I wrote this statement in confinement, so... The following facts are provided in support of the providence inquiry for my court martial, United States v. Pfc. Bradley E. Manning.

I am a 25-year old Private First Class in the United States Army currently assigned to Headquarters and Headquarters Company, HHC, US Army Garrison-USAG, Joint Base Myer, Henderson Hall, Fort Meyer, Virginia. Prior to this assignment, I was assigned to HHC, 2nd Brigade Combat Team, 10th Mountain Division at Fort Drum, New York. My primary military occupational specialty or PMOS is 35 fox-trot: intelligence analyst. I entered active duty status on 2 October 2007. I enlisted with the hope of obtaining both real-world experience and earning benefits under the GI Bill for college opportunities.

Facts Regarding My Position as an Intelligence Analyst

In order to enlist in the army, I took the Standard Armed Services Aptitude Battery or ASAB. My score [unavailable] was high enough for me to qualify for any enlisted MOS position. My recruiter informed me that I should select an MOS that complimented my interests outside the military. In response, I told him I was interested in geopolitical matters and information technology. He suggested I consider becoming an intelligence analyst. After researching the intelligence analyst position, I agreed this would be a good fit for me. In particular, I enjoyed the fact that an analyst could use information derived from a variety of sources to create work products that informed the command of its available choices for determining the best course of action or COAs. Although the MOS required working knowledge of computers, it primarily required me to consider how raw information can be combined with other available intelligence sources in order to create products that assisted the command in its situational awareness or SA.

I assessed that my natural interest in geopolitical affairs and my computer skills would make me an excellent intelligence analyst. After enlisting I reported to the Fort Meade military entrance processing station on 1 October 2007. I then traveled to-and reported at-Fort Leonard Wood, Missouri, on 2 October 2007 to begin basic combat training or BCT.

Once at Fort Leonard Wood, I quickly realized that I was neither physically nor mentally prepared for the requirements of basic training. My BCT experience lasted six months instead of the normal 10 weeks. Due to medical issues, I was placed on a hold status. A physical examination indicated that I sustained injuries to my right shoulder and left foot. Due to those injuries I was unable to continue basic. During medical hold, I was informed that I may be out processed from the Army, however, I resisted being chaptered out because I felt that I could overcome my medical issues and continue to serve. On 20 January 2008, I returned to basic combat training. This time I was better prepared, and I completed training on 2 April 2008.

Then I reported for the MOS specific Advances Individual Training or AIT on 7 April 2008. AIT was an enjoyable experience for me. Unlike basic training, where I felt different from the other soldiers, I fit in well. I preferred the mental challenges of reviewing a large amount of information from various sources and trying to create useful or actionable products. I especially enjoyed the practice of analysis through the use of computer applications and methods that I was familiar with.

I graduated from AIT on 16 August 2008 and reported to my first duty station, Fort Drum, NY, on 28 August 2008. As an analyst, Significant Activities or SigActs were a frequent source of information for me to use in creating work products. I started working extensively with SigActs early after my arrival at Fort Drum. My computer background allowed me to

use tools, such as the Distributed Common Ground System-Army or D6-A computers to create polished work products for the 2nd Brigade Combat Team chain of command. The non-commissioned officer in charge, or NCOIC, of the S2 section, then Master Sergeant David P. Adkins recognized my skills and potential and tasked me to work on a tool abandoned by a previously assigned analyst-the incident tracker. The incident tracker was viewed as a back-up to the Combined Information Data Network Exchange or CIDNE and as a unit historical reference.

In the months preceding my upcoming deployment, I worked on creating a new version of the incident tracker and used SigActs to populate it. The SigActs I used were from Afghanistan because at the time our unit was scheduled to deploy to the Logar and Wardak Provinces of Afghanistan. Later my unit was reassigned to deploy to Eastern Baghdad, Iraq. At that point, I removed the Afghanistan SigActs and switched to Iraq SigActs.

As and analyst I viewed the SigActs as historical data. I believed this view is shared by other all-source analysts as well. SigActs giae a first look impression of a specific or isolated event. This event can be an improvised explosive device attack or IED, small-arms fire engagement or SAF engagement with a hostile force, or any other event a specific unit documented and recorded in real time. In my perspective, the information contained within a single SigAct or group of SigActs is not very sensitive. The events encapsulated within most SigActs involve either enemy engagements or casualties. Most of this information is publicly reported by the public affairs office or PAO, embedded media pools, or host-nation-HN-media.

