DIA [REDACTED]

UNCLASSIFIED//~~FOUO~~

SUBJECT: (U) [REDACTED] (b)(3)

There are noted Base Realignment and Closure (BRAC) issues related to this request and my staff will work closely with your facilities and IT infrastructure points of contact to address them.

(U) FUNDING:

This request may entail associated funding which will be fully addressed when necessary.

I look forward to our continued joint efforts. Please let me know who your lead is for this action. My primary points of contact are [REDACTED] (b)(3) Assistant Director, Analysis, Collection, and Coordination Directorate, [REDACTED] (b)(3) and [REDACTED] (b)(3) Chief of Staff, [REDACTED] (b)(3)

[REDACTED] (b)(3) _____ Date _____

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL COUNTERINTELLIGENCE EXECUTIVE
WASHINGTON, DC 20505

NCIX-039-11

MEMORANDUM FOR: LTG Ronald L. Burgess, Jr.
Director, Defense Intelligence Agency

SUBJECT: (U) (b)(3)
(b)(3)

(U//FOUO) (b)(3)
(b)(3)

(b)(3); 10 USC 424; (b)(6) (U//FOUO) (b)(3)
and DIA (b)(3)
(b)(3)

(U//FOUO) (b)(3)
(b)(3)

(U) STATUTORY AUTHORITY:

In accordance with its statutory responsibility, as stated in 50 USC 402c(e)(4), the National Counterintelligence Executive (NCIX) leads and coordinates comprehensive government-wide assessments of the damage resulting from unauthorized disclosures.

(b)(3); 10 USC 424; (b)(5) DIA

(b)(3)

SUBJECT: (U)

(b)(3)

(b)(3);10
USC 424

DIA

There are noted Base Realignment and Closure (BRAC) issues related to this request and my staff will work closely with your facilities and IT infrastructure points of contact to address them.

(U) FUNDING:

This request may entail associated funding which will be fully addressed when necessary.

I look forward to our continued joint efforts. Please let me know who your lead is for this action. My primary points of contact are (b)(3) Assistant Director, Analysis, Collection, and Coordination Directorate, (b)(3) and (b)(3) Chief of Staff, (b)(3)

(b)(3)

Date

2/17/11

#402

~~TOP SECRET//SI//NOFORN~~



Office of the Director of National Intelligence



WikiLeaks Situation Update

(b)(3)

Assistant Director

Office of the National Counterintelligence Executive

April 7, 2011

This briefing is classified

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~



TOP SECRET//SI//NOFORN

Office of the Director of National Intelligence



AGENDA

- ★ Analysis and Production Update
- ★ WikiLeaks Situation Update
- ★ NCIX Outreach Update
- ★ SVTC Participants
- ★ Questions / Guidance

Information Review Task Force Intelligence Update

The next page is
withheld in full.



DIA [Redacted]

(b)(3):10 USC 424;(b)
(6)

IRTF Chief
7 April 2011 - 1600

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

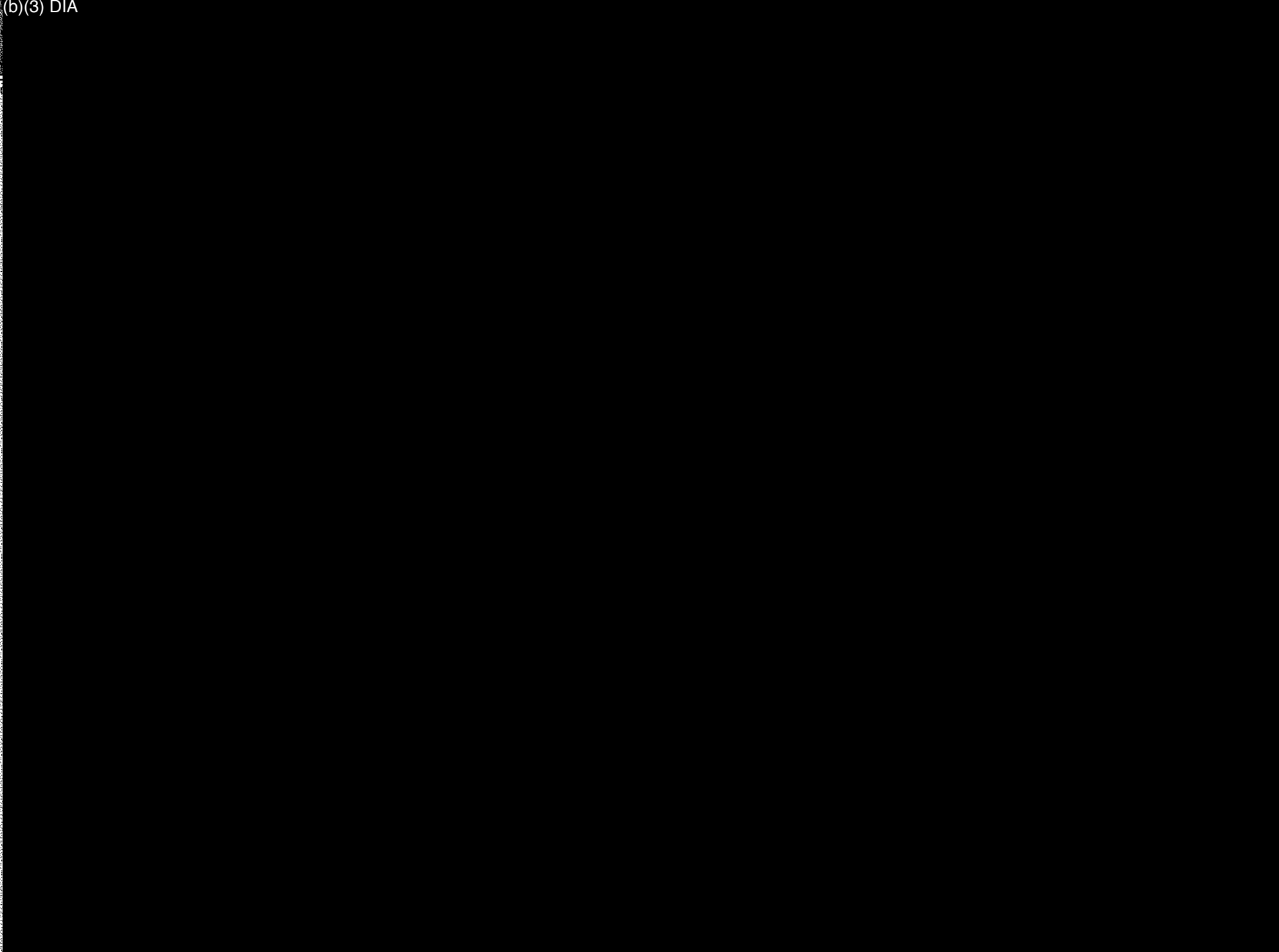
Derived from: ~~Multiple Sources~~
Declassify on: ~~2000-105~~

This briefing is classified

~~TOP SECRET~~ DIA ~~NOFORN~~

UNCLASSIFIED

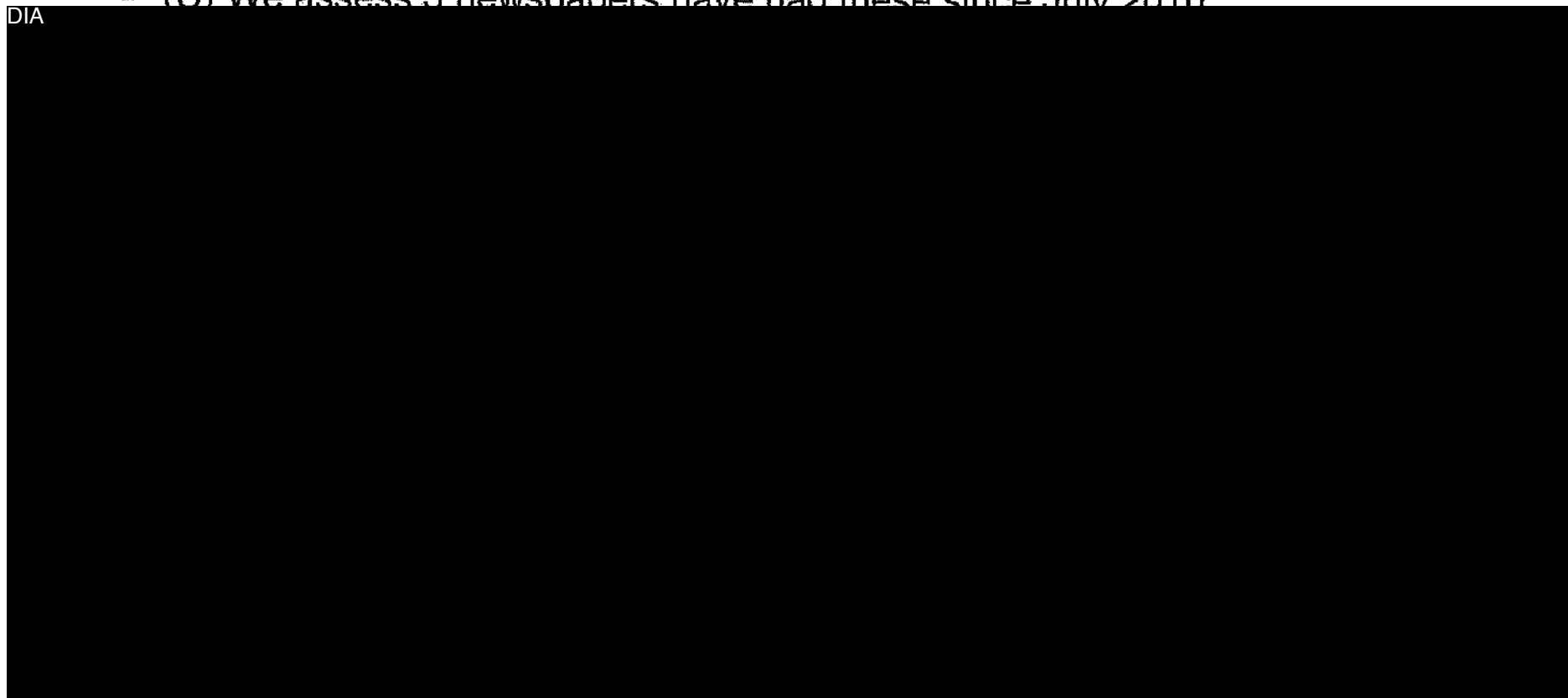






15k Data Set

- (U) WikiLeaks withheld 15k records pending “harm minimization”
 - (U) We assess 3 newspapers have had these since July 2010

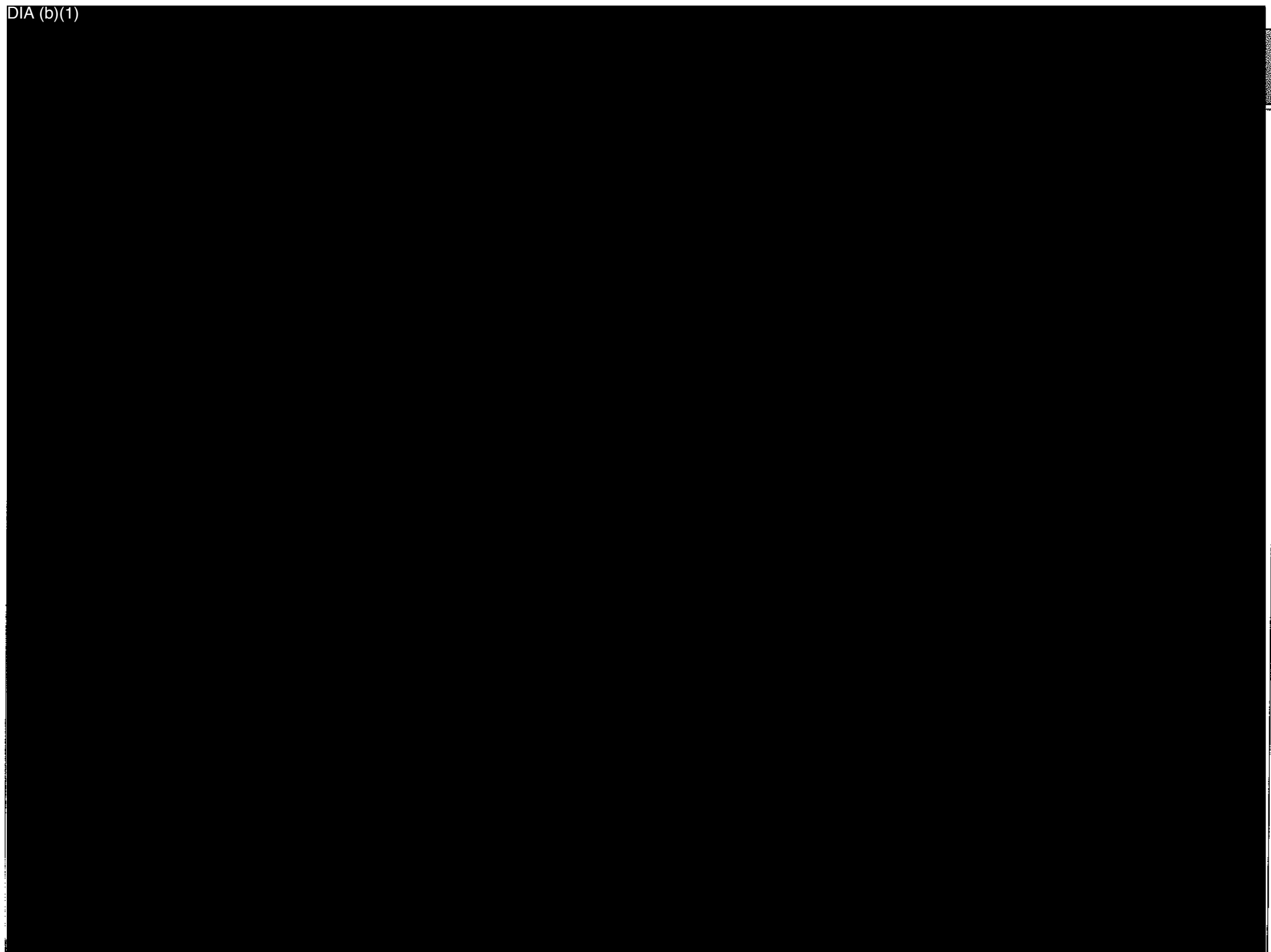


DIA

(b)(1);(b)(3):10 USC 424;(b)(3):50 USC 3024(i);(b)(5);Sec. 1.4(c);Sec. 1.4(d)









WikiLeaks Sparks Conscientious Objector Claim

- (U) UK Royal Navy medic filed for conscientious objector status after reading WikiLeaks Afghanistan data
 - (U) First person to meet Advisory Committee on Conscientious Objectors in 14 years
 - (U) Faces up to 10 years in prison for willful misconduct

- (U) *"If more people in my position stood up, there would be less innocent lives lost"*

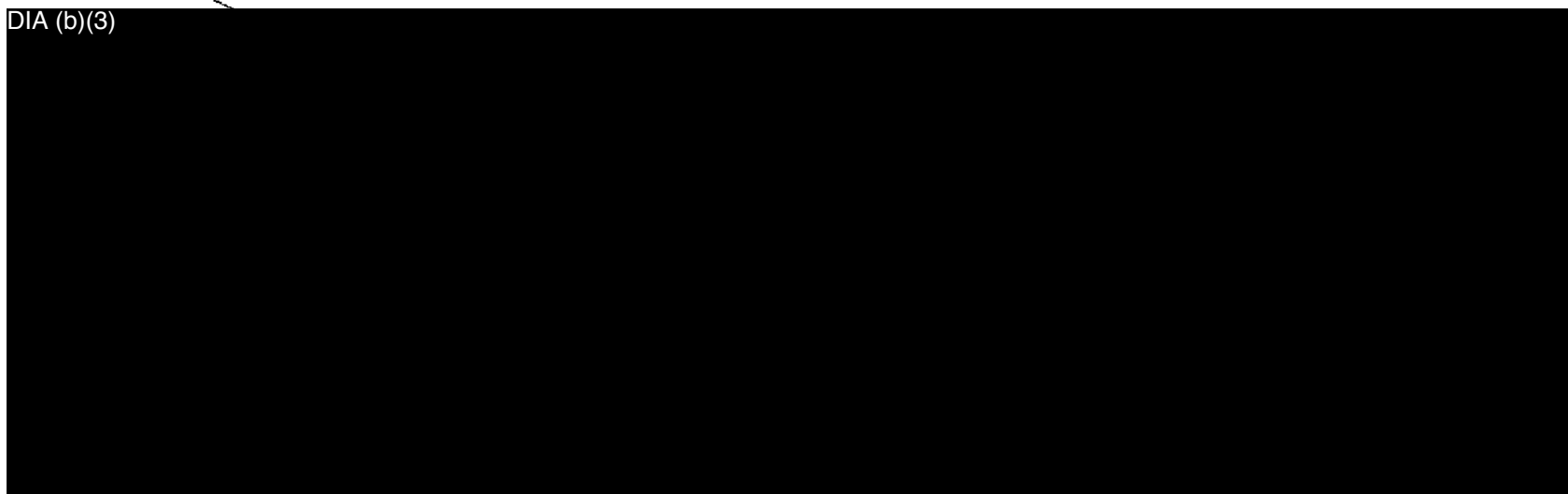
- (U) Press coverage could inspire additional conscientious objector claims



(b)(3):10 USC 424;(b)(3):50 USC 3024(f)

Laying the Groundwork for GTMO?

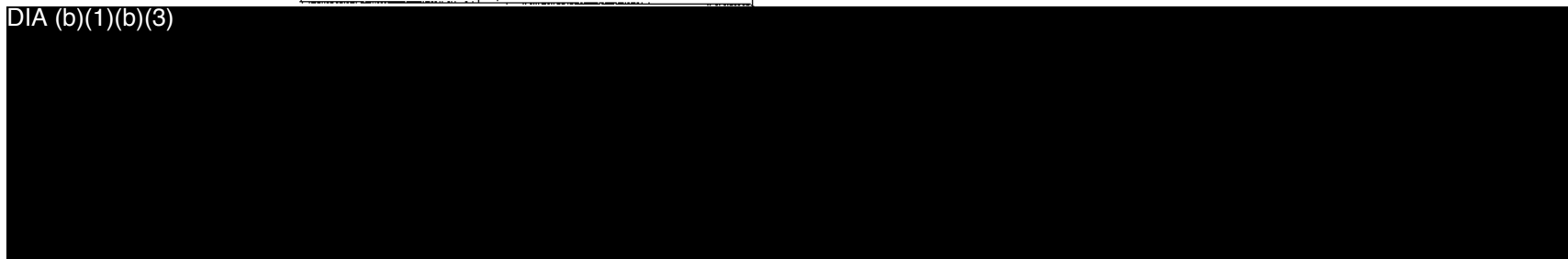
DIA (b)(3)



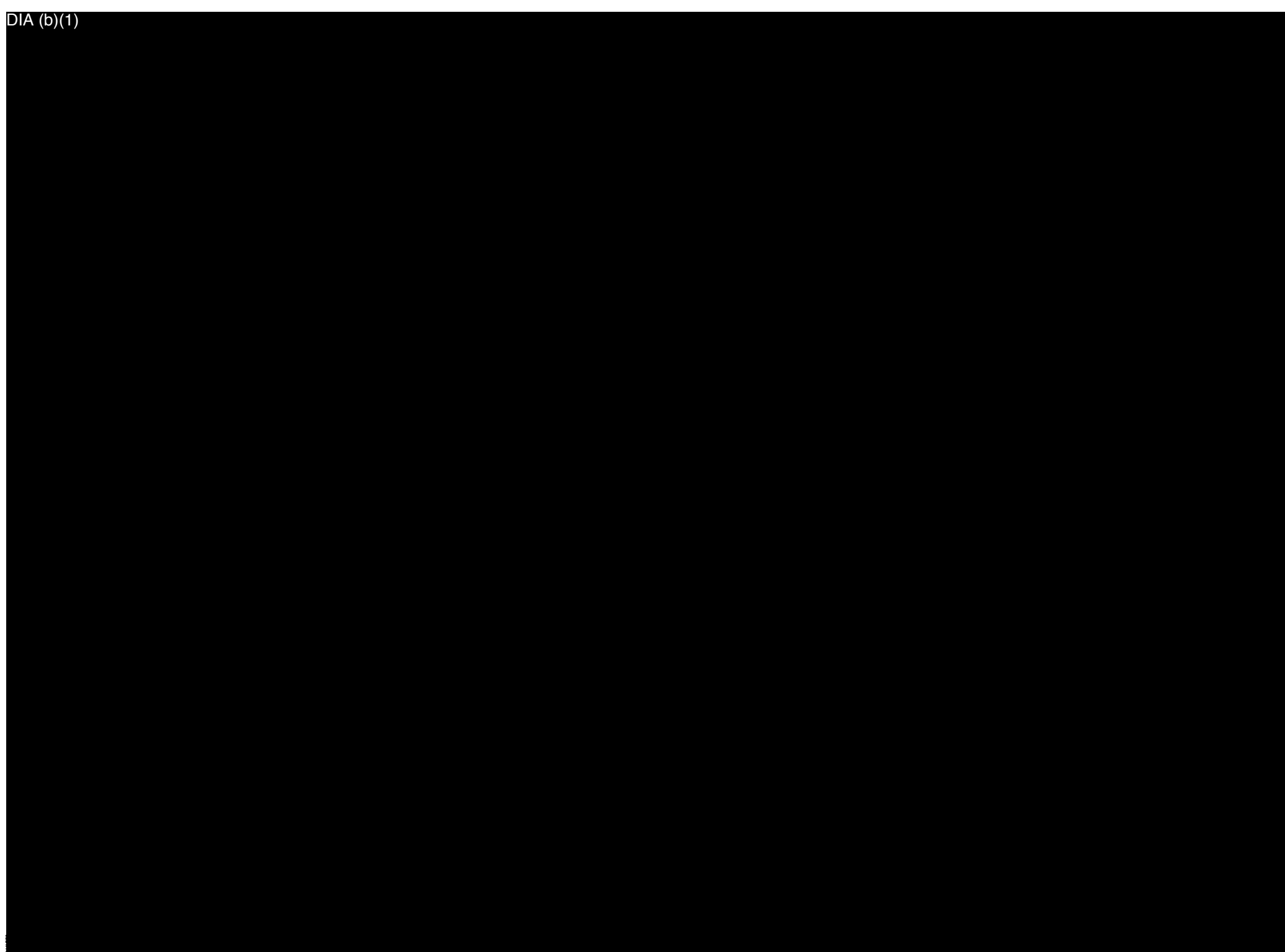
- (U) 9-11 May: Assange scheduled to speak on GTMO, among other topics, at Oslo Freedom Foundation event
- (U) Apparent discussions with journalists in U.S. and London

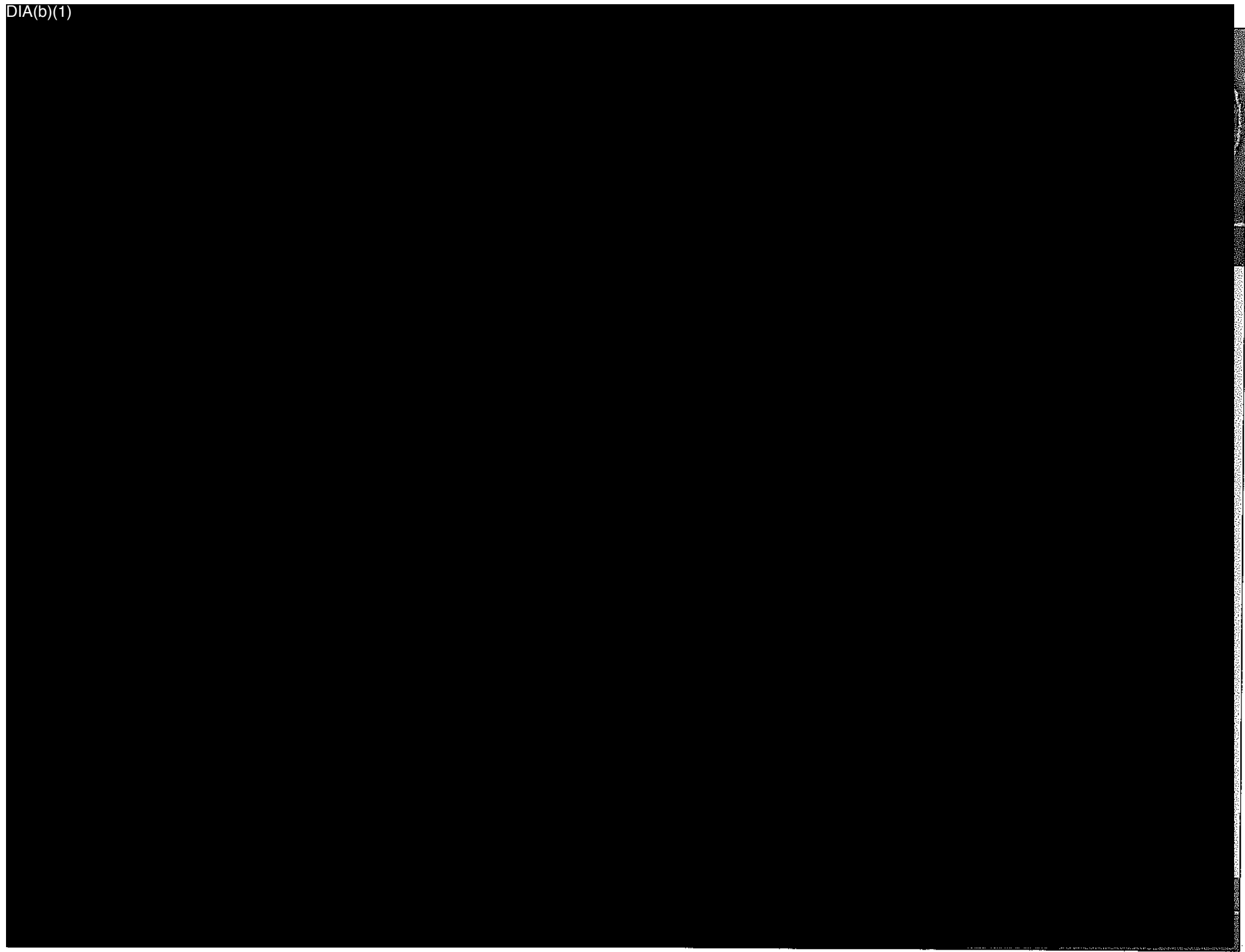
(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

DIA (b)(1)(b)(3)



1961-2011
CELEBRATING OUR LEGACY
FORGING OUR FUTURE





TOP SECRET//SI//NOFORN

Office of the Director of National Intelligence

QUESTIONS / GUIDANCE

TOP SECRET//SI//NOFORN

844

~~SECRET//NOFORN~~

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL COUNTERINTELLIGENCE EXECUTIVE
WASHINGTON, DC 20505

NCIX-192-10

MEMORANDUM FOR: Distribution

SUBJECT: ~~(U//FOUO)~~ (b)(3)
(b)(3)

~~(U//FOUO)~~ The Counterintelligence Enhancement Act of 2002 provides that, as directed by the Director of National Intelligence (DNI) and in consultation with appropriate elements of the departments and agencies of the United States Government (USG), the Office of the National Counterintelligence Executive (ONCIX) is responsible for the oversight and coordination of the production of strategic analyses of counterintelligence matters, including counterintelligence damage assessments.

~~(S//NF)~~ (b)(1)
(b)(1)

~~(C//NF)~~ (b)(1)
(b)(1)

~~(U//FOUO)~~ My point of contact is (b)(3) who can be reached at (b)(3)
(b)(3) ONCIX appreciates your full support in this important endeavor.

(b)(3)

Date 8/17/10

Attachments:
1. ~~(C//NF)~~ (b)(1)

Declassify On: 20350224
Derived From: ODNI ANA S-08

~~SECRET//NOFORN~~

SUBJECT: (U//FOUO) [REDACTED] (b)(3)
 [REDACTED] (b)(3)

Distribution:

Assistant Director, Counterintelligence Division, Federal Bureau of Investigation
 Deputy Assistant Director for Cyber, Federal Bureau of Investigation
 Deputy Director, Threat Operations Center, National Security Agency/Central Security Service
 Director, Central Intelligence Agency, Chief, Counterintelligence Center
 Deputy Under Secretary of Defense (HUMINT, CI & Security)

CC:

Director of National Intelligence
 Principal Deputy Director of National Intelligence
 Director of the Intelligence Staff
 Director, Intelligence, Joint Staff
 Acting Under Secretary for Intelligence & Analysis, Department of Homeland Security
 Deputy Attorney General, Department of Justice
 Director, Office of Intelligence and CI, Department of Energy
 Director, Diplomatic Security Service, Department of State
 Director, Counterintelligence, Department of State - INR
 Senior Director for Intelligence Programs, National Security
 Director, Defense CI and HUMINT Center, Defense Intelligence Agency
 Deputy Assistant Secretary, Department of Treasury
 Associate Director for Security and CI, National Security Agency
 Director, National Geospatial-Intelligence Agency
 Acting Under Secretary for Industry and Security, Department of Commerce
 Director, Counterintelligence, National Reconnaissance Office
 Director, Defense Security Service
 Commander, Air Force Office of Special Investigations
 Director, CI, HUMINT, Disclosure and Security, United States Army
 Director, Naval Criminal Investigative Service

Pages 1 and 3-4 are withheld in full and are not included.

~~SECRET//NOFORN~~

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

Executive Summary (U)

(U) WikiLeaks claims to have a compendium of over 91,000 reports covering the war in Afghanistan from 2004 to 2010, which they refer to as the Afghan War Diary. On 25 July 2010, WikiLeaks posted over 76,000 Afghan war reports to their website (www.wikileaks.org) and threatens to release another 15,000 reports in the near future.

(b)(1);(b)(5);(b)(3):10 USC 424;Sec. 1.4(c);Sec. 1.4(d);(b)(3):50 USC 3024(i)

~~SECRET//NOFORN~~

(b)(5);(b)(3):10 USC 424;(b)(3):50 USC 3024(i)

(U) Due to the sheer volume of information that 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.

(b)(3):10 USC 424

(U) Interagency Collaboration

(b)(5);(b)(3):10 USC 424;(b)(3):50 USC 3024(i)

Background (U)

(U) On 25 July 2010 at 1700 hours Eastern Daylight Time the WikiLeaks organization released approximately 76,000 government reports to the general public through its website; WikiLeaks.org (dedicated webpage at <http://wardiary.wikileaks.org>).

(b)(1);(b)(5);(b)(3):10 USC 424;Sec. 1.4(c);Sec. 1.4(d);(b)(3):50 USC 3024(i)

(U) The WikiLeaks website provided access to the Afghan data in a variety of formats, to include 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 25 July 2010 public posting of reports from CIDNE-A, 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 the 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 to date.

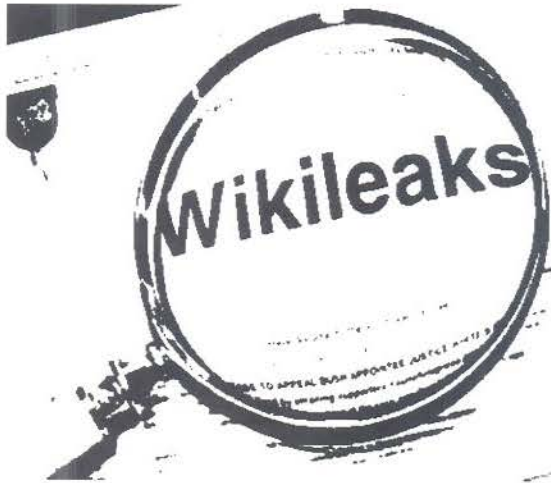
(U) WikiLeaks also posted a 1.4 gigabyte (GB) encrypted file to the "*Afghan War Diary, 2004-2010*" webpage, which is labeled "*Insurance file*." Minimal information about this file is disclosed on the website, other than "*name: insurance.aes256*" and "*type: unknown file type, 1.38GB*." It appears to be encrypted with AES-256, a publicly available symmetric-key encryption standard.⁵ This file is publicly available for download in its encrypted form but without 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.

(U) IRTF Assessment:

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

⁵ (U) AES-256: Advanced Encryption System (AES) that uses a 256-bit encryption key (password).

APPENDIX A – GENERAL BACKGROUND INFORMATION ON WIKILEAKS (U)



(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 way for people with damning, potentially helpful, or just plain embarrassing information to make it public without providing any linkage back to the source who leaked or disclosed the information.

"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.

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

¹² (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.

From: [Redacted]
To: [Redacted]
Subject: (S) IANSA PREPARING FOR EARLY ELECTIONS, HESITANT ON BORDER AGREEMENT
Date: Monday, July 25, 2011 10:50:03 AM

B3
B6

CLASSIFICATION: SECRET//NOFORN

[Redacted]

B1
1.4(B)
1.4(C)
1.4(D)

RELEASE IN PART
1.4(B),B1,1.4(D),B3,B6,1.4(C)

O R 201220Z JUL 11

FM AMEMBASSY LJUBLJANA
TO RUEHC/SECSTATE WASHDC
INFO EUROPEAN POLITICAL COLLECTIVE

BT
S E C R E T LJUBLJANA 000135
SENSITIVE
NOFORN

***** THIS IS A COMBINED MESSAGE *****
E.O. 13526: DECL: 2021/07/20
TAGS: PREL, PGOV, PBYS, ZL, IIR, SI
SUBJECT: (S) [Redacted]

REF: A) 11 LJUBLJANA 127;
CLASSIFIED BY: H. MARTIN MCDOWELL, POL-ECON SECTION CHIEF, DEPT. OF
STATE, EMBASSY LJUBLJANA; REASON: 1.4(B), (D)
1. (S/NF) SUMMARY: [Redacted]

1.4(B)
1.4(D)
B1

[Redacted]

END SUMMARY.

WIKILEAKS AND EARLY ELECTIONS: AN UNSPOKEN NEXUS

2. (S) [Redacted]

[Redacted]

1.4(B)
1.4(D)
B1

3. (S)

[Redacted]

4. (S)

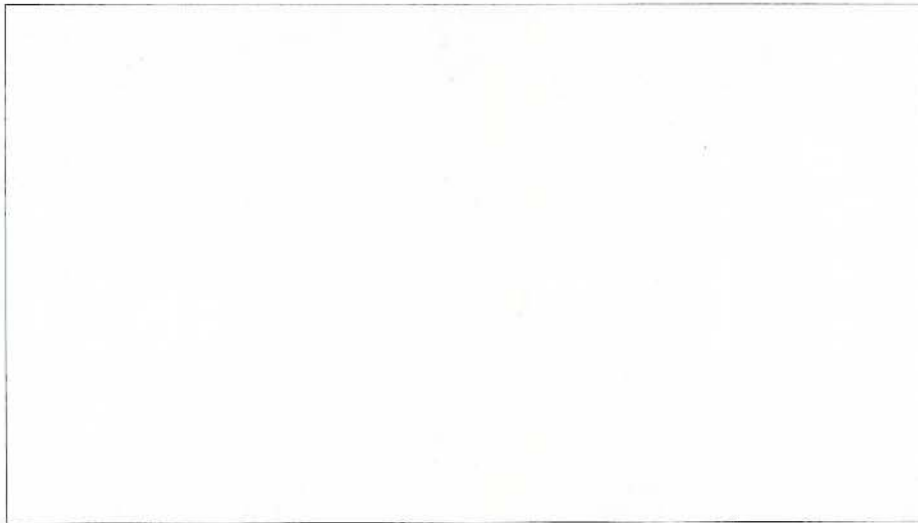
[Redacted]

5. (S)

[Redacted]

6. (S)

[Redacted]

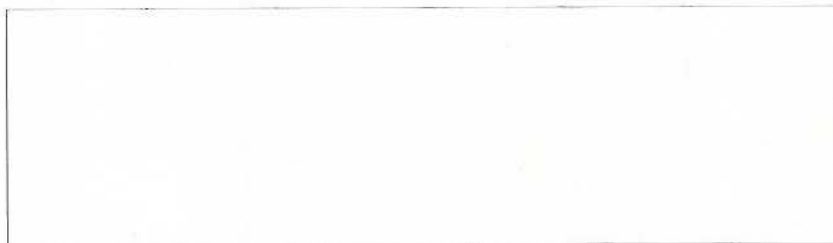


1.4(B)
1.4(D)
B1



MUSSOMELI

BT
#0135



B3
B6

DERIVED FROM: ms
DECLASSIFY ON: 20360723
DATE OF SOURCE: 20110725

CLASSIFICATION: SECRET//NOFORN

38

From: [Redacted]
To: [Redacted]
Subject: Emailing: Message Text.htm
Date: Tuesday, February 22, 2011 8:31:52 AM

RELEASE IN PART B1,B3
INA,1.4(D),B6,B3

B3
B6

CLASSIFICATION: SECRET//NOFORN

SECRET
NOFORN;

ENVELOPE

OAASZYUW RUEHDBU0045 0491224-SSSS--RUZDTPW.
ZNY SSSSS ZOC STATE ZZH
TOQ4428
OO RUEHC

HEADER

O 181224Z FEB 11
FM AMEMBASSY DUSHANBE
TO RUEHC/SECSTATE WASHDC
BT

CONTROLS

S E C R E T DUSHANBE 000045
NOFORN
NOFORN
E.O. 13526: DECL: 2021/02/18

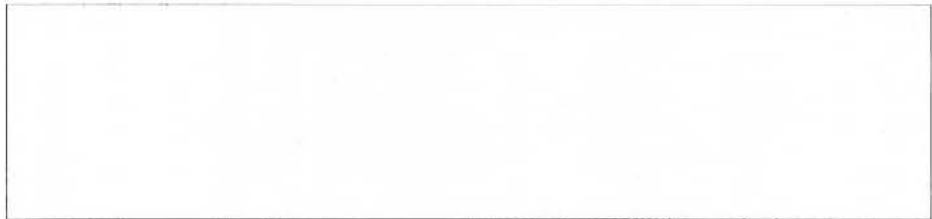
BODY

TAGS: PHUM, PGOV, PREF, TI
SUBJECT: P1 REFUGEE ADMISSIONS REFERRALS [Redacted]
REF: A) 2007 DUSHANBE 1420; B) 2011 DUSHANBE 27; C) 2011 DUSHANBE 13310;
CLASSIFIED BY: KEN GROSS, AMBASSADOR, DOS, EXEC; REASON: 1.4(B), (D)

[Redacted]

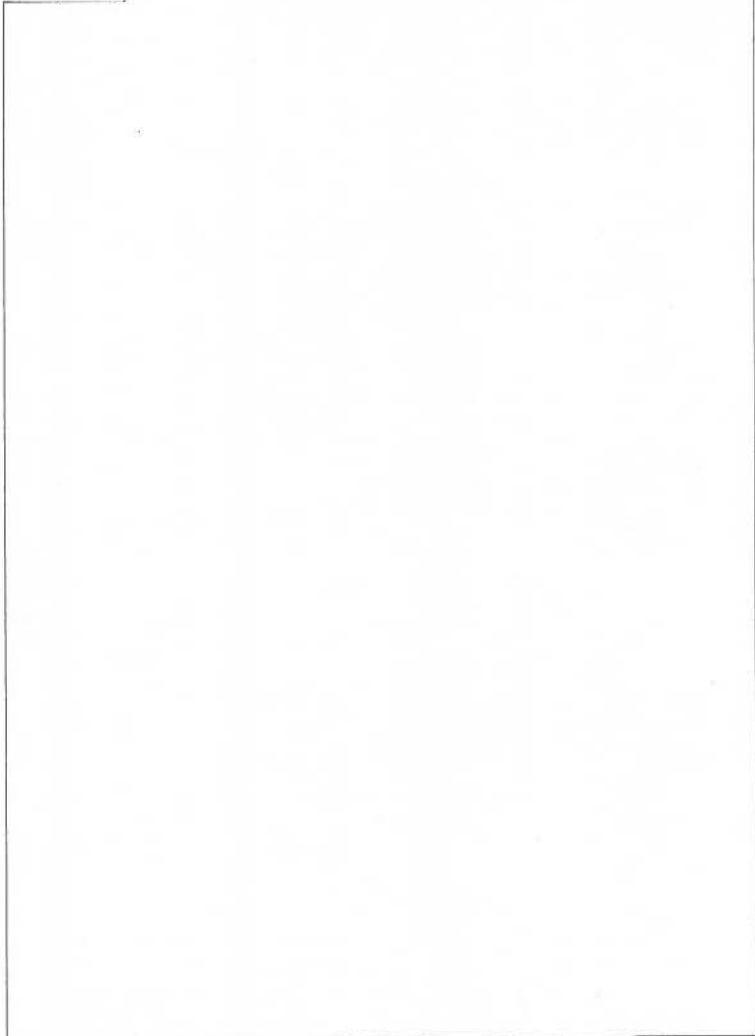
B3 INA
B6

B3 INA
B6
B1
1.4(D)

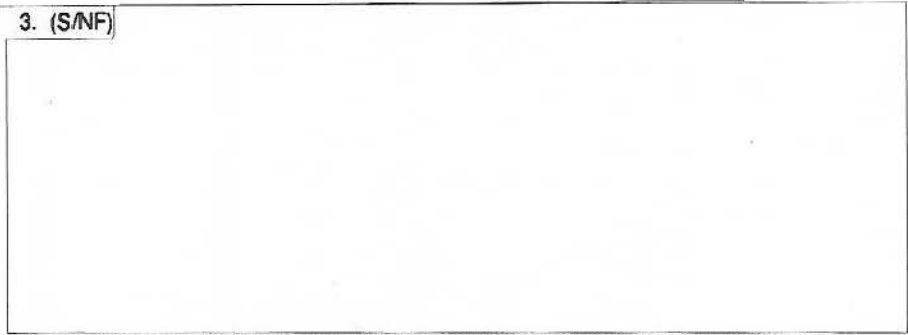


1.4(D)
B1
B3 INA
B6

2. (S/NF)



3. (S/NF)



4. (U) CONTACT INFORMATION CAN BE OBTAINED FROM MANUEL MICALLER,
EMBASSY DUSHANBE POLITICAL/ECONOMIC SECTION CHIEF: MICALLER
MP1@STATE.SGOV.GOV.