As I started working with SigActs, I felt they were similar to a daily journal or log that a person may keep. They capture what happens on a particular day in time. They are created immediately after the event, and

are potentially updated over a period of hours until final version is published on the CIDNE [Combined Information Data Network Exchange]. Each unit has its own Standard Operating Procedure or SOP for reporting recording SigActs. The SOP may differ between reporting in a particular deployment and reporting in garrison. In a garrison a SigAct normally involves personnel issues such as driving under the influence or DUI incidents or an automobile accident involving the death or serious injury of a soldier. The reports starts at the company level and goes up to the battalion, brigade, and even up to the division level.

In a deployed environment a unit may observe or participate in an event and a platoon leader or platoon sergeant may report the event as a SigAct to the company headquarters and the radio transmission operator or RTO. The commander or RTO will then forward the report to the battalion battle captain or battle non-commissioned officer or NCO. Once the battalion battle captain or battle NCO receives the report they will either 1) notify the battalion operations officer or S3, 2) conduct an action, such as launching a quick reaction force, or 3) record the event and report and further report it up the chain of command to the brigade.

The reporting of each event is done by radio or over the Secret Internet Protocol Router Network or SIPRNet, normally by an assigned soldier, usually junior enlisted E-4 and below. Once the SigAct is recorded, the SigAct is further sent up the chain of command. At each level, additional information can either be added or corrected as needed. Normally within 24 to 48 hours, the updating and reporting of a particular SigAct is complete. Eventually all reports and SigActs go through the chain of command from brigade to division and division to corp. At corp level the SigAct is finalized and [cataloged?].

The CIDNE system contains a database that is used by thousands of

Department of Defenseâ€"DoD-personel including soldiers, civilians, and contractors. It was the United States Central Command or CENTCOM reporting tool for operational reporting in Iraq and Afghanistan. Two separate but similar databases were maintained for each theater: CIDNE-I for Iraq and CIDNE-A for Afghanistan. Each database encompasses over a hundred types of reports and other historical information for access. They contain millions of vetted and finalized directories including operational intelligence reporting.

CIDNE was created to collect and analyze battle data to provide daily operational and Intelligence Community (IC) reporting relevant to a commander s daily decision making process. The CIDNE-I and CIDNE-A databases contain reporting and analysis fields for multiple disciplines including Human Intelligence or HUMINT reports, Psychological Operations or PSYOP reports, Engagement reports, counter improvised explosive device or CIED reports, SigAct reports, targeting reports, social and cultural reports, civil affairs reports, and human terrain reports.

As an intelligence analyst, I had unlimited access to the CIDNE-I and CIDNE-A databases and the information contained within them. Although each table within the database is important, I primarily dealt with HUMINT reports, SigAct reports and Counter IED reports because these reports were used to create a work product I was required to published as an analyst. In working on an assignment I looked anywhere and everywhere for information. As an all-source analyst, this was something that was expected. The D6-A systems had databases built in, and I utilized them on a daily basis. This simply was the search tools available on the D6-A systems on SIPRNet such as Query Tree and the DoD and Intellink search engines. Primarily, I utilized the CIDNE database using the historical and HUMINT reporting to conduct my analysis and provide a back-up for my work product. I did statistical analysis on historical data including SigActs

to back-up analyses that were based on HUMINT reporting and produce charts, graphs, and tables. I also created maps and charts to conduct predictive analysis based on statistical trends.

The SigAct reporting provided a reference point for what occurred and provided myself and other analysts with the information to conclude possible outcomes. Although SigAct reporting is sensitive at the time of their creation, their sensitivity normally dissipates within 48 to 72 hours as the information is either publicly released or the unit involved is no longer in the area and not in danger. It was my understanding that the SigAct reports remain classified only because they are maintained within CIDNE because it is only accessible on SIPRnet. Everything on CIDNE-I and CIDNE-A to include SigAct reporting was treated as classified information.