GROSS

ADMIN

BT
#0045

NNNN

SECRET
NOFORN;

DERIVED FROM: ms
DECLASSIFY ON: 20360222
DATE OF SOURCE: 20110222

CLASSIFICATION: SECRET//NOFORN

From:
To:
Subject:
Date:



B3
B6

CLASSIFICATION: CONFIDENTIAL

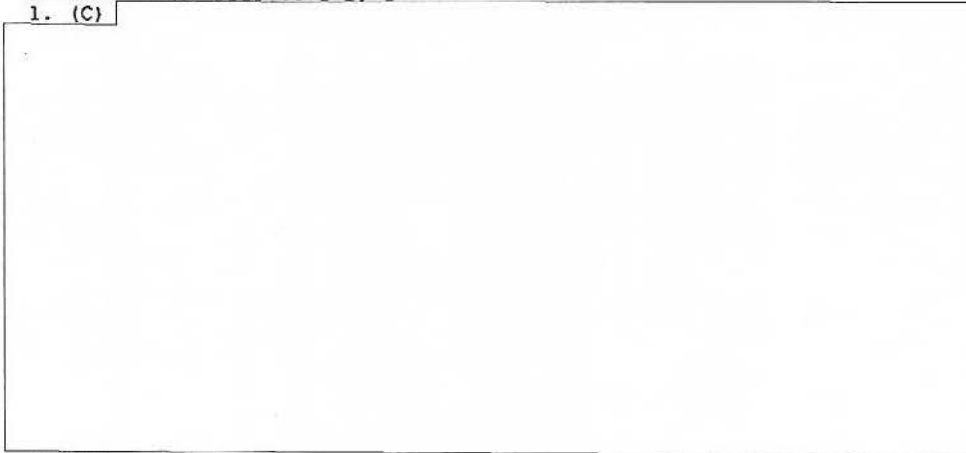
RELEASE IN PART
B1,1.4(B),1.4(D),B3,B6

R 200952Z JUL 11

FM AMEMBASSY PHNOM PENH

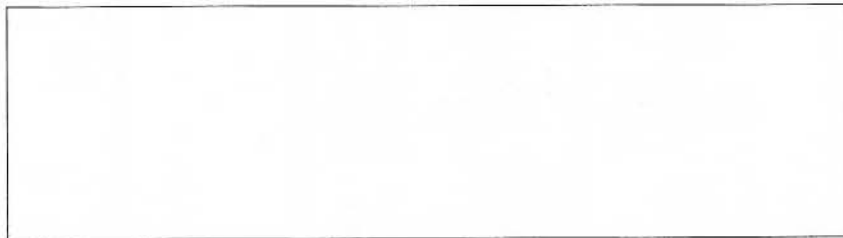
TO RUEHC/SECSTATE WASHDC
INFO ASEAN MEMBER COLLECTIVE

BT
C O N F I D E N T I A L PHNOM PENH 000221
R.O. 13526; DECT: 2021/07/20
TAGS: PGOV, PHUM, CB
SUBJECT: CAMBODIA: INDIVIDUAL NAMED IN WIKILEAKED CABLE RECEIVES
PHONE THREATS
REF: A) 07 PHNOM PENH 820;
DERIVED FROM: DSCG 05-1 B, D
1. (C)



1.4(B)
1.4(D)
B1
B6

DAIGLE
BT
#0221



B3
B6

DERIVED FROM: ms
DECLASSIFY ON: 20360723
DATE OF SOURCE: 20110725

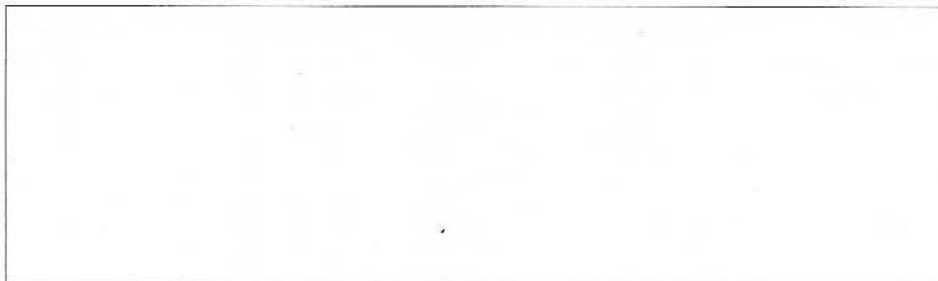
CLASSIFICATION: CONFIDENTIAL

#39

RELEASE IN PART
B5

WG Colleagues, please forward the info below to your FOs and to any posts that need a heads-up. All regional bureaus/posts should relay to the WG and S/CT any reactions from or engagements with host governments regarding this issue.

Current standard guidance that may be helpful, pending more specific guidance that S/CT may provide for clearance in the morning:



B5

INR Watch, please forward this information to watches at: NSA, OSD, NMCC, DHS, DOE, CIA, DIA, and CYBERCOM.

From: CMS TaskForce1C-Coordinator
Sent: Monday, December 06, 2010 1:35 AM
Subject: Reaching out re: 09 STATE 15113

On 12/5 at approximately 1500 EST, WikiLeaks released a cable alleged to be 09 STATE 15113, a S/NF cable from February 2009 that contains the entire list of about 300 U.S. critical foreign dependencies from the 2008 Critical Foreign Dependencies Initiative (CFDI) report. The CFDI is the international annex to the National Infrastructure Protection Plan (NIPP), both of which list and prioritize U.S. critical infrastructure and key resources (CIKR). The NIPP and CFDI are DHS responsibilities, but S/CT works with them to produce the CFDI lists.



B5

The WikiLeaks WG is reviewing all response cables and will contact posts which need a heads-up. We have reached out to WHSR, DOD, DHS, and the intelligence community. In the morning, S/CT and the WikiLeaks Working Group will coordinate guidance

for PA and affected posts. Until cleared specific guidance is released, posts and others should rely on current standard guidance regarding WikiLeaks, as contained in ALDACs.

Regards,

Deborah Schneider
Coordinator, WikiLeaks Working Group

#40

From:
To:

[Redacted]

B3
B6

Subject:

[Redacted]

B1

1.4(D)

Date:

Monday, July 25, 2011 1:11:11 PM

1.4(C)

B1

CLASSIFICATION: CONFIDENTIAL

RELEASE IN PART
B1,1.4(C),1.4(D),B3,B6

B3

B6

[Redacted]

[Redacted]

B1

1.4(D)

Full cable below:

O R 130805Z JUL 11

FM AMEMBASSY KUALA LUMPUR

TO RUEHC/SECSTATE WASHDC
INFO ASEAN MEMBER COLLECTIVE
RHHJJPI/PACOM IDHS HONOLULU HI

BT

CONFIDENTIAL KUALA LUMPUR 000567
***** THIS IS A COMBINED MESSAGE *****
E.O. 13526: DECL: 2021/07/13
TAGS: PGOV, PREL, MY

SUBJECT:

REF: A) 11 KUALA LUMPUR 321; B) 10 KUALA LUMPUR 839; C) 09 KUALA LUMPUR 268;
D) 10 KUALA LUMPUR 103; E) 10 KUALA LUMPUR 37; F) 10 KUALA LUMPUR 59;
G) 10 KUALA LUMPUR 20;

CLASSIFIED BY: PAUL W. JONES, AMBASSADOR; REASON: 1.4(D)

SUMMARY

1. (C)

[Redacted]

1.4(D)
B1

[Redacted]

2. (C)

[Redacted]

3. (C)

[Redacted]

4. (C)

[Redacted]

5. (C)

[Redacted]

6. (C)

*

*

[Redacted]



B1
1.4(D)



B3
B6

DERIVED FROM: ms
DECLASSIFY ON: 20360723
DATE OF SOURCE: 20110725

CLASSIFICATION: CONFIDENTIAL

~~SECRET//NOFORN~~

**Final Report of the
Department of Defense Information Review Task Force**

Executive Summary

(U) The Information Review Task Force (IRTF), at the direction of the Secretary of Defense, assessed the impact caused by the unauthorized WikiLeaks disclosure of U.S. government records. To complete the task, the IRTF completed a comprehensive review of more than 740,000 records known or believed to have been compromised to WikiLeaks. The IRTF coordinated its review throughout the Intelligence Community and integrated its efforts with those of the National Counterintelligence Executive (NCIX).

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

(U) *Overarching Summary of Impacts.* After a comprehensive review of all known compromised datasets, the IRTF assesses the greatest impact to the following Department of Defense equities:

- ~~(S//NF)~~ The lives of cooperating Afghans, Iraqis, and other foreign interlocutors have been placed at increased risk.

(b)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(1);(b)(5);(b)(3);10 USC 424;Sec. 1.4(c);Sec. 1.4(d)

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

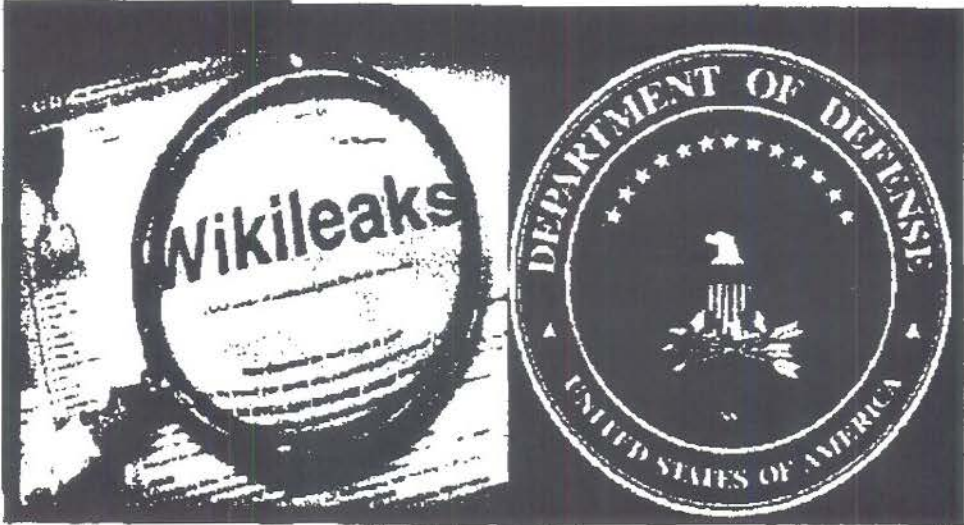
(b)(1);(b)(5);(b)(3);10 USC 424;Sec. 1.4(c);Sec. 1.4(d)

~~SECRET//NOFORN~~

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

June 15, 2011

21050126



(U) Information Review Task Force

(b)(3):10 USC 424

Defense Intelligence Agency

Derived From: DoD C-5240.8
Reason: (U)
Declassify on: 204005

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

(U) Table of Contents

(U) Executive Summary3
(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

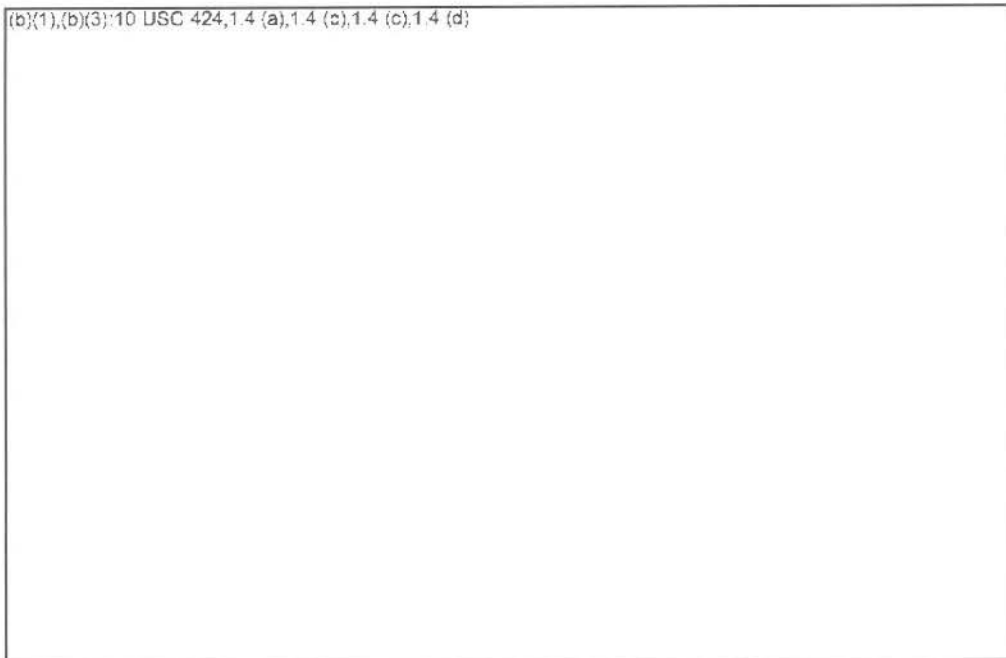
(U) At the direction of the U.S. Secretary of Defense (SecDef), the Information Review Task Force (IRTF) assessed the impact of unauthorized WikiLeaks disclosure of United States Government (USG) records. The IRTF completed a comprehensive review of more than 740,000 records known or believed compromised 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~~

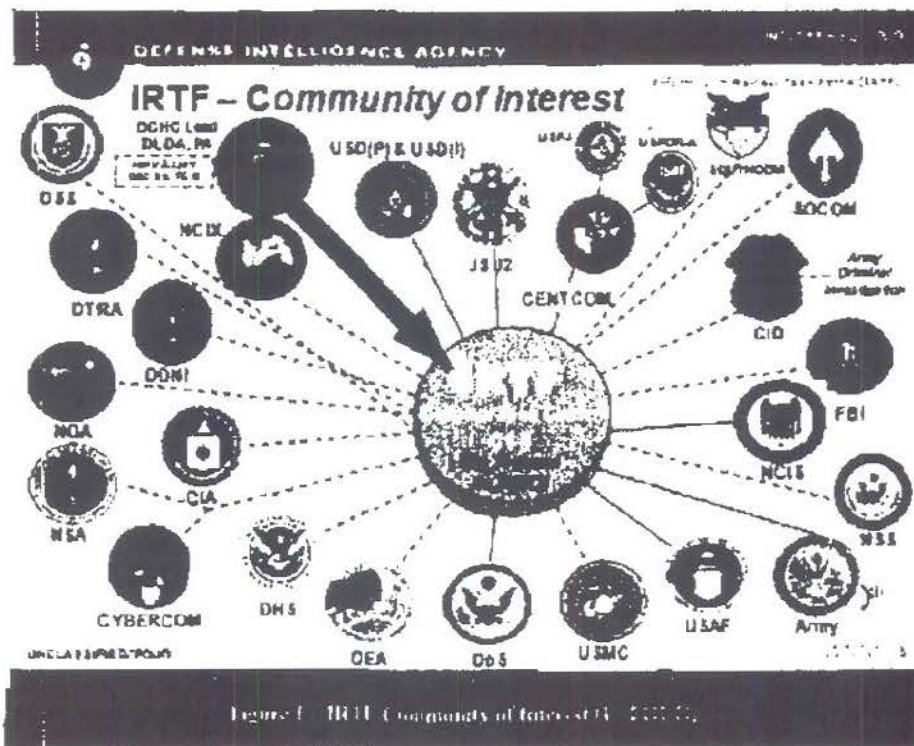
(U) Due to the sheer volume of information the IRTF reviewed, this report focuses on the most significant findings centered on the seven key focus areas, a general overview of what was learned, and selected examples and summaries of relevant reports to provide context.

(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.



(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.

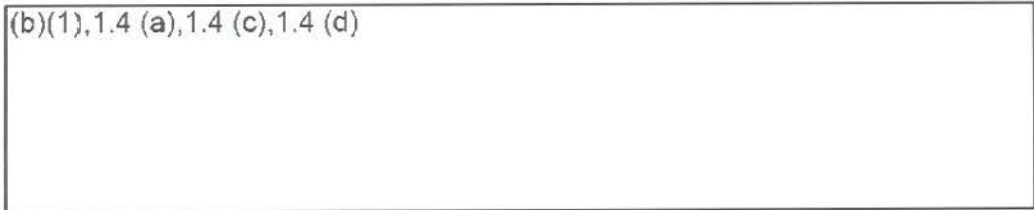
(b)(3):50
USC 3024(i)

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

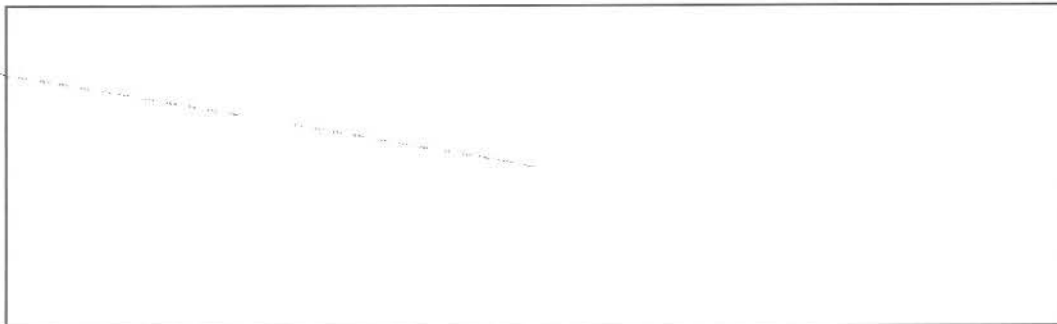


Figure 2. CIDNE-A Data Sets (SI)

- (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

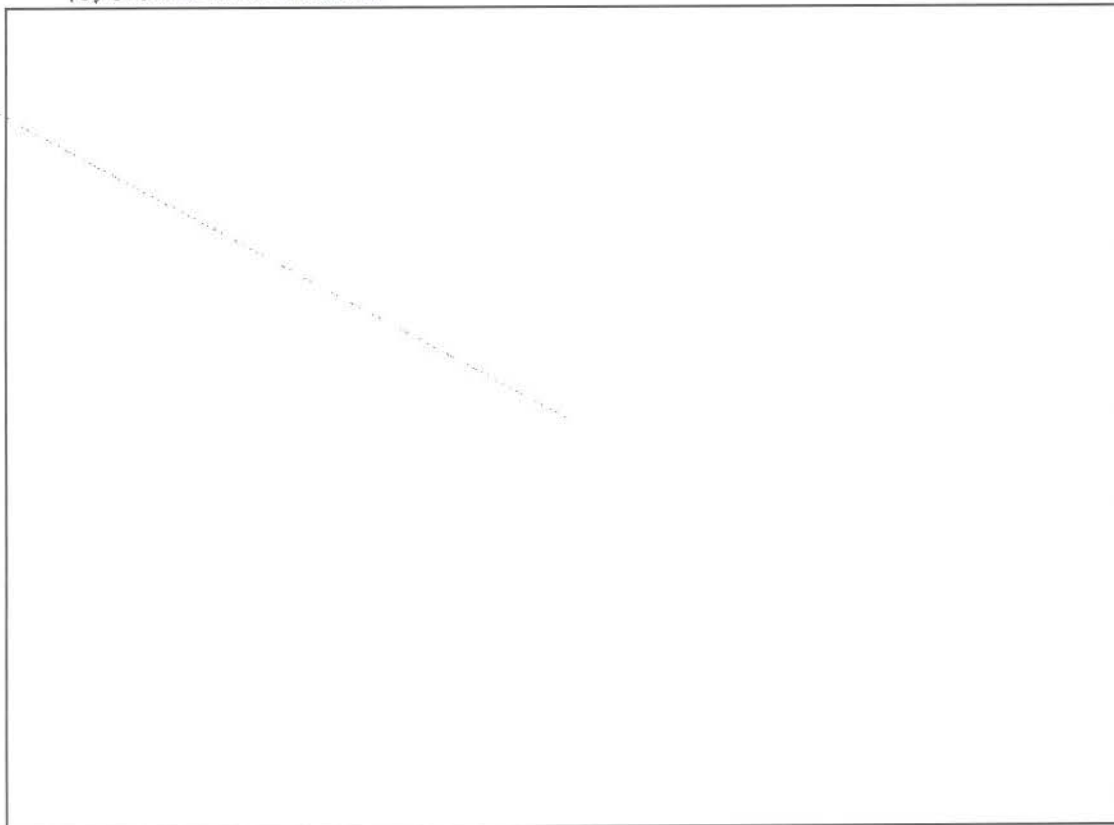
(b)(3):50 USC
3024(i)

(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.

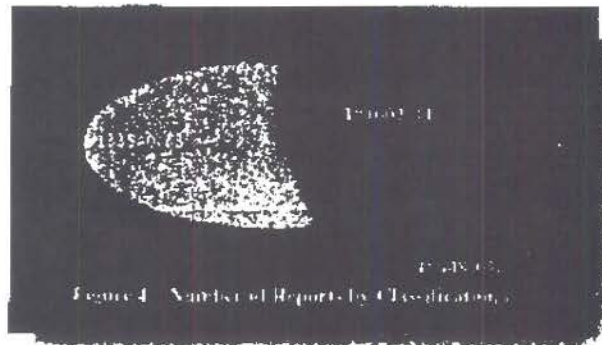


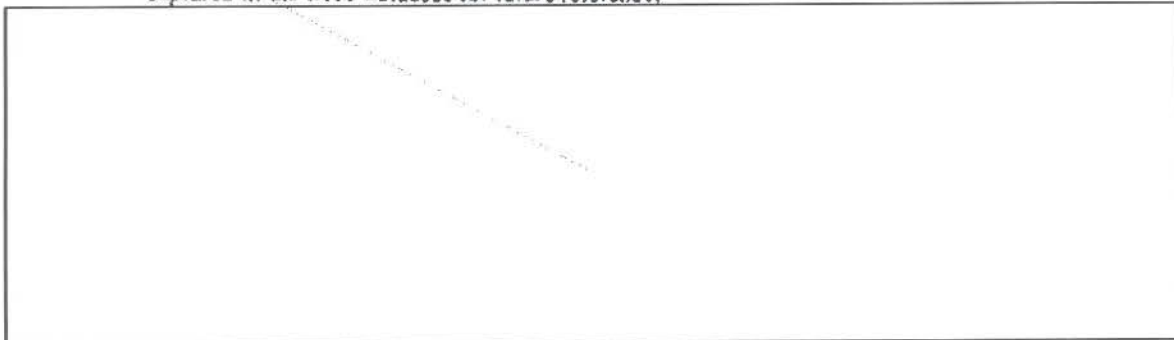
Figure 4 - Number of Reports by Classification

~~(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." 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)

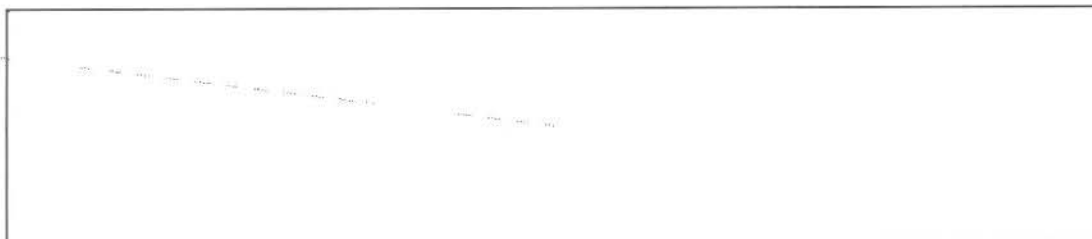
(U) The WikiLeaks website provided access to the Afghan data in a variety of formats, including HTML (web), CSV (comma-separated values), SQL (database), and KML (Keyhole Markup Language) geospatial data that can be used with visualization tools such as Google Earth.

(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)

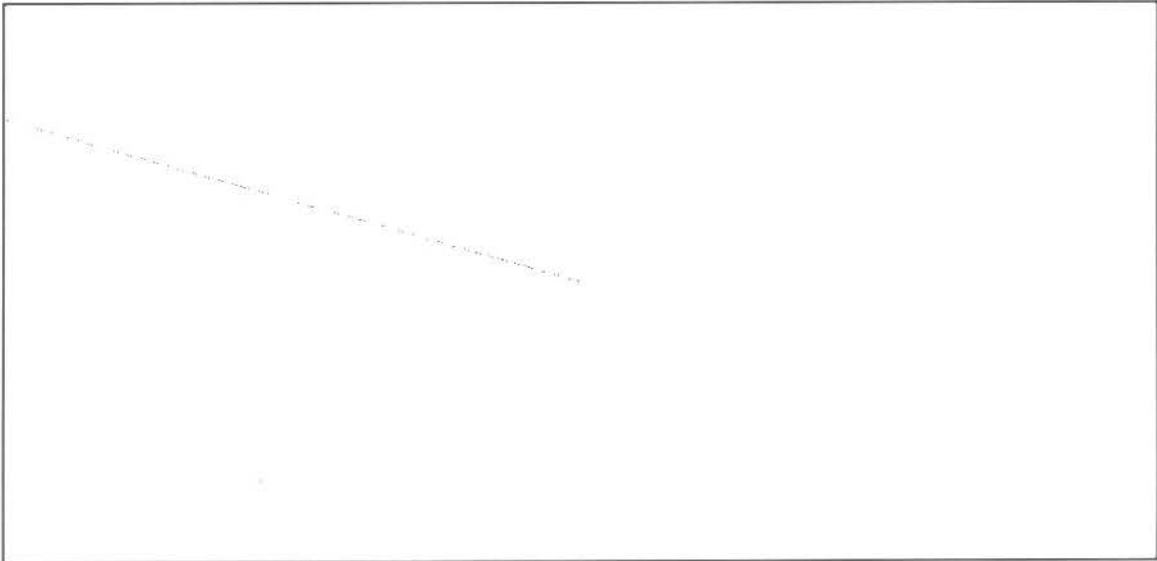
- (U//~~FOUO~~) PII concerning 23 U.S. soldiers, including full names and social security numbers. All affected individuals have been notified.

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

~~SECRET//NOFORN~~

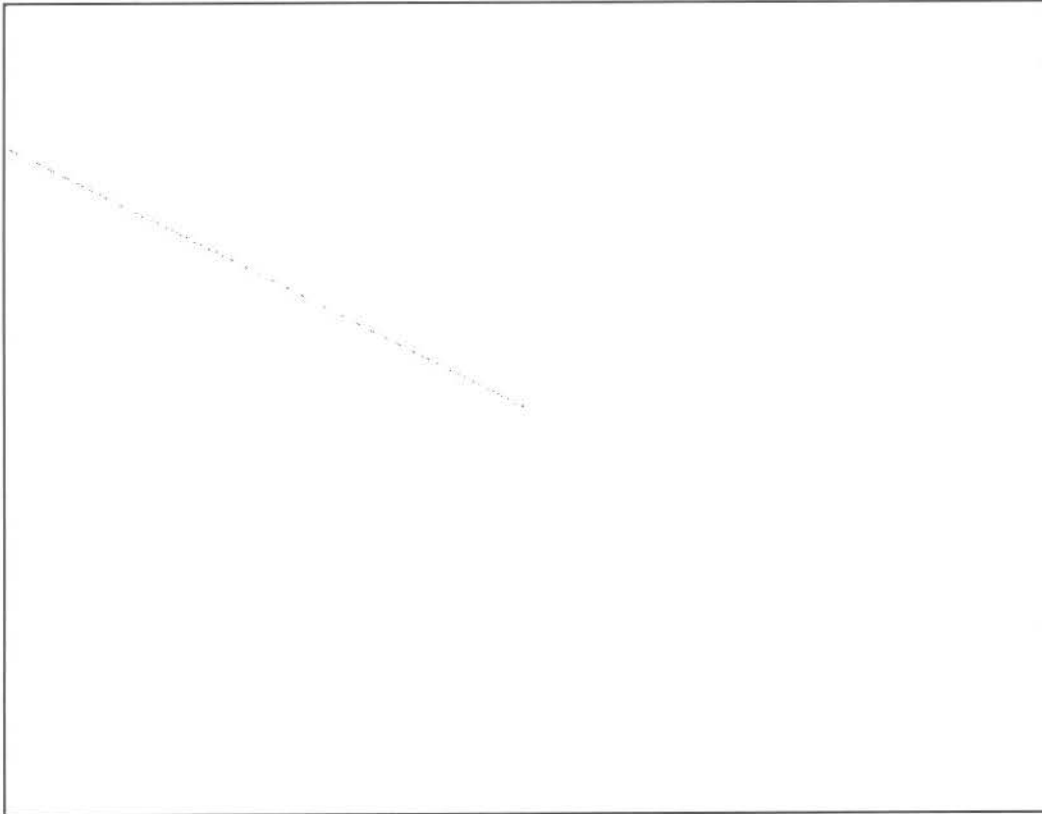
~~SECRET//NOFORN~~

(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)

~~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)

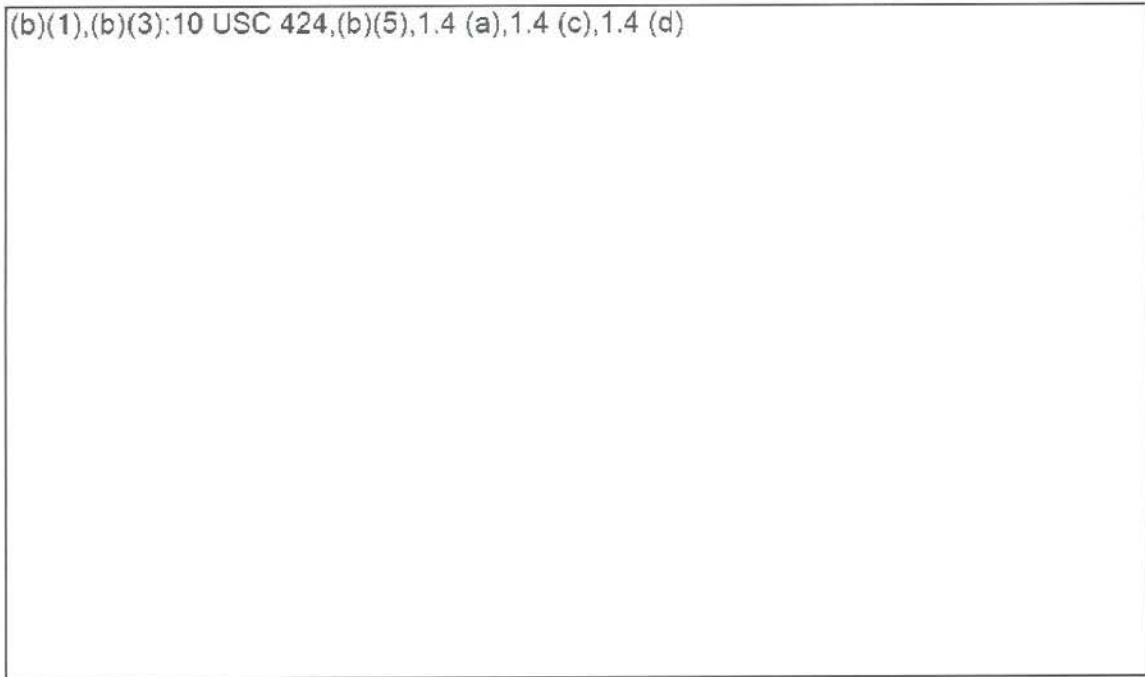
- (U) Other Causes:

(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)



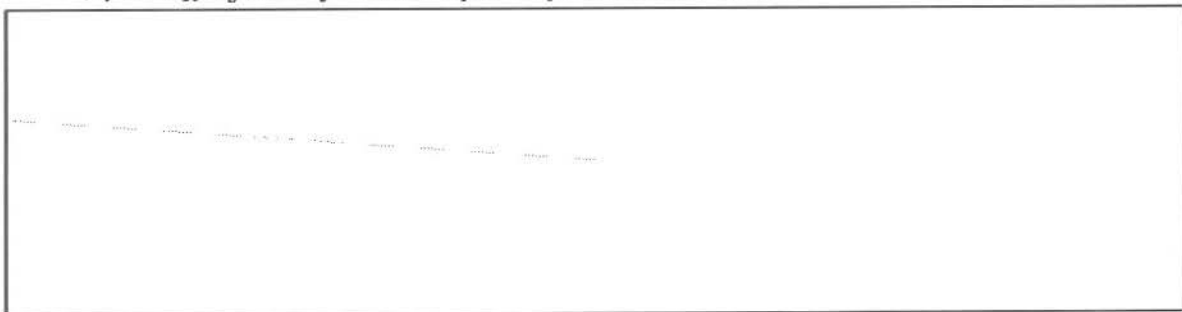
(U) Current and Former Senior U.S. Leadership in Iraq

(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~~

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

¹¹ (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~~

(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

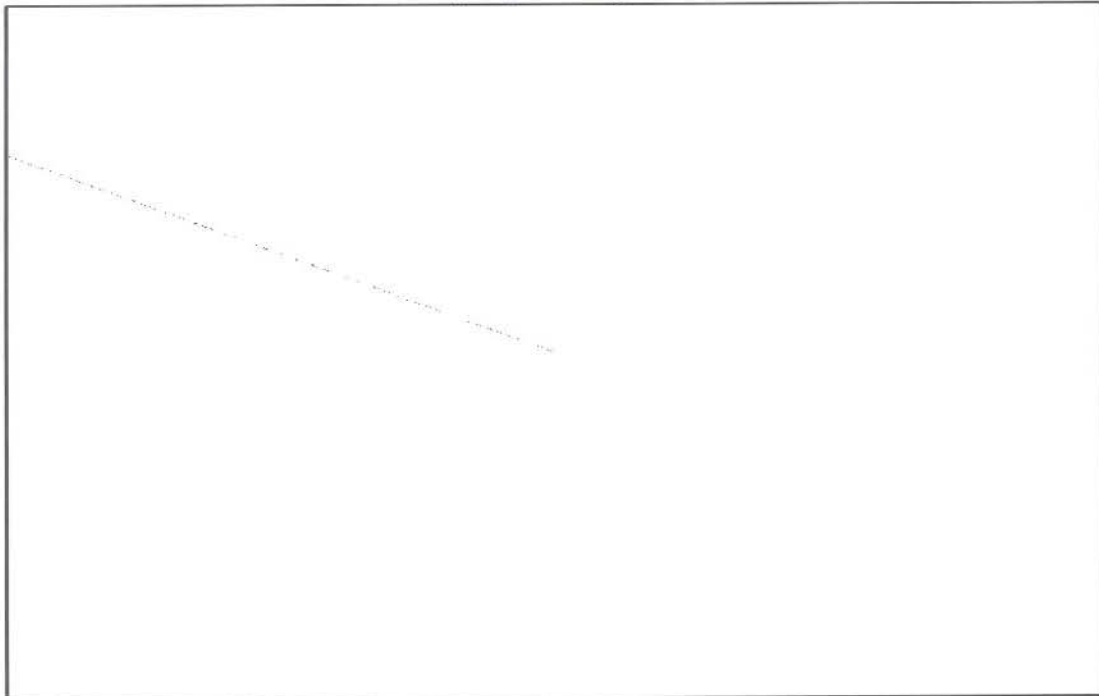
(U) Background

(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)

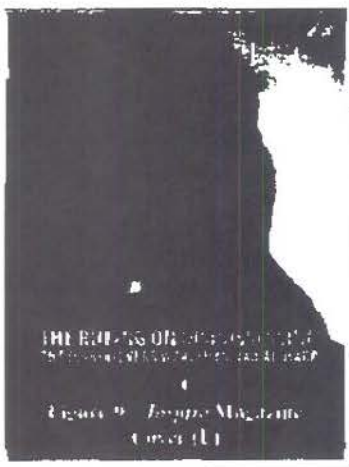
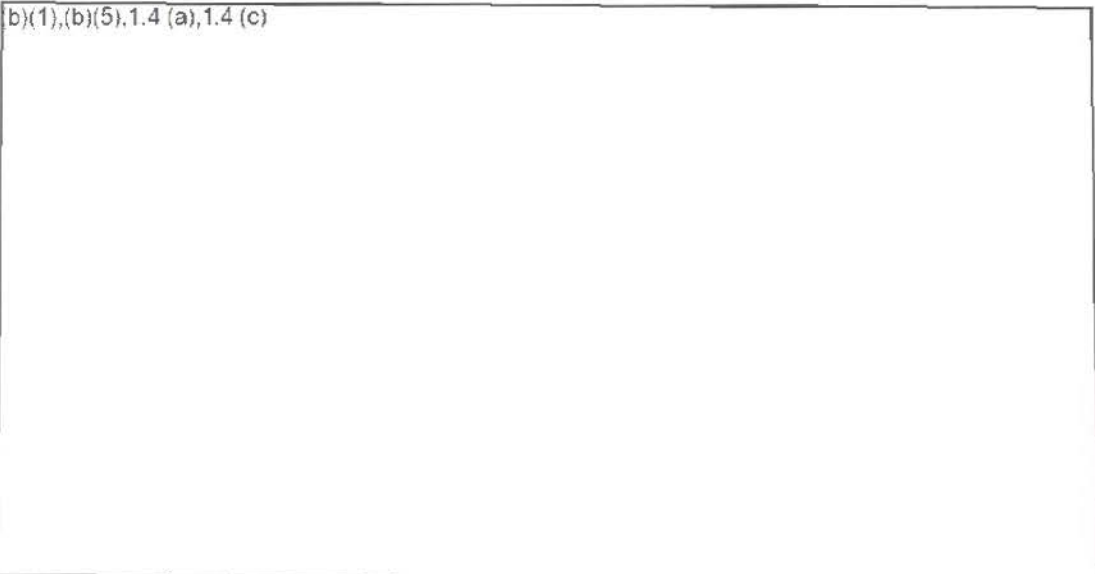
(U) Force Dispositions and Vulnerabilities

(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

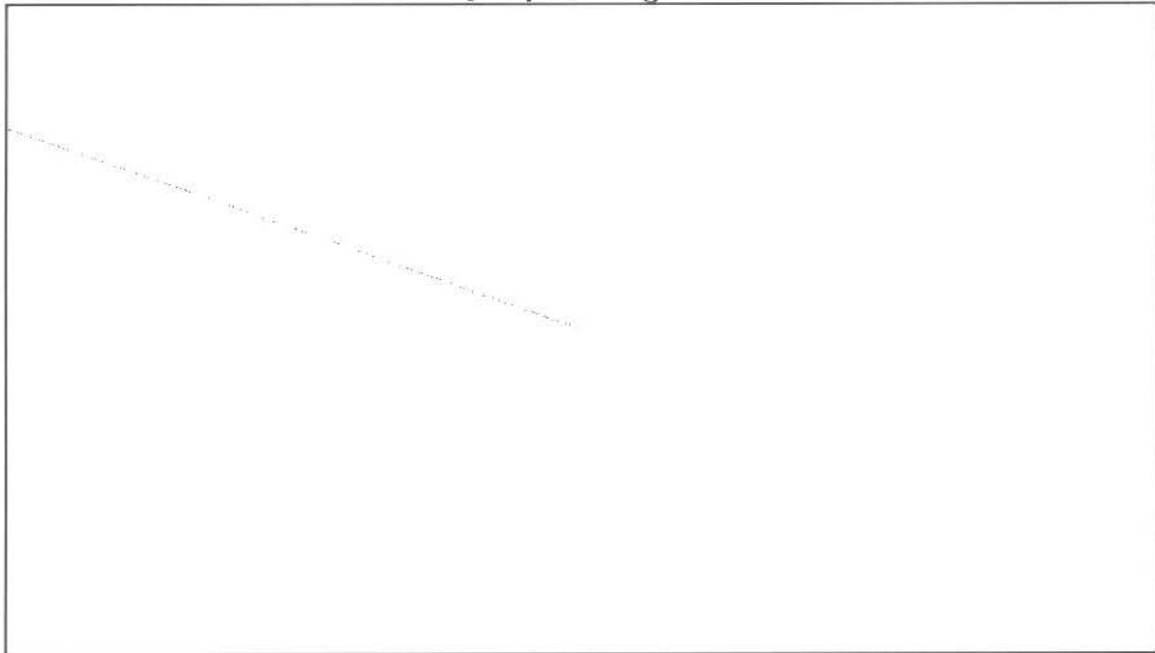
(b)(1),(b)(3):10 USC 424,(b)(3):50 USC 3024(i),1.4 (a),1.4 (c)

~~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 Intellipedia 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~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

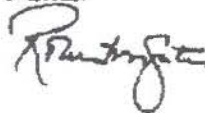
~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

- ~~(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 USD(I) 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~~

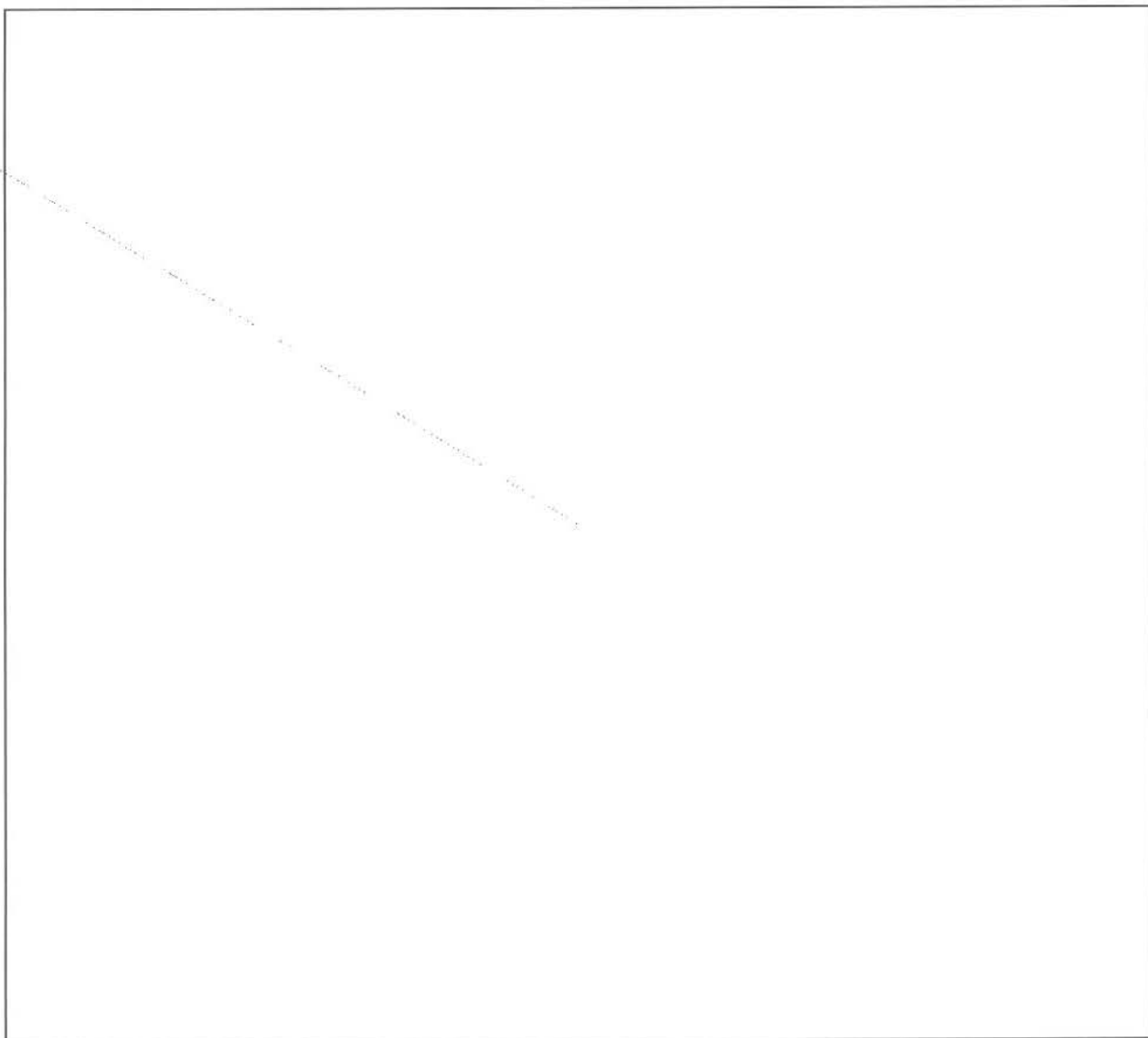
~~SECRET//NOFORN~~

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	Israel	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~~

(b)(3):10 USC
424,(b)(6)

From: [Redacted]
To: [Redacted]
Cc: [Redacted]
Subject: FW: (U) Information Review Task Force (IRTF) – February 22 and 28, 2011 Updates
Date: Tuesday, March 01, 2011 3:57:58 PM
Attachments: [11-0362 \(U\) Information Review Task Force \(IRTF\) – February 22, 2011 Update.pdf](#)
[11-0415 \(U\) Information Review Task Force \(IRTF\) – February 28, 2011 Update.pdf](#)

CLASSIFICATION: ~~SECRET//NOFORN~~

We got an A+ from the DD. Thank you again for your excellent edits!