Facts Regarding the Storage of SigAct Reports

As part of my training at Fort Drum, I was instructed to ensure that I create back-ups of my work product. The need to create back-ups was particularly acute given the relative instability and reliability of the computer systems we used in the field during deployment. These computer systems included both organic and theater provided equipment (TPE) D6-A machines.

The organic D6-A machines we brought with us into the field on our deployment were Dell laptops and the TPE D6-A machines were Alien-ware brand laptops. The D6-A laptops were the preferred machine to use as they were slightly faster and had fewer problems with dust and temperature than the theater provided Alienware laptops. I used several D6-A machines during the deployment due to various technical problems with the laptops.

With these issues several analysts lost information, but I never lost information due to the multiple back-ups I created. I attempted to back-up as much relevant information as possible. I would save the information so that I or another analyst could quickly access it whenever a machine crashed, SIPRnet connectivity was down, or I forgot where the data was stored. When backing up information I would do one or all of the following things based on my training:

1) Physical back-up. I tried to keep physical back-up copies of information on paper so that the information could be grabbed quickly. Also, it was easier to brief with hard copies of research and HUMINT reports.

2) Local drive back-up. I tried to sort out information I deemed relevant and kept complete copies of the information on each of the computers I used in the Temporary Sensitive Compartmented Information Facility or T-SCIF, including my primary and secondary D6-A machines. This was stored under my user profile on the desktop.

3) Shared drive backup. Each analyst had access to what we call a T-drive, shared across the SIPRnet. It allowed others to access information that was stored on it. The S6 operated the T-drive.

4) Compact disk rewritable or CD-RW back-up. For larger data sets I saved the information onto a rewritable disk, labeled the disks, and stored them in the conference room of the T-SCIF. This redundancy allowed us to not worry about information loss. If the system crashed, I could easily pull the information from a secondary computer, the T-drive, or one of the CD-RWs. If another analysts wanted to access my data, but I was unavailable she could find my published products directory on the T-drive or on the CD-RWs. I sorted all of my products or research by date, time,

and group; and updated the information on each of the storage methods to ensure that the latest information was available to them.

During the deployment I had several of the D6-A machines crash on me. Whenever one computer crashed, I lost information but the redundancy method ensured my ability to quickly restore old back-up data and add current information to the machine when it was repaired or replaced.

I stored the back-up CD-RW with larger datasets in the conference room of the T-SCIF or next to a workstation. I marked the CD-RWs based on the classification level and its content. Unclassified CD-RWs were only labeled with the content type and were not marked with classification markings.

Early on in the deployment, I only saved and stored SigActs that were within or near operational environment. Later, I thought it would be easier to just to save all of the SigActs onto a CD-RW. The process would not take very long to complete, and so I downloaded the SigActs from CIDNE-I onto a CD-RW. After finishing with CIDNE-I, I did the same with CIDNE-A. By retrieving the CIDNE-I and CIDNE-A SigActs, I was able to retrieve the information whenever I needed it, and not rely upon the unreliable and slow SIPRnet connectivity needed to pull. Instead, I could just find the CD-RW and open up a pre-loaded spreadsheet.

This process began in late December 2009 and continued through early January 2010. I could quickly export one month of the SigAct data at a time and download in the background as I did other tasks. The process took approximately a week for each table. After downloading the SigAct tables, I periodically updated them, by pulling the most recent SigActs and simply copying them and pasting them into the database saved on the CD-RW. I never hid the fact that I had downloaded copies of both the SigAct tables

from CIDNE-I and CIDNE-A. They were stored on appropriately labeled and marked CD-RW, stored in the open.

I viewed saving copies of CIDNE-I and CIDNE-A as for both for my use and the use of anyone within S2 section during the SIPRnet connectivity issues.

In addition to the SigAct tables, I had a large repository of HUMINT reports and Counter IED reports downloaded from CIDNE-I. These contained reports relevant to the area in and around our operational environment in Eastern Baghdad and the Diyala Province of Iraq.

In order to compress the data to fit onto a CD-RW, I used a compression algorithm called "bzip2". The program used to compress the data is called "WinRAR". WinRAR is an application that is free, and can be easily downloaded from the internet via the Non-secure Internet Relay Protocol Network or NIPRnet. I downloaded WinRAR on NIPRnet and transfered it to the D6-A machine user profile desktop using a CD-RW. I did not try to hide the fact that I was downloading WinRAR onto my SIPRnet D6-A machine or computer.