(b)(3):10 USC
424,(b)(6)

From: [Redacted]
Sent: Tuesday, March 01, 2011 12:48 PM
To: [Redacted]
Cc: [Redacted]
Subject: (U) Information Review Task Force (IRTF) – February 22 and 28, 2011 Updates

CLASSIFICATION: ~~SECRET//NOFORN~~

All –

(U) Attached please find the last two WikiLeaks IMs for your records. I appreciate the very quick turnaround on this week's IM so we could get it to the DD for his signature before he left for his TDY tomorrow. The DD had the follow feedback on this week's IM:

(b)(1),Sec. 1.4
(c)

[Redacted]

(U) Please be sure to pass the feedback to the seniors. Thanks again for the quick turn.

(b)(3):10 USC
424,(b)(6)

[Redacted]

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~20260301~~

DATE OF SOURCE: ~~20110301~~

CLASSIFICATION: ~~SECRET//NOFORN~~

DERIVED FROM: ~~MS~~

DECLASSIFY ON: ~~20360301~~

DATE OF SOURCE: ~~20110301~~

CLASSIFICATION: ~~SECRET//NOFORN~~

The next page is withheld in full and is not included.

(b)(3):10 USC
424,(b)(6)

From: [Redacted]
To: [Redacted]
Subject: [Redacted]
Date: Monday, August 09, 2010 6:41:00 AM

(b)(5)

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

FYSA

(b)(3):10 USC
424

[Redacted]

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

(b)(3):10 USC
424,(b)(6)

From: [Redacted]
Sent: Friday, August 06, 2010 12:19 PM
To: [Redacted]
Cc: [Redacted]
Subject: RE: [Redacted]

(b)(5)

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(5)

I'm going to call [Redacted] and advise him of the situation. I'll let you know what they say.

(b)(3):10 USC
424

[Redacted]

(b)(3):10 USC
424,(b)(5)

From: [Redacted]
Sent: Friday, August 06, 2010 11:23 AM
To: [Redacted]
Cc: [Redacted]
Subject: [Redacted]

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

(b)(3):10 USC
424

[Redacted]

(b)(3):10 USC
424,(b)(5),(b)(6)

Thank you for your input regarding this issue. [Redacted]

V/r,
[Redacted]

(b)(3):10 USC
424



This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

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

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

The remaining 4 pages are withheld in full and are not included.

INFO MEMO

~~S~~ 11-0285A/IRTF

30 March 2011

(b)(3):10 USC
424, (b)(6)

FROM: Chief, Information Review Task Force

SUBJECT: (U) Key Areas of Concern for Pakistan in Net Centric Diplomacy Database

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

(U) Force Protection Concerns

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

Derived from: ~~Multiple Sources~~
Declassify on: ~~FOUO~~

Information Review Task Force Situation Update



(b)(3); 10 USC 424,(b)(6)

IRTF Chief

1 December 2010 – 0800

Derived from: ~~Multiple Sources~~
Declassify on: ~~20051201~~

This briefing is classified
~~SECRET//NOFORN~~

UNCLASSIFIED



CELEBRATING OUR LEGACY
FORGING OUR FUTURE



Agenda

Battle Rhythm

Functional Representatives

- **Congressional and Public Affairs**

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

Staff Director and DA Update

Analysis & Production

Task Tracking

Questions / Guidance





1 Dec Battle Rhythm

	IRTF	SUSPENSES TO DX	SENIOR LEVEL MEETINGS
06:00 :30			
07:00 :30	Morning Pre-Brief	Email Brief to VTC Members	
08:00 :30	Morning Brief		IRTF Morning Brief
09:00 :30	IRTF Leadership Meeting		
10:00 :30			
11:00 :30	Daily Talking Points for BG Carr Due		HPSCI Briefing
12:00 :30		Daily Talking Points Due	
13:00 :30			
14:00 :30			
15:00 :30	Interagency Pre-Brief	Email Brief to VTC Participants	(b)(3):10 USC 424,(b)(6)
16:00 :30	Interagency VTC		Interagency VTC
17:00 :30			
18:00			



Congressional and Public Affairs Liaison

- Media: AP, NY Times, Guardian, Voice of Russia, Telegraph, Boston Herald, Register, MSNBC, The Hindu, NY Post, Politico, Reuters, Deutsche Welle, Financial Times, Chronicle Herald, Korea Times, Prague Post, Radio Free Europe, NPR, Bloomberg, Asia Times online, Al Arabiya... **“Virtually all media outlets continue carrying WikiLeaks story”**

(b)(3): 10 USC 424

- Reporting Examples:
 - WikiLeaks website blocked behind Chinese firewall (AP)
 - U.S. Officials insist Clinton not ordering diplomats to spy (CNN)
 - WikiLeaks says Bank of America is next target (Asia Bizz)
 - WikiLeaks: Kuwait wanted GTMO detainees to be killed in combat (Telegraph)

50th



The next 4 pages are withheld in full and are not included.

Congressional and Public Affairs Liaison

- Reporting Examples Cont:
 - Interpol adds Assange to wanted list (Business Week)
 - WikiLeaks disclosures complicate Clinton’s visit to Kazakhstan (Wash Post)
 - Putin criticizes U.S. remarks on Russia (NY Times)

- Congressional: Briefings
 - HPSCI Briefing – 1100 Wednesday Rm. HVC 304
 - SSCI Briefing – 1400 Wednesday “Cancelled”
 - Briefing to Senate consolidated Committee – 1030 Thursday Rm. SVC 217
 - Briefing to House consolidated Committee – 1200 Thursday Rm. 2118 Rayburn


(b)(3); 10 USC 424, (b)(6)





The next 3 pages are withheld in full and are not included.

Assange Interpol Arrest Warrant




30 November 2010

- Home
- About INTERPOL
- News
- Flags
- Criminal organizations
- Pharmaceutical crime
- Financial and High Tech crime
- Intellectual Property
- Rights Programme
- Fugitives

Wanted

ASSANGE, Julian Paul



Home | Search | Contact | Help

Legal

Present family name	ASSANGE
Forename	JULIAN PAUL
Sex	MALE
Date of birth	3 July 1971 (39 years old)
Place of birth	TOWNSVILLE, Australia
Language spoken	English
Nationality	Australia

Offences

Categories of offences	SEX CRIMES
------------------------	-------------------





The next 5 pages are withheld in full and are not included.

Der Spiegel – Haggling with Allies over New Homes for Detainees

- Critical on German government, article supportive of GTMO closure. Why was German government intractable?
- Negative reaction of Chinese government over Uighers. Berlin reluctant to take 17 Uighers despite population of 500 in Munich.
- Supportive of Amb Fried and humanitarian cause
 - After rebuffed on Uigher issue supportive of Amb Fried to repatriate sick detainee and his brother, both Uigher
- Efforts by U.S. to get cooperation on rehabilitation centers in Maldives, Yemen and Slovenia
- Plight of 8 Uigher detainees in Albania frustrated Washington
 - Situation in Tirana threatened to spiral out of control

50th



QUESTIONS / GUIDANCE

50th

CELEBRATING OUR LEGACY
FORGING OUR FUTURE

Information Review Task Force Situation Update



(b)(3):10 USC 424,(b)(6)

IRTF Chief

1 November 2010 – 0800

Derived from: ~~Multiple Sources~~
Declassify on: ~~2005-1-01~~

This briefing is classified

~~SECRET//NOFORN~~

UNCLASSIFIED



1961-2011
CELEBRATING OUR LEGACY
FORGING OUR FUTURE



Agenda

Battle Rhythm

Functional Representatives

- **Congressional and Public Affairs**

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

Staff Director and DA Update

Analysis & Production

Task Tracking

Questions / Guidance



1 Nov Battle Rhythm

Information Review Task Force (IRTF)

	IRTF	SUSPENSES TO DX	SENIOR LEVEL MEETINGS
06:00			
:30			
07:00	Morning Pre-Brief		
:30		Email Brief to VTC Members	
08:00	Morning Brief		IRTF Morning Brief
:30			
09:00	IRTF Leadership Meeting		
:30			
10:00			
:30			
11:00			OSD Steering Group
:30	Daily Talking Points for BG Carr Due		
12:00		SECDEF Weekly Update	
:30			
13:00			
:30			
14:00			
:30			
15:00	Afternoon Pre-Brief		
:30		Email Brief to VTC Participants	
16:00	Interagency VTC		Interagency VTC
:30			
17:00			
:30			
18:00			



Congressional and Public Affairs Liaison

- Media: New York Times, WSJ, Guardian, Huffington Post, New York Magazine, Boston Globe, Sydney Morning Herald, Asia Times online, Atlantic, Al-Arabiya, Times of India, Mathaba, Cryptome, cnet, Raw Story

(b)(3):10 USC 424

- Reporting Highlights:
 - UK Troops face 90 new claims of abuse in Iraq (Guardian)
 - Guarding secrets that define us (Boston Globe)
 - Guard led 3 Americans across the Iran border, released hiker says (New York Times)
 - Journalism scoops WikiLeaks (WSJ)
 - U.S. Senator urges WikiLeaks Probe (Press TV)
 - Sweeping away a culture of secrecy (Sydney Morning Herald)



The next 17 pages are withheld in full and are not included.

Information Review Task Force (IRTF)

Congressional and Public Affairs Liaison

- Reporting Highlights:
 - WikiLeaks threatens journalism and espionage (Cryptome)
 - Sharing secrets at arms length (NY Times)
 - Reporter's roundtable – Can you trust WikiLeaks? (cnet)
 - One day in Iraq – WikiLeaks War Logs (New Zealand Herald)

- Public Affair Posture Support: TPs and PAG and Q & A Completed (15k) – Ready for approval by DCHC Leadership

- Congressional: NSTR



QUESTIONS / GUIDANCE



1961-2011
CELEBRATING OUR LEGACY
FORGING OUR FUTURE

#614

Pages 2-5 are withheld in full
and are not included.

~~SECRET//NOFORN~~

Information Review Task Force Information Brief (U)



(b)(3):10 USC 424;(b)(6)

15 October 2010

This briefing is classified

~~SECRET//NOFORN~~

Derived from: ~~Multiple Sources~~

Declassify on: ~~20331000~~

~~SECRET//NOFORN~~



WikiLeaks & Julian Assange



- Australian journalist, programmer and Internet activist
- “Australia’s most infamous former computer hacker” according to Counter Punch magazine
- Best known for his involvement with WikiLeaks
 - Sits on nine-member advisory board of WikiLeaks
 - Prominent media spokesman on its behalf
 - Claims to be an “unpaid volunteer”
- Ongoing internal strife with other staffers & volunteers

“I am the heart and soul of this organization, its founder, philosopher, spokesperson, original coder, organizer, financier and all the rest. If you have a problem with me, piss off.”

-- Julian Assange*

* As quoted in *Unpublished Iraq War Logs Trigger Internal WikiLeaks Revolt* by Kevin Poulsen and Kim Zetter, 27 Sep 2100, Wired.com



QUESTIONS



(b)(3):10 USC 424

#615

The next 4 pages are withheld in full and are not included.

UNCLASSIFIED

Information Review Task Force Information Brief (U)



DoD HUMINT/CI Legal Workshop December 2010

This briefing is classified

~~SECRET//NOFORN~~

Derived from: ~~Multiple Sources~~

Declassify on: ~~20051025~~

50th

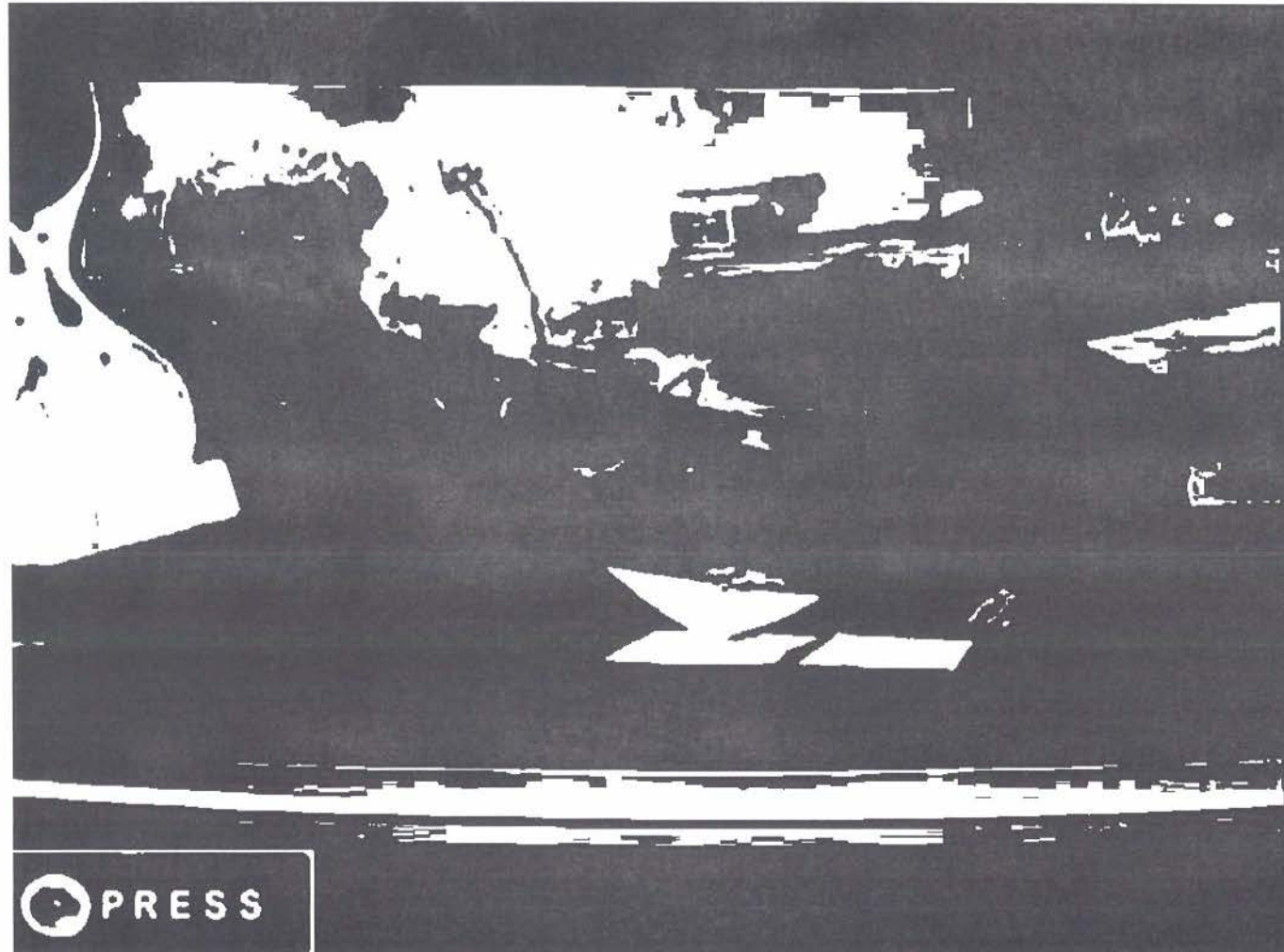
CELEBRATING OUR LEGACY
FORGING OUR FUTURE

UNCLASSIFIED

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION



WikiLeaks Release of the secret data in “Iraq War Logs” endangers US troops, Iraqis, Afghans.



50th

CELEBRATING OUR LEGACY
FORGING OUR FUTURE



WikiLeaks & Julian Assange



- Australian journalist, programmer and Internet activist
- “Australia’s most infamous former computer hacker”
-- Counter Punch Magazine
- Best known for his involvement with WikiLeaks
 - Sits on nine-member advisory board of WikiLeaks
 - Prominent media spokesman on its behalf
 - Claims to be an “unpaid volunteer”
- Ongoing internal strife with other staffers & volunteers

“I am the heart and soul of this organization, its founder, philosopher, spokesperson, original coder, organizer, financier and all the rest. If you have a problem with me, piss off.”

-- Julian Assange*

* As quoted in *Unpublished Iraq War Logs Trigger Internal WikiLeaks Revolt* by Kevin Poulsen and Kim Zetter, 27 Sep 2100, Wired.com



QUESTIONS



(b)(3):10 USC 424



MISC BACKUP SLIDES



Open Source – Baghdad Air Strike Video

- On 5 April 2010, WikiLeaks released classified U.S. military footage from a series of attacks on 12 July 2007 in Baghdad by a U.S. helicopter that killed 12, including two Reuters news staff, on a website called “Collateral Murder”
- Footage consisted of a 39-minute unedited version and an 18-minute version which had been edited and annotated
- Analysis of the video indicates that the pilots thought the men were carrying weapons (which were actually camera equipment)

Source: <http://en.wikipedia.org/wiki/WikiLeaks> (accessed 9/15/2010)

Posted to WikiLeaks website on 5 April 2010

50th



What We Mean When We Say

We use phrases such as we judge, assess, estimate, anticipate, believe, or expect to convey analytical assessments. Such statements are not facts, knowledge, or proof.

LIKELINESS EXPRESSIONS

Because analytic judgments are not certain, we use probabilistic language to reflect our judgment of the likelihood that a development or an event will occur.

In rare circumstances when we cannot assess likelihood, we use terms *may*, *could*, *might*, or *possibly*.

CONFIDENCE LEVELS

Confidence is a judgment based on three factors: strength of the knowledge base, to include the quality of the sources and our depth of understanding about the issue; the number and importance of assumptions used to fill information gaps; and the strength of logic underpinning the argument, which encompasses the number and strength of analytic inferences as well as the rigor of the analytic methodology in the product.

HIGH	Well-corroborated information from proven sources, minimal assumptions, and/or strong logical inferences.
MODERATE	Partially corroborated information from good sources, several assumptions, and/or a mixture of strong and weak inferences.
LOW	Uncorroborated information from good or marginal sources, many assumptions, and/or mostly weak inferences.



Initial Iraqi Reactions (Open Source)

- Iraqis asked about the content of the release generally responded that they weren't surprised
- Most stated that the casualty count is even higher than the new numbers
- Iraqis said reflections of Iranian meddling in the reporting merely corroborated their opinions
- Prime Minister Maliki's office criticized WikiLeaks, accusing it of releasing documents that were being used "against national parties and leaders, especially against the prime minister."

50th



Passed to WikiLeaks – continued

- **26 Jul 2010, Info leaked to WikiLeaks...** (www.wired.com)
“A detailed Army database of 500,000 events in the Iraq war from 2004 through 2009. This has not been published or acknowledged by Wikileaks.”
- **27 Jul 2010, “WikiLeaks Iraq Cache More Than Three Times As Big”** (www.newsweek.com/declassified)
“...cache of classified U.S. military reports on the Iraq War.... Assange is keeping tighter personal control over the Iraq material than he maintained over the Afghan material, ...it’s not clear whether any media organizations have had advance access to it or when it might be made public.”

50th



Passed to WikiLeaks – continued

- 9 Sep 2010, ***“Exclusive: WikiLeaks Collaborating With Media Outlets on Release of Iraq Documents”***
(www.newsweek.com/declassified)

“A London-base journalism nonprofit is working with the WikiLeaks Web site and TV and print media in several countries on programs and stories based on what is described as massive cache of classified U.S. military field reports related to the Iraq War.”



*“A London-based journalism nonprofit is working with the WikiLeaks Web site and TV and print media in several countries on programs and stories based on what is described as (a) massive cache of classified U.S. military field reports related to the Iraq War.” Newsweek
9 September 2010*





Passed to WikiLeaks – continued

- 28 Sep 2010, “*Wikileaks is Imploding*” (www.theinquirer.net)

“Wikileaks is set to release the trove of Iraq data on 18 October, which ex-staffers feel is far too early. They want to make sure that the names of US collaborators and informants in Iraq are properly removed to make sure they are not killed.”

409K
CIDNE-I
391,832 Reports
Released

“...at least six Wikileaks staffers have apparently quit in recent weeks, including Daniel Domscheit-Berg, who was Wikileaks’ German spokesman.”



“...editing of the most recent batch of 15,000 documents was completed weeks ago, according to some former Wikileaks’ staffers, but Assange has held off publishing those reports for reasons he has not shared with the group.”

15K
CIDNE-A
Pending Release

Iraq War Logs posted to WikiLeaks website 5:00 pm 22 October 2010



#620

The next page is withheld in full and is not included.

UNCLASSIFIED

Information Review Task Force National Security Impact Brief (U)



(b)(3):10 USC 424;(b)(6)

27 January 2011

This briefing is classified

~~TOP SECRET~~ (b)(3):50 USC 3024 ~~NF~~

Derived from: ~~Multiple Sources~~
Declassify on: ~~00000106~~



UNCLASSIFIED

CELEBRATING OUR LEGACY
FORGING OUR FUTURE



What is WikiLeaks Doing?

According to Assange:

- **Harm the US War Effort:** *“The most dangerous men are those who are in charge of war. And they need to be stopped.” “I enjoy helping people who are vulnerable. And I enjoy crushing bastards. So it is enjoyable work.”*
- **Expose Sources:** *“We are not obligated to protect other people’s sources,” including sources of “spy organizations or militaries.” ...the Afghan public “should know about” people who have been involved in “genuinely traitorous” acts.*





QUESTIONS

(b)(3):10 USC 424



#624

Information Review Task Force Situation Update



(b)(6);(b)(3):10 USC 424

14 February 2011 - 1600

Derived from: ~~Multiple Sources~~
Declassify on: ~~20000211~~

This briefing is classified

~~TOP SECRET~~ (b)(3):50 USC 3024(f) ~~NOFORN~~

UNCLASSIFIED



CELEBRATING OUR LEGACY
FORGING OUR FUTURE



Agenda

- **Analysis and Production Update**

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

- **VTC Participants**
- **Questions / Guidance**





QUESTIONS / GUIDANCE

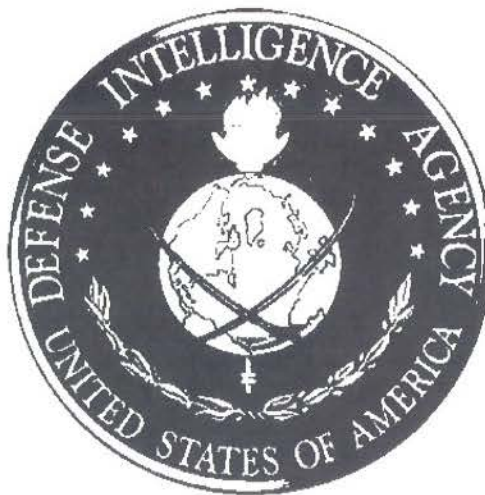
(b)(3):10 USC 424

50th

#1025

UNCLASSIFIED

Information Review Task Force Situation Update



(b)(6);(b)(3);10 USC 424

25 October 2010 - 1600

Derived from: ~~Multiple Sources~~
Declassify on: ~~20051025~~

This briefing is classified

~~SECRET//NOFORN~~

UNCLASSIFIED

50th

CELEBRATING OUR LEGACY
FORGING OUR FUTURE



Agenda

Analysis and Production Update

- **WikiLeaks Status Update**

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

Ongoing Lines of Operation

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

IRTF VTC Participants

Questions / Guidance





WikiLeaks Status

WikiLeaks.org and related sites are active

- Primary WikiLeaks.org site is active and directing traffic to two interfaces for accessing reports, WarDiary and WARlogs
- Both allow easy exploration of the 392k in a user friendly graphic interface
- Both contain significant redactions





QUESTIONS / GUIDANCE

50th

Information Review Task Force Situation Update



(b)(6);(b)(3);10 USC 424

30 November 2010 - 1600

Derived from: ~~Multiple Sources~~
Declassify on: ~~2005-1-00~~

This briefing is classified
~~SECRET//NOFORN~~

UNCLASSIFIED



CELEBRATING OUR LEGACY
FORGING OUR FUTURE



Agenda

- **Ongoing IRTF Analysis and Production**
- **IRTF VTC Participants**
- **Questions / Guidance**

50th



Open Source Notes

- The Frontline Club has announced a panel discussion on WikiLeaks and the embassy cables as part of the "First Wednesday" event series. Speakers include:
 - The panel will take place on Wednesday, December 1st, 2010
 - WikiLeaks spokesperson, Kristinn Hrafnsson
 - James Ball, a data journalist, who has been working with WikiLeaks
 - Nicky Hager, author and investigative journalist

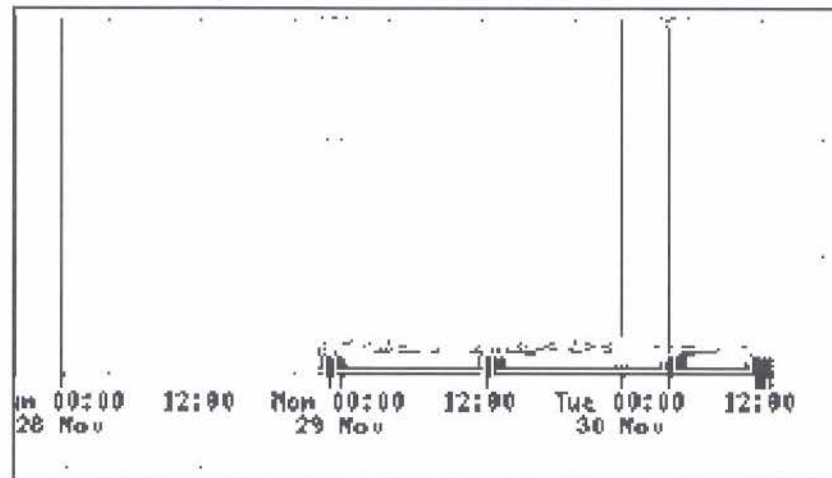
- New media partners?
 - "...negotiations are underway..."

th



WikiLeaks Under Attack Again

- WikiLeaks hit by another massive distributed denial of service hacker attack
 - While access to the site was slowed, WikiLeaks' decentralized nature makes shutdown more difficult than ever
 - According to WikiLeaks, today's distributed denial of service hacker attack exceeded 10 gigabits per second, much higher than Sunday's and highly complex
 - No significant impact to access from North America; WikiLeaks was inaccessible to Europe for much of the business day

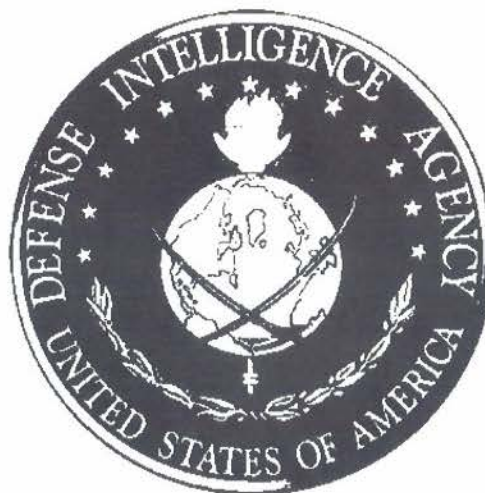




Media on Redactions

- The Guardian: Redactions have been made principally to protect individual sources where publication could put them or their families at personal risk. We have also considered questions of national security and military sensitivity, as well as legal considerations of defamation. Where the cables have proved simply embarrassing to western diplomats, we have usually considered them "fair game" and left those in.
- The New York Times: excludes, in its articles and in supplementary material, in print and online, information that would endanger confidential informants or compromise national security; redactions were shared with other news organizations and communicated to WikiLeaks
 - Explains redactions were provided to the Obama administration; some government redaction suggestions were taken, others not.
- Der Spiegel: efforts were made to consider national security and other issues.

50th



QUESTIONS / GUIDANCE

(b)(3):10 USC 424

50th

611

Pages 2-35 are withheld in full
and are not included.

~~SECRET//NOFORN~~

Information Review Task Force Information Brief (U)



"IRTF Slide Deck"
15 September 2010

Derived from: ~~Multiple Sources~~
Declassify on: ~~2000010~~

THIS BRIEF IS CLASSIFIED
~~SECRET//NOFORN~~

Current as of: 15 Sep 2010 (0800 hrs)

~~SECRET//NOFORN~~



QUESTIONS



(b)(3):10 USC 424



MISC BACKUP SLIDES

Information Review Task Force Information Brief (U)



IRTF Slide Deck 31 March 2011

This briefing is classified
~~SECRET//NOFORN~~

Derived from: ~~Multiple Sources~~
Declassify on: ~~20000001~~



CELEBRATING OUR LEGACY
FORGING OUR FUTURE

UNCLASSIFIED



QUESTIONS



(b)(3):10 USC 424



IRTF BACK UP SLIDES



WikiLeaks & Julian Assange



- Australian journalist, programmer and Internet activist
- “Australia’s most infamous former computer hacker”
-- Counter Punch Magazine
- Best known for his involvement with WikiLeaks
 - Sits on nine-member advisory board of WikiLeaks
 - Prominent media spokesman on its behalf
 - Claims to be an “unpaid volunteer”
- Ongoing internal strife with other staffers & volunteers

“I am the heart and soul of this organization, its founder, philosopher, spokesperson, original coder, organizer, financier and all the rest. If you have a problem with me, piss off.”

-- Julian Assange*

* As quoted in *Unpublished Iraq War Logs Trigger Internal WikiLeaks Revolt* by Kevin Poulsen and Kim Zetter, 27 Sep 2010, Wired.com

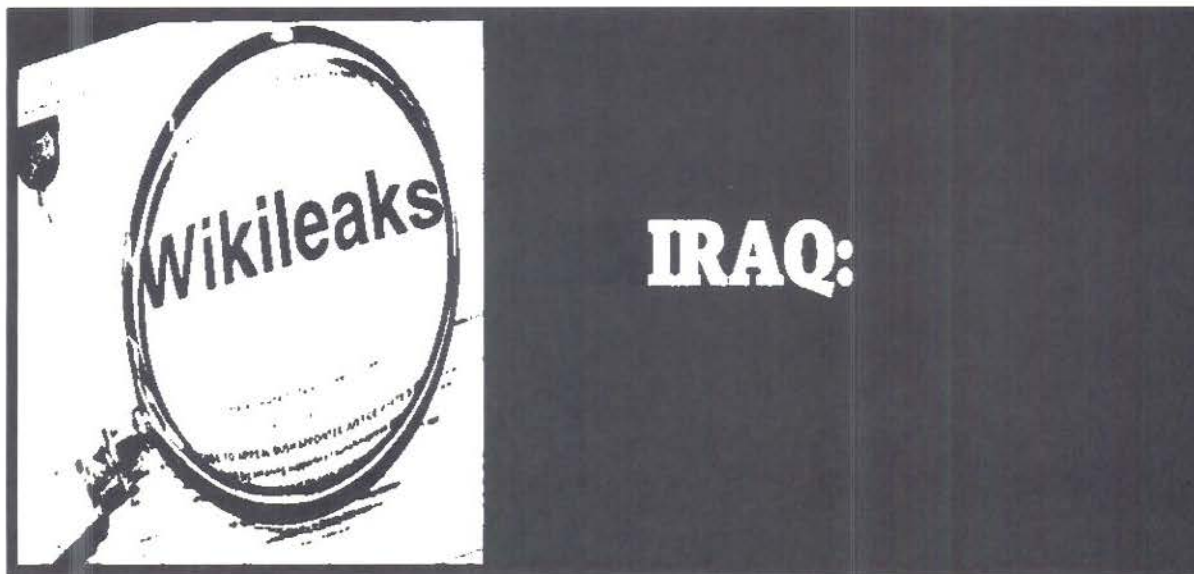
#627

The next 4 pages are withheld in full and are not included.

~~SECRET//NOFORN~~

INFORMATION REVIEW TASK FORCE SUMMARY REPORT - IRAQ DATASET (U)

12 January 2011



*Information Review Task Force
Defense Counterintelligence and Human Intelligence Center
Defense Intelligence Agency*

Derived From ~~████████████████████~~
Reason ~~████████~~
Declassify on: ~~██████████~~

~~SECRET//NOFORN~~

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

(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.

(b)(3):10 USC 424

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

The next 26 pages are withheld in full and are not included.

~~SECRET//NOFORN~~

Background (U)

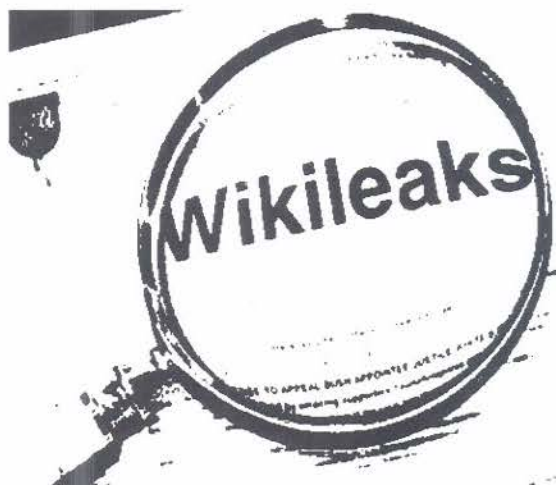
(U) On 22 October 2010 at 1700 Eastern Daylight Time the WikiLeaks organization released approximately 391,832 government records to the general public through its website; WikiLeaks.org (dedicated webpage at <http://wardiary.wikileaks.org>). Prior to the 22 October public posting of reports from CIDNE-I, 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)(1);(b)(3):10 USC 424;Sec. 1.4(c);Sec. 1.4(d)

(b)(3):10 USC 424;(b)(3) 50 USC 3024(f)

~~SECRET//NOFORN~~

APPENDIX A – GENERAL BACKGROUND INFORMATION ON WIKILEAKS (U)



(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.

"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.

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

⁶ (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.

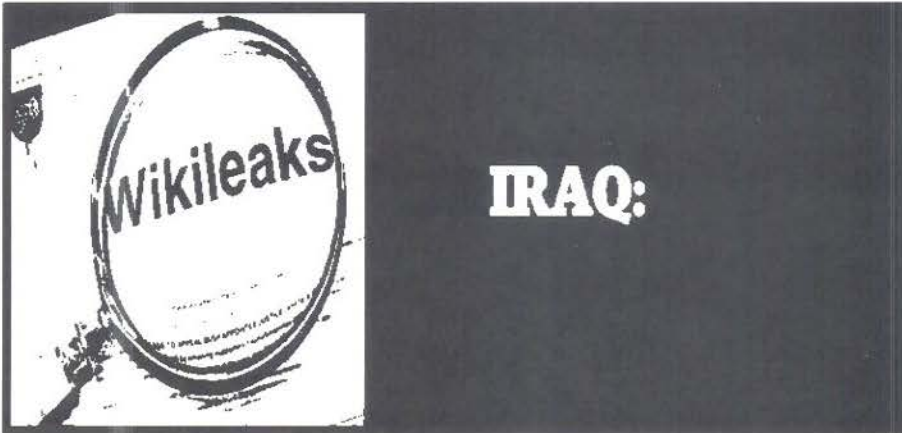
#628

The next 4 pages are withheld
in full and are not included.

~~SECRET//NOFORN~~

**INFORMATION REVIEW TASK FORCE
SUMMARY REPORT - IRAQ DATASET (U)**

30 December 2010



*Information Review Task Force
Defense Counterintelligence and Human Intelligence Center
Defense Intelligence Agency*

Derived From: ~~SECRET//NOFORN~~
Reason: ~~SECRET//NOFORN~~
Declassify on: ~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(b)(3):10 USC 424

(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.

(b)(3):10 USC 424

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

~~SECRET//NOFORN~~

The next 24 pages are withheld in full and are not included.

~~SECRET//NOFORN~~

Background (U)

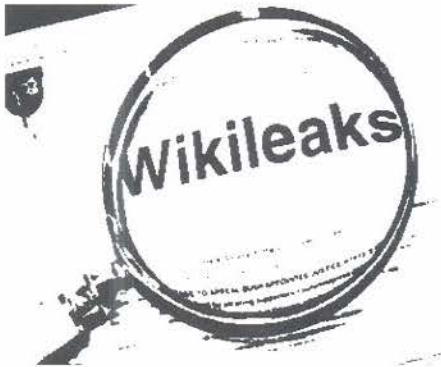
(U) On 22 October 2010 at 1700 Eastern Daylight Time the WikiLeaks organization released approximately 391,832 government records to the general public through its website: WikiLeaks.org (dedicated webpage at <http://wardiary.wikileaks.org>). Prior to the 22 October public posting of reports from CIDNE-I, 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)(1);(b)(3):10 USC 424;(b)(5);Sec. 1.4(c);Sec. 1.4(d)

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

~~SECRET//NOFORN~~

APPENDIX A – GENERAL BACKGROUND INFORMATION ON WIKILEAKS (U)



(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.

"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.

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

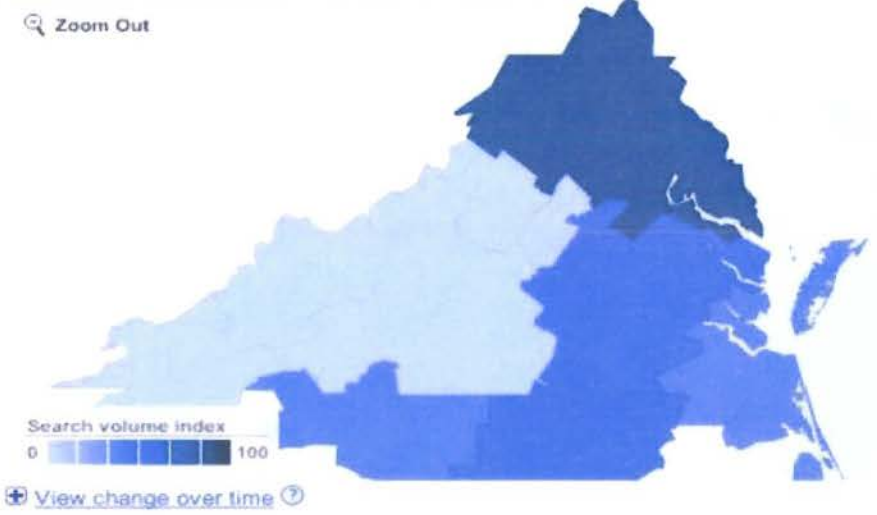
⁶ (U) TLS (Transport Layer Security) a cryptographic protocol that provides security for communication over networks such as the Internet. TLS protocol allows client/server applications to communicate across a network in a way to prevent eavesdropping and tampering. A prominent use of TLS is for securing World Web traffic by HTTP to form HTTPS



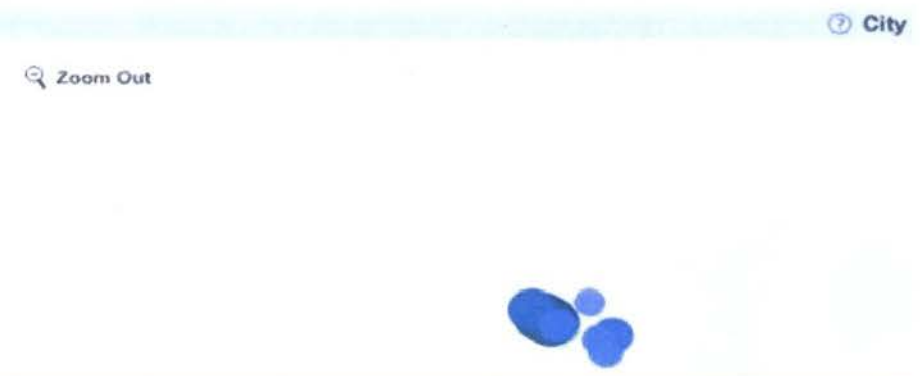
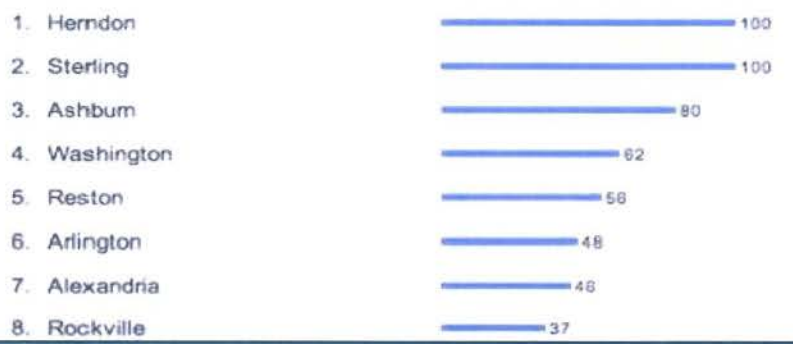
Pages 1 and 3-12 are withheld in full and are not included.

Information Review Task Force (IRTF)

Who's Googling WikiLeaks The Most?



Regional interest



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

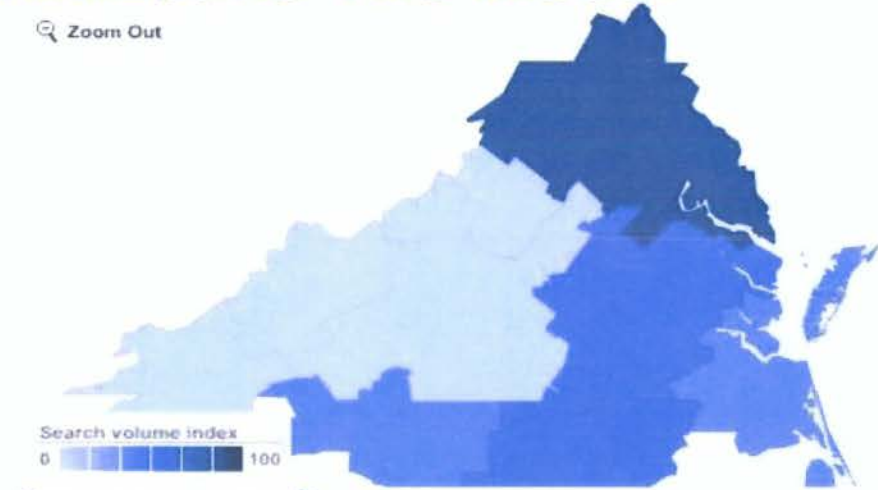


Information Review Task Force (IRTF)

Who's Googling WikiLeaks The Most?



Zoom Out



View change over time

Regional interest

City



Zoom Out



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



More Media Outlets Gain Access To Unreleased Cables

- (U) WikiLeaks-approved cable transfers
 - (U) **The Hindu** – Indian daily newspaper - received approx 5,100 cables from Assange
 - (U) *Publication leads to calls for PM resignation*
 - (U) **Taraf** – Turkish daily newspaper - received approx 11,000 cables from Assange
 - *Will reportedly publish all 11,000 cables*
- (U) Both outlets agreed to redact only when necessary and only to protect individuals from harm



(b)(1);Sec. 1.4(c);Sec. 1.4(g)

(b)(3):10 USC
424, (b)(6)

From:

To:

Cc:

Subject:

RE: Additional items

Date:

Friday, December 10, 2010 8:50:02 AM

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

CLASSIFICATION: ~~SECRET~~ ~~NOFORN~~

(b)(3):10 USC
424, (b)(5), (b)(6)

Thank you for the heads up. Assuming the docs

to arrange for a

by COB.

Goal is

(b)(6)

FYSA. If you have additional or alternate guidance, please let me know.

(b)(3):10 USC
424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

-----Original Message-----

(b)(3):10 USC
424, (b)(6)

From:

Sent: Friday, December 10, 2010 6:52 AM

To:

Cc:

Subject: FW: Additional items

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

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

CLASSIFICATION: ~~SECRET~~ ~~NOFORN~~

(b)(3):10 USC
424, (b)(5), (b)(6)

This will require some coordination with someone who exercises classification authority.

needs

of the attached documents to determine the following with respect to

Though it's not stated, I think it's understood that the suspense is asap. Thank you.

(b)(3):10 USC
424

(b)(3):10 USC
424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is

not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

-----Original Message-----

(b)(3):10 USC
424, (b)(6) From: [redacted]
Sent: Thursday, December 09, 2010 8:09 PM
To: [redacted]
Subject: FW: Additional items [redacted] (b)(3):10 USC
424, (b)(3):50
USC 3024(i)

(b)(3):50 USC
3024(i) CLASSIFICATION: ~~SECRET~~ [redacted] ~~NOFORN~~

FYI

-----Original Message-----

(b)(3):10 USC
424, (b)(3):50
USC 3024(i), (b)
(6) From: [redacted]
Sent: Thursday, December 09, 2010 8:07 PM
To: [redacted]
Subject: Additional items [redacted]

(b)(3):50 USC
3024(i) CLASSIFICATION: ~~SECRET~~ [redacted] ~~NOFORN~~

Thanks,

(b)(6) [redacted]

(b)(3):50 USC
3024(i) CLASSIFICATION: ~~SECRET~~ [redacted] ~~NOFORN~~

CLASSIFICATION: ~~SECRET~~ [redacted] ~~NOFORN~~

DERIVED FROM: ~~445~~
DECLASSIFY ON: ~~MD~~
DATE OF SOURCE: ~~20101210~~

(b)(3):50 USC
3024(i) CLASSIFICATION: ~~SECRET~~ [redacted] ~~NOFORN~~

DERIVED FROM: ~~446~~
DECLASSIFY ON: ~~MD~~
DATE OF SOURCE: ~~20101210~~

(b)(3):50 USC
3024(i) CLASSIFICATION: ~~SECRET~~ [redacted] ~~NOFORN~~

The next page is withheld in full and is not included.

(b)(3):10 USC 424,
(b)(3):50 USC
3024(i),(b)(6)

From: [redacted]
To: [redacted]
Subject: RE: Comparison of compromised [redacted]
Date: Friday, November 19, 2010 10:12:59 AM

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(3):10 USC
424,(b)(5),(b)(6)

[redacted]

(b)(3):10 USC
424,(b)(3):50
USC 3024(i),(b)
(6)

From: [redacted]
Sent: Friday, November 19, 2010 7:07 AM
To: [redacted]
Subject: RE: Comparison of compromised/assessments

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(3):10 USC
424,(b)(6)

[redacted] Perhaps I should know but I don't. Meanwhile, I'll send this to our [redacted] for a quick check before giving you my final coord. I also sent an earlier comment but that was before I knew this was also intended for [redacted] I should be able to accomplish final review by 0900. Trust that will work. v/r, [redacted]

(b)(3):10 USC
424

(b)(3):10 USC
424,(b)(6)

(b)(3):10 USC
424

[redacted]

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

(b)(3):10 USC 424,
(b)(3):50 USC
3024(i),(b)(6)

From: [redacted]
Sent: Thursday, November 18, 2010 5:31 PM
To: [redacted]
Subject: Comparison of compromised/ [redacted]

CLASSIFICATION: ~~SECRET//NOFORN~~

(b)(3):10 USC
424,(b)(6)

[redacted] Please review this email before I send it to [redacted] and provide any comments back to me. [redacted]

(b)(3):10 USC
424,(b)(6)

INFO MEMO

8-10-0221/IRTF

27 September 2010

FOR: DIRECTOR, DEFENSE INTELLIGENCE AGENCY

THROUGH: Director, Defense Counterintelligence and HUMINT Center

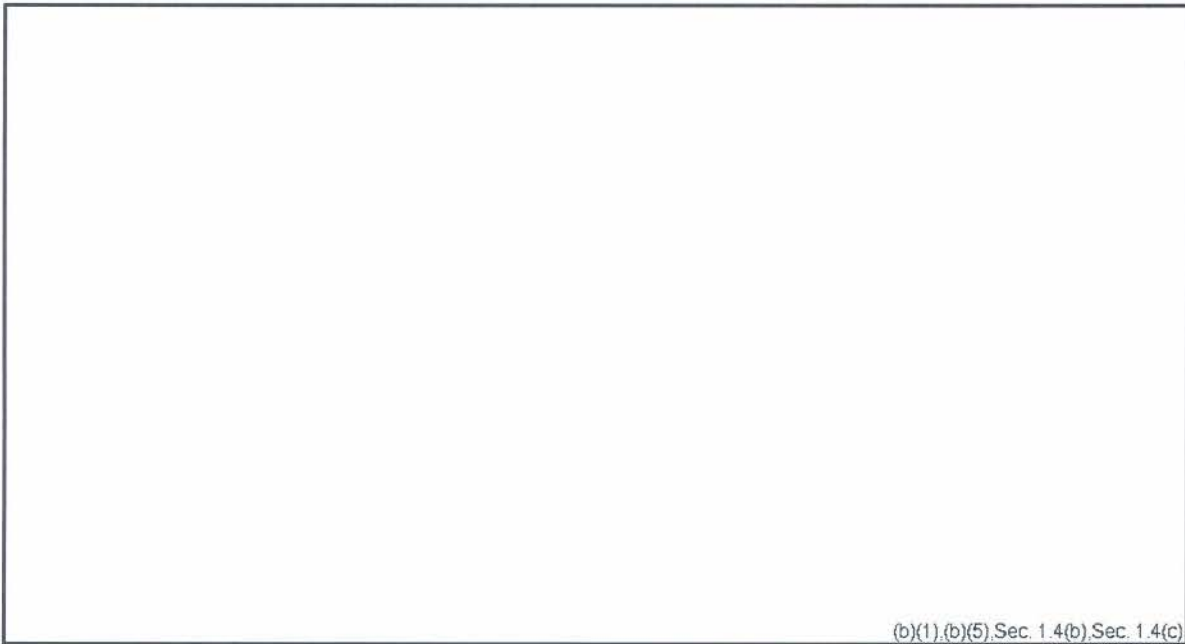
FROM: Chief, Information Review Task Force

(b)(1),(b)(3), 10 USC 424,(b)(3); 50 USC 3024(i),(b)(5),(b)(6), Sec. 1.4(b), Sec. 1.4(c)

SUBJECT:

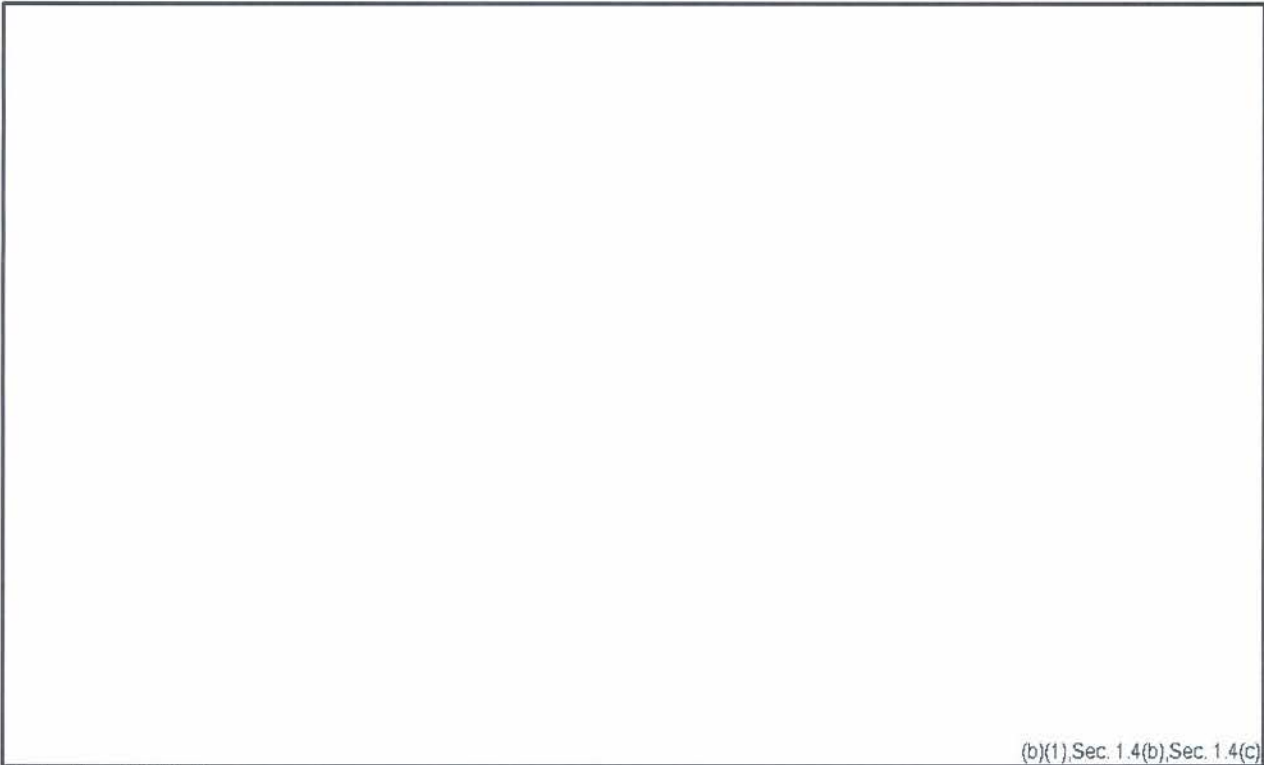
[Redacted content]

Derived from: [Redacted]
Declassify on: [Redacted]



(b)(1),(b)(5),Sec. 1.4(b),Sec. 1.4(c)

(U) Reporting Background



(b)(1),Sec. 1.4(b),Sec. 1.4(c)

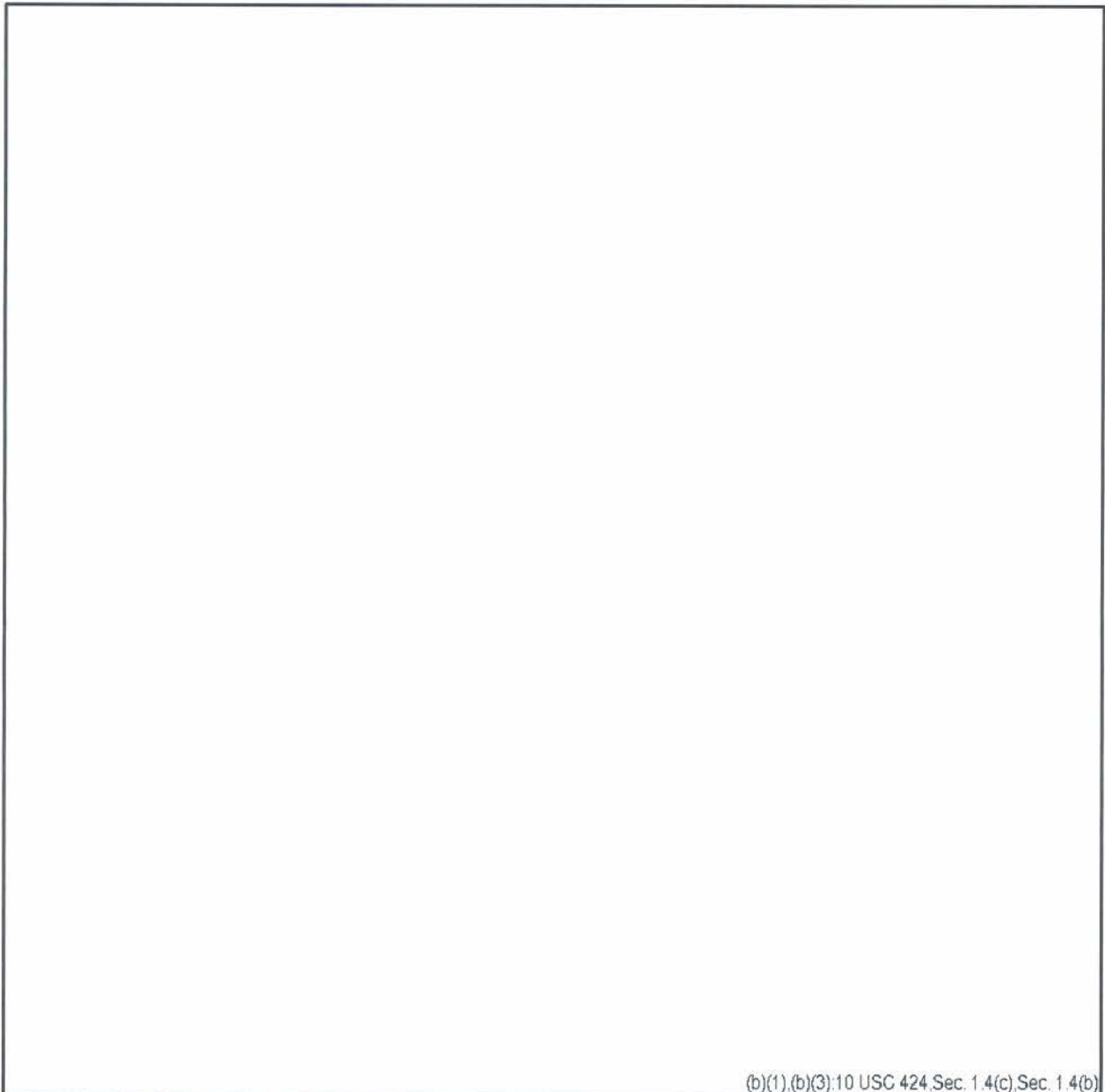
Derived from: ~~Multiple Sources~~
Declassify on: ~~OSI~~

The next page is withheld in full and is not included.



(b)(1),Sec. 1.4(c),Sec. 1.4(b)

(U) Data Characterization:



(b)(1),(b)(3);10 USC 424,Sec. 1.4(c),Sec. 1.4(b)

Derived from: ~~██████████~~
Declassify on: ~~██████████~~

(b)(1),(b)(3):10 USC 424,Sec. 1.4(b),Sec. 1.4(c)

Prepared by:
Reviewed by:

[Redacted]

(b)(3):10 USC 424,(b)(6)

Derived from: ~~multiple sources~~
Declassify on: ~~FOUO~~

~~XXXXXXXXXX~~

INFO MEMO

10-0238/IRTF

15 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

[Redacted content]

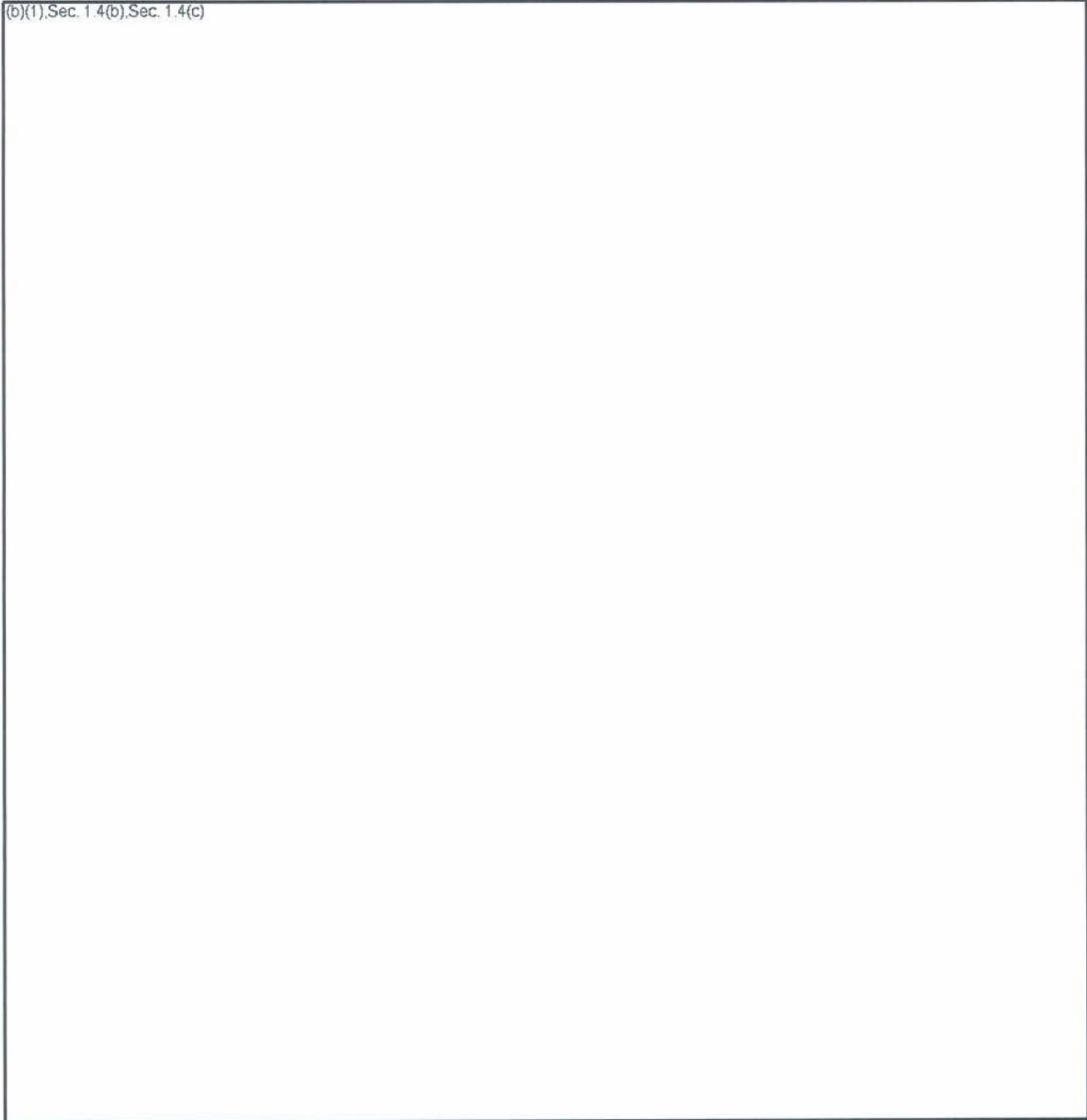
(b)(1),(b)(3) 10 USC 424 (b)(3) 50 USC 3024(i),(b)(5),(b)(6) Sec. 1.4(b) Sec. 1.4(c)

Derived from: ~~XXXXXXXXXX~~
Declassify on: ~~XXXX~~

~~XXXXXXXXXX~~

(U) Data Characterization

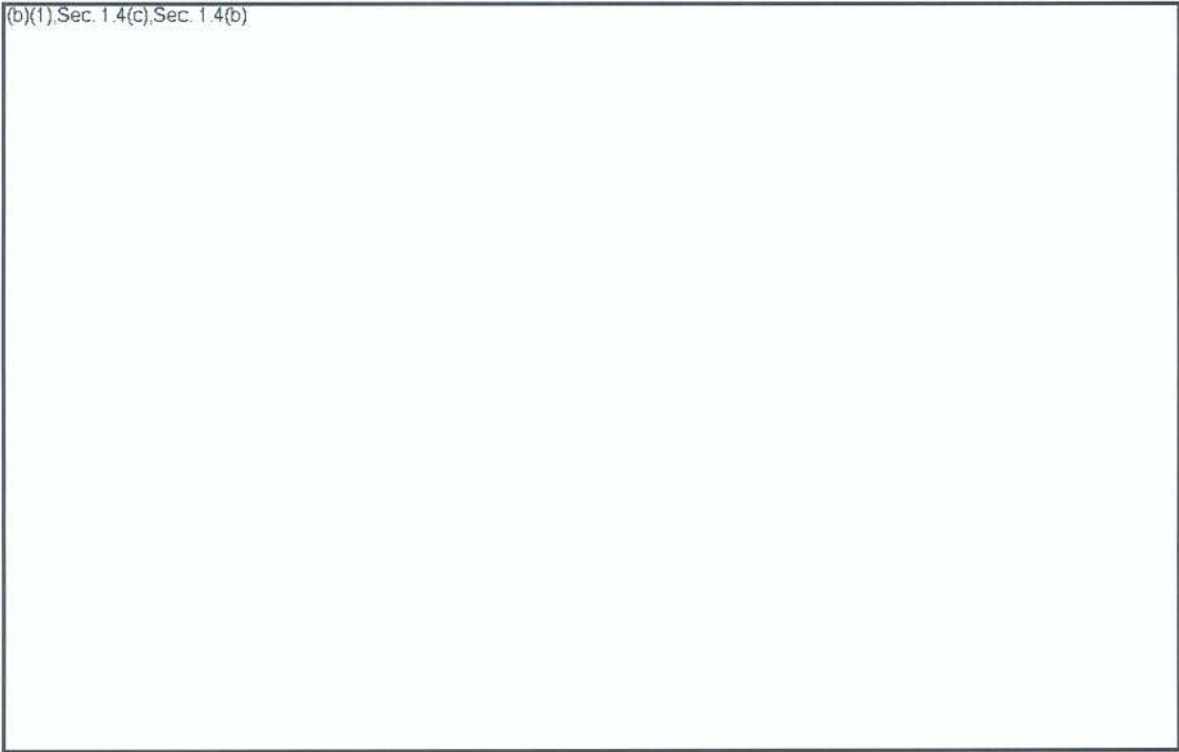
(b)(1), Sec. 1.4(b), Sec. 1.4(c)



Derived from: [REDACTED]
Declassify on: [REDACTED]

The next page is withheld in full and is not included.

(b)(1),Sec. 1.4(c),Sec. 1.4(b)



(U) Mitigating Considerations

(b)(1),(b)(5),Sec. 1.4(c),Sec. 1.4(b)



Derived from: ~~██████████~~
Declassify on: ~~██████~~

Prepared by:
Reviewed by:

(b)(3);10 USC 424,(b)(6)

Derived from: ~~Multiple sources~~
Declassify on: ~~25 Y1~~

INFO MEMO

10-0239/IRTF

7 October 2010

FOR: Director, Defense Counterintelligence and HUMINT Center

FROM: Chief, Information Review Task Force

SUBJECT:

(b)(1),(b)(3):10 USC 424,(b)(3):50 USC 3024(i),(b)(5),(b)(6),Sec. 1.4(b),Sec. 1.4(c)

Reviewed by:

Derived from: ~~XXXXXXXXXX~~
Declassify on: ~~XXXXXX~~

From: (b)(3):10 USC 424;(b)(6)
Subject: RE: DoDGC Brief to AG/DAG Version 15 (U)
Date: Monday, January 31, 2011 2:10:58 PM

CLASSIFICATION: ~~SECRET//NOFORN~~

Ah, yes. Leads me to recall (b)(6);(b)(3):10 USC 424 comment about lawyers and editing ...

(b)(3):10 USC 424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From: (b)(6);(b)(3):10 USC 424
Sent: Monday, January 31, 2011 2:09 PM
To:
Subject: RE: DoDGC Brief to AG/DAG Version 15 (U)

CLASSIFICATION: ~~SECRET//NOFORN~~

Of course, [redacted] will have some recommended edits...that brings us to version 16...my bet is V20 by the time it is actually briefed...

(b)(3):10 USC 424;(b)(6)

(b)(3):10 USC 424

From: [redacted]
Sent: Monday, January 31, 2011 1:52 PM
To: [redacted]
Cc: (b)(6);(b)(3):10 USC 424
Subject: RE: DoDGC Brief to AG/DAG Version 15 (U)

CLASSIFICATION: ~~SECRET//NOFORN~~

looks fine. Thank you.

(b)(6);(b)(3):10 USC 424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From: (b)(6)

Sent: Monday, January 31, 2011 1:38 PM

(b)(3):10 USC 424;(b)(6)

Subject: RE: DoDGC Brief to AG/DAG Version 15 (U)

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

Version 15 is born. Please give this a quick look and let me know if anything is amiss. Many thanks (b)(6)

From: (b)(3):10 USC 424

Sent: Monday, January 31, 2011 1:08 PM

(b)(3):10 USC 424;(b)(6)

Subject: RE: DoDGC Brief to AG/DAG Version 12 (U)

CLASSIFICATION: ~~TOP SECRET~~ (b)(3):50 USC 3024(i) ~~NOFORN~~

this incorporates changes we discussed (b)(6)

(b)(6);(b)(3):10 USC 424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From: (b)(6)

Sent: Monday, January 31, 2011 11:55 AM

(b)(3):10 USC 424;(b)(6)

Subject: RE: DoDGC Brief to AG/DAG Version 12 (U)

Importance: High

Classification: ~~SECRET~~

The mtg with the GC just got moved up to 1400 so please send whatever you have in the way of updates soonest. Thanks!

(b)(3):10 USC 424;(b)(6)

Subject: RE: DoDGC Brief to AG/DAG Version 12 (U)

Classification: ~~SECRET~~

(b)(5);(b)(6);(b)(3):10 USC 424

We are scheduled to meet at 1600 with the GC on WikiLeaks.

Many thanks,

From: (b)(3):10 USC 424

Sent: Monday, January 31, 2011 6:43 AM

(b)(3):10 USC 424;(b)(6)

Subject: RE: DoDGC Brief to AG/DAG Version 12 (U)

CLASSIFICATION: ~~SECRET~~

Thank you. I'll be in touch this morning to discuss your recommended changes.

(b)(6);(b)(3):10 USC 424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

From: (b)(6) **Sent:**

Friday, January 28, 2011 4:24 PM **To:**

(b)(3):10 USC 424;(b)(6)

Subject: RE: DoDGC Brief to AG/DAG Version 12 (U)

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

(b)(5);(b)(6);(b)(3):10 USC 424

(b)(5),(b)(6)

(b)(3):10 USC 424;(b)(6)

Subject: DoDGC Brief to AG/DAG Version 12

CLASSIFICATION: ~~TOP SECRET~~ (b)(3):50 USC 3024(i) ~~NOFORN~~

Attached is an updated slide deck that includes ref to

(b)(5),(b)(6);(b)(3):10 USC 424

(b)(3):10 USC 424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~25X1~~
DATE OF SOURCE: ~~20110128~~

CLASSIFICATION: ~~TOP SECRET~~ (b)(3):50 USC 3024 ~~NOFORN~~

This may contain information exempt from mandatory disclosure under the Freedom of Information Act (FOIA).

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~MR~~
DATE OF SOURCE: ~~20110121~~

CLASSIFICATION: ~~SECRET~~

DERIVED FROM: ~~Multiple Sources~~
DECLASSIFY ON: ~~31 Jan 2021~~

DERIVED FROM: ~~Multiple Sources~~
DECLASSIFY ON: ~~31 Jan 2021~~

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~25X1~~
DATE OF SOURCE: ~~20110131~~

CLASSIFICATION: ~~TOP SECRET~~ (b)(3);50 USC 3024(i) ~~NOFORN~~

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~MR~~
DATE OF SOURCE: ~~20110131~~

CLASSIFICATION: ~~SECRET//NOFORN~~

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~MR~~
DATE OF SOURCE: ~~20110131~~

CLASSIFICATION: ~~SECRET//NOFORN~~

DERIVED FROM: ~~MS~~
DECLASSIFY ON: ~~MR~~
DATE OF SOURCE: ~~20110131~~

CLASSIFICATION: ~~SECRET//NOFORN~~

#597

From: (b)(6);(b)(3):10 USC 424;(b)(3):50 USC 3024(i)
To:
Subject:
Date: Saturday, December 18, 2010 4:35:18 PM

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

Interesting reading

From: (b)(6);(b)(3):10 USC 424;(b)(3):50 USC 3024(i)
Sent: Friday, December 17, 2010 8:15 AM
To:
Cc:
Subject:

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

(b)(3):10 USC 424;(b)(6)

An interesting article follows from the Netherlands on comments and operations within WikiLeaks currently.

Vr,

(b)(3):10 USC 424;(b)(6)

WikiLeaks Staff Cited on Infighting, Internal Operation of Whistleblower Site (U//~~FOUO~~)

EUP20101216024001 Rotterdam NRC Handelsblad Online in Dutch 15 Dec 10 (U//~~FOUO~~)

[Report by Leonie van Nierop: "The WikiLeaks Youngsters Are Idealistic, They Want To Manipulate Systems" (U//~~FOUO~~)

[OSC Translated Text]

Reykjavik, 15 December -- A relatively large number of former employees of the core group running WikiLeaks live in Reykjavik. They are only too pleased to talk about the whistleblowing website. "I don't like to play James Bond."

At the Kormaks og Skjaldar beer house in the capital Reykjavik there is a lot of talk about WikiLeaks. The talk is mainly about the criminal charges against the Australian

founder Julian Assange for sex offenses. To be precise ; About the question of whether the Swedish women involved are hysterical and jealous lesbian feminists or are under the influence of the CIA.

There are also criticisms of WikiLeaks. Because the foundation that supports the soldier Bradley who is suspected of making the leaks is said not to have received a single cent of the money that WikiLeaks collected for him. Because evil tongues claim that the media have to pay large sums of money to gain access to the quarter of a million US diplomatic cables, just a fraction of which are published. Because chaos has allegedly broken out internally following Assange's arrest last week in London. Because the organization that advocates openness itself remains a mystery.

Such malicious talk is being spread not least of all by people who have left WikiLeaks in recent years. Although on the Internet they say that they have no comment to make about Assange or WikiLeaks, they are only too willing to talk, and openly. Also the Icelanders, which make up a relatively large proportion of the small core that runs the whistleblowing site, are easier to reach than is generally believed. Three former members of the team and three current members spoke in Reykjavik about who they are and how the organization operates. To protect their safety, names have been omitted.

The unverifiable "facts" they provide: The permanent inner core consists of -- in addition to Assange and at least three Icelanders -- a Brit and an Australian university employee. The only two or three hackers who are familiar with the entire web infrastructure take great care to remain anonymous. And although the organization runs largely on trust, there is a high rate of turnover about the associates. Of the nine people who worked for WikiLeaks in March at least five have left.

Internet activist Smari McCarthy (26) is one of the few former employees who left in the last year without having a row. He still has contacts with Wikileaks, has been able to see all the cables and fully supports their circulation. Other aspects he is less enthusiastic about. Such as having to constantly change telephone number for fear of the intelligence services. "Some get a kick out of it but I don't like playing at James Bond."

He followed the traditional career path of a hacker. As a youngster -- the kind of youngster who finds pleasure in taking a toaster apart -- he was given a computer on his twelfth birthday. He soon discovered he could improve it and discovered similar souls in chatrooms with whom he talked technicalities. McCarthy: "It was only later that I heard about the bigger problems in the world, also offline. We slowly became politicized." In 2001 he attended his first hackers congress in Amsterdam, about self-determination on the web. Nine years later he helped Assange produce the video showing US soldiers shooting dead civilians and journalists in Baghdad.

McCarthy describes himself as "a hacker in the positive sense of the word." A hacker is not somebody who breaks into computers to steal, but somebody who is interested in "manipulating the system." And precisely this interest in a higher mission, absolute freedom of information, is something that McCarthy finds is now lacking on

WikiLeaks. "They seem to be interested in quick scoops not in changing the system."

The legal case in Sweden also bothers him. "Through his insinuations that the charges are politically motivated, Assange has become a martyr. But that is playing into the hands of the United States. All the attention focusing on him is not focusing on the diplomatic cables."

There is not the romantic image of Assange as the vilified man prepared to take on the rest of the world. He is also seen as a paranoid and self-obsessed autocrat. Former employees say that all decisions had to pass through him, which is difficult when somebody is on the run or in jail. That is possibly why the German foundation Wau Holland, which manages a part of the funds, has not yet transferred any money to support Bradley Manning.

Since Assange's arrest Kristinn Hrafnsson has been the WikiLeaks spokesperson out of London. The Icelandic investigative journalist travelled to Iraq at the beginning of the year to produce the video. Last weekend he was briefly in Reykjavik. He denies that the media pay for the information. He attributes the rumor to the "excessive attacks" on WikiLeaks. But he says little else. He will not say what is contained in the locked file that WikiLeaks is advising everybody to download in the event of Wikileaks going under, or at what point the key to unlock it will be released. "We are still a long way from that moment. And we hope that it never comes to that."

According to WikiLeaks there are still hundreds of volunteers for its cause. For example 25-year-old Herbert Snorrason. When, in the summer of 2009, Wikileaks published an explosive piece about an Icelandic bank, he asked WikiLeaks in a chatroom for some technical details. He continued to hang out there. When a year later the chatroom was flooded out, following the release of around 90,000 documents about the war in Afghanistan, Snorrason himself started to moderate and to answer questions. WikiLeaks was happy to let him continue. Since then he has helped with about 40 other volunteers to remove personnel details from 15,000 of these documents.

Snorrason's activities for WikiLeaks ended when in a chatroom conversation with Assange he defended Daniel Domscheit-Berg (known at the time as Daniel Schmitt). This 32-year-old German left in September after conflict with Assange, who Domscheit-Berg claimed was dictatorial in his behavior and only interested in dramatic revelations. When Snorrason complained, Assange wrote "piss off." And that was it for Snorrason.

His revenge is sweet. Soon he will be launching a rival whistleblowing website with Domscheit-Berg: [OpenLeaks](#). The founders have high hopes for it. WikiLeaks wishes it all the best. Because on one thing friend and foe are agreed: This information revolution is unstoppable.

[Description of Source: Rotterdam NRC Handelsblad Online in Dutch -- Website of prestigious left-of-center newspaper; URL: <http://www.nrc.nl>]

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

The next page is withheld in full and is not included.

(b)(3):10 USC 424,(b)(6)

From: [Redacted]
To: [Redacted]
Subject: FW: Privacy Act Analysis
Date: Monday, August 09, 2010 6:41:00 AM

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

FYSA

(b)(3):10 USC 424

[Redacted]

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

(b)(3):10 USC 424,(b)(6)

From: [Redacted]
Sent: Friday, August 06, 2010 12:19 PM
To: [Redacted]
Cc: [Redacted]
Subject: RE: Privacy Act Analysis

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

I'm going to call DoD's Privacy Officer now and advise him of the situation. I'll let you know what they say.

(b)(3):10 USC 424

[Redacted]

From: [Redacted]
Sent: Friday, August 06, 2010 11:23 AM
To: [Redacted]
Cc: [Redacted]
Subject: Privacy Act Analysis

(b)(3):10 USC 424

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

(b)(3):10 USC 424

[Redacted]

(b)(3):10 USC 424,(b)(5),(b)(6)

Thank you for your input regarding this issue. [Redacted]

V/r,
[Redacted]

(b)(3)10 USC
424

This email, including any attachments, is intended for the use of the individual or entity to which it is addressed. It may contain ATTORNEY WORK PRODUCT information that is privileged, confidential, or otherwise protected by law. This email may be ATTORNEY-CLIENT PRIVILEGED/FOIA EXEMPT. If the reader of this email is not the intended recipient or the employee or agent responsible for delivering the email to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this email or its contents is strictly prohibited. If you have received this email in error, please notify me immediately by replying to this message and destroy all copies of this email.

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

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~

CLASSIFICATION: UNCLASSIFIED//~~FOUO~~



~~SECRET//NOFORN~~

DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-5100



INFO MEMO

~~S~~-11-0362/CE

FEB 24 2011

FOR: SECRETARY OF DEFENSE

FROM: Ronald L. Burgess, Jr., Lieutenant General, USA, Director, Defense Intelligence Agency *RLB*

SUBJECT: (U) Information Review Task Force (IRTF) – February 22, 2011 Update

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

[Redacted content]

Derived from ~~████████████████████~~
Declassify on ~~██████████~~

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~
DEFENSE INTELLIGENCE AGENCY
WASHINGTON, D.C. 20340-5100



INFO MEMO

11-0415/CE

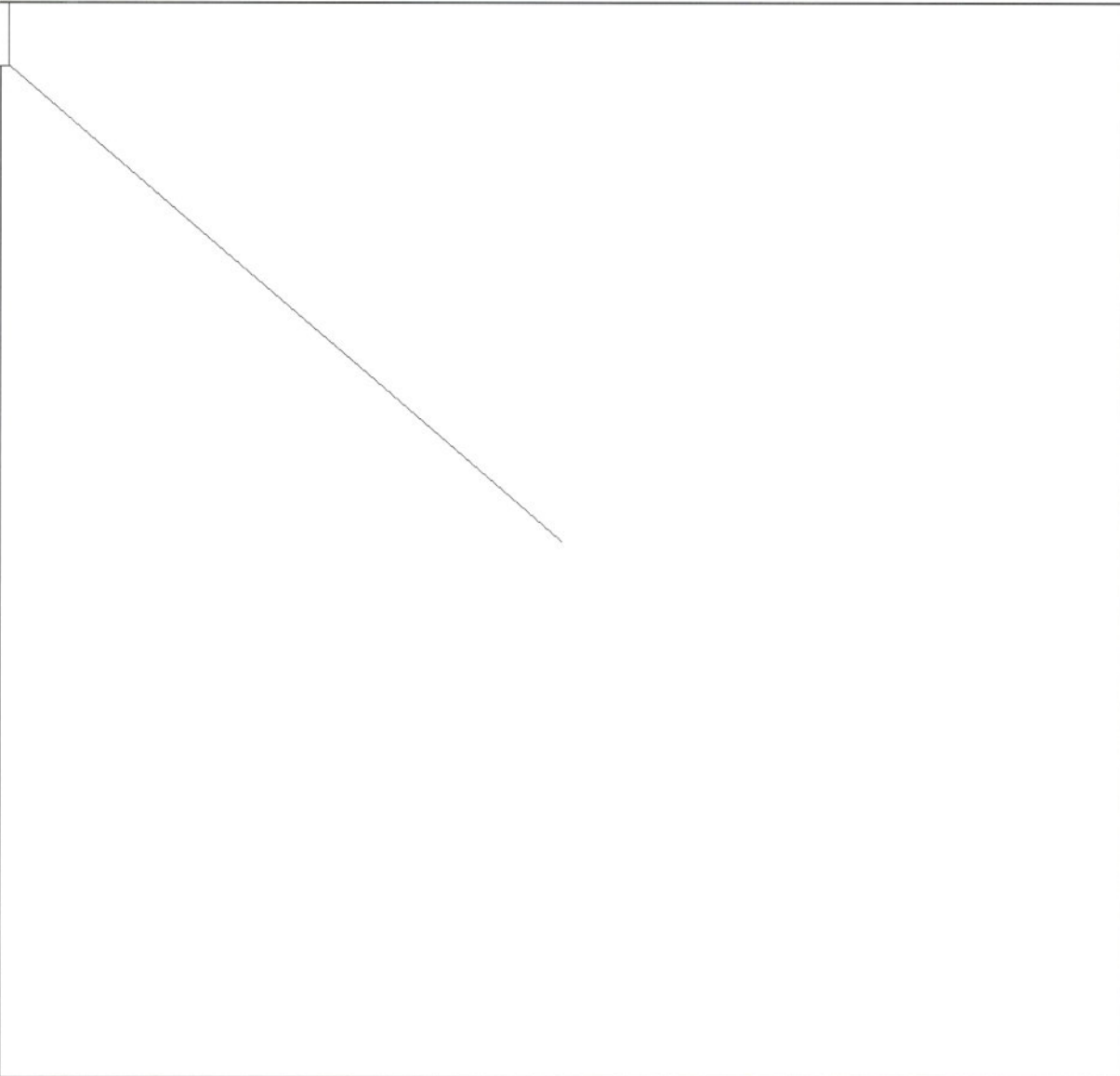
MAR 01 2011

FOR: SECRETARY OF DEFENSE

FROM:  Ronald L. Burgess, Jr., Lieutenant General, USA, Director, Defense Intelligence Agency

SUBJECT: (U) Information Review Task Force (IRTF) – February 28, 2011 Update

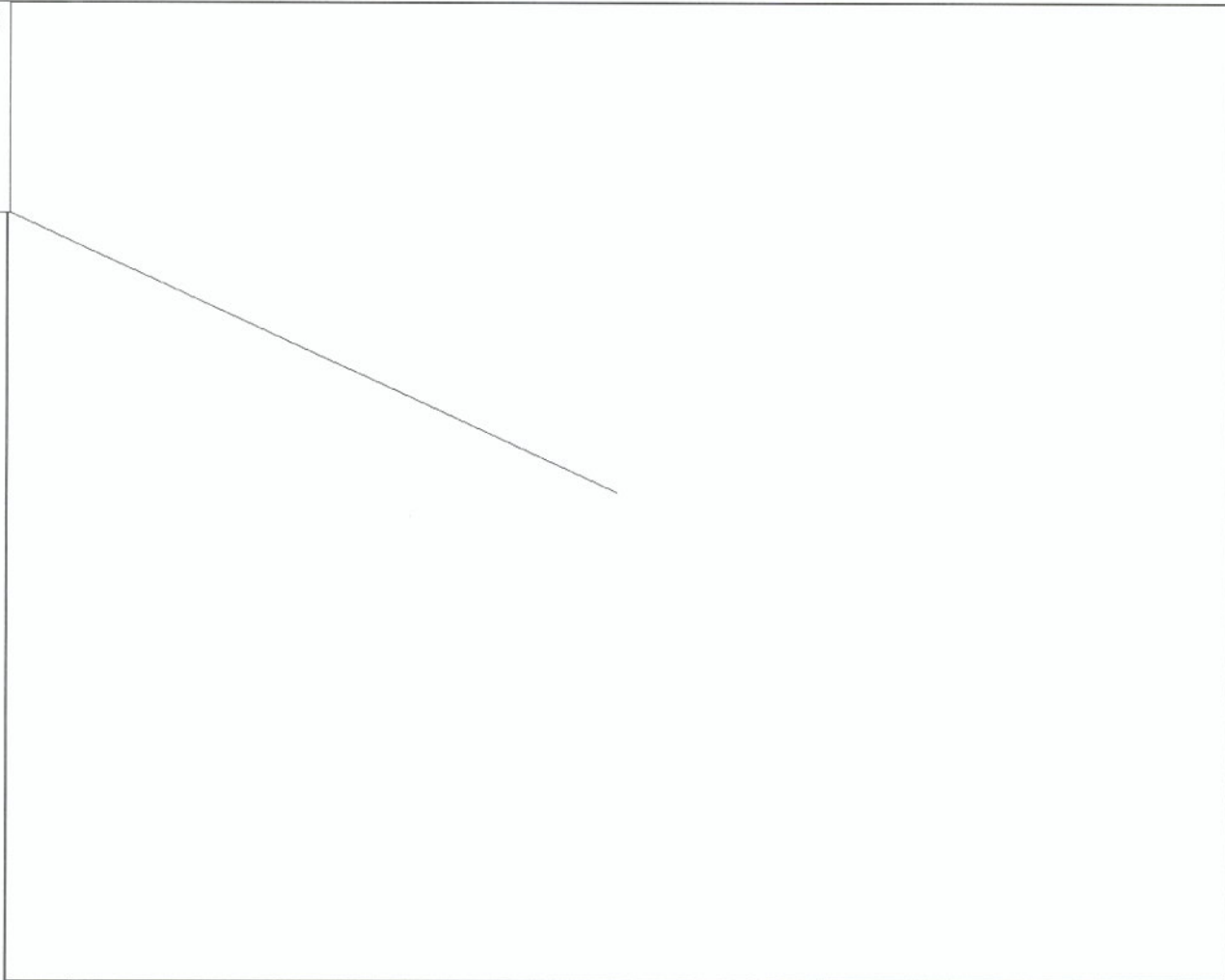
(b)(1)1.4(c);
(b)(1)1.4(d)



Derived from: ~~████████████████████~~
Declassify on: ~~██████████~~

~~SECRET//NOFORN~~

(b)(5);(b)(6);
(b)(1)1.4(c);
(b)(1)1.4(d)



(U) Attorneys for Julian Assange have yet to file an appeal to the February 24, 2011 initial ruling that he should be extradited from the United Kingdom to Sweden.