With the assistance of the bzip2 algorithm using the WinRAR program, I was able to fit all of the SigACts onto a single CD-RW and relevant HUMINT and Counter ID reports onto a separate CD-RW.

Facts Regarding My Knowledge of the WikiLeaks Organization (WLO)

I first became vaguely aware of the WLO during my AIT at Fort Huachuca, Arizona, although I did not fully pay attention until WLO released purported Short Messaging System or SMS messages from 11 September 2001 on 25 November 2009. At that time references to the release and the WLO

website showed up in my daily Google news open source search for information related to US foreign policy.

The stories were about how WLO published about approximately 500,000 messages. I then reviewed the messages myself and realized that the posted messages were very likely real given the sheer volume and detail of the content.

After this, I began conducting research on WLO. I conducted searched on both NIPRnet and SIPRnet on WLO beginning in late November 2009 and early December 2009. At this time I also began to routinely monitor the WLO website. In response to one of my searches in December 2009, I found the United States Army Counter Intelligence Center or USACIC report on the WikiLeaks organization. After reviewing the report, I believed that this report was the one that my AIT referenced in early 2008.

I may or may not have saved the report on my D6-A workstation. I know I reviewed the document on other occasions throughout early 2010, and saved it on both my primary and secondary laptops. After reviewing this report, I continued doing research on WLO. However, based upon my open-source collection, I discovered information that contradicted the 2008 USACIC report including information that indicated that similar to other press agencies, WLO seemed to be dedicated to exposing illegal activities and corruption.

WLO received numerous award and recognition for its reporting activities. Also, while reviewing the WLO website, I found information regarding US military SOPs for Camp Delta at Guantanamo Bay, Cuba and information on outdated rules of engagement-ROE-in Iraq for cross-border pursuits of former members of Saddam Hussein s government.

After seeing the information available on the WLO website, I continued following it and collected open sources information from it. During this time period, I followed several organizations and groups including wire press agencies such as the Associated Press and Reuters and private intelligence agencies including Strategic Forecasting or Stratfor. This practice was something I was trained to do in AIT, and was something that good analysts were expected to do. During the searches of WLO, I found several pieces of information that I found useful in my work as an analyst, specifically I recall WLO publishing documents related to weapons trafficking between two nations that affected my OP. I integrated this information into one or more of my work products.

In addition to visiting the WLO website, I began following WLO using Instant Relay Chat or IRC Client called XChat sometime in early January 2010. IRC is a protocol for real time internet communications by messaging and conferencing, colloquially referred to as chat rooms or chats. IRC chat rooms are designed for group communication discussion forums. Each IRC chat room is called a channel, similar to a TV where you can tune in and follow a channelâ€" as long as it is open. Once you join a specific IRC conversation, other users in the conversation can see you have joined the room. On the Internet there are millions of different IRC channels across several services. Channel topics span a range of topics covering all kinds of interests and hobbies.

My primary reason for following WLO on IRC was curiosity, particularly in regards to how and why they obtained the SMS messages referenced above. I believed that collecting information on the WLO would assist me in this goal. Initially, I simply observed the IRC conversations. I wanted to know how the organization was structured, and how they obtained their data. The conversations I viewed were usually technical in nature but sometimes switched to a lively debate on issues the particular individual may have

felt strongly about.

Over a period of time I became more involved in these discussions especially when conversations turned to geopolitical events and information technology topics, such as networking and encryption methods. Based on these observations, I would describe the WLO organization [discussions?] as almost academic in nature. In addition to the WLO conversations, I participated in numerous other IRC channels across at least three different networks. The other IRC channels I participated in normally dealt with technical topics, including with Linux and Berkley Secure Distribution BSD operating systems or OS s, networking, encryption algorithms and techniques and other more political topics, such as politics and current events.

I normally engaged in multiple IRC conversations simultaneously-mostly publicly but often privately. The XChat client enabled me to manage these multiple conversations across different channels and servers. The screen for XChat was often busy, but its screens enabled me to see when something was interesting. I would then select the conversation and either observe or participate.

I enjoyed the IRC conversations pertaining to the WLO, however, at some point in late February or early March of 2010, the WLO IRC channel was no longer accessible. Instead, regular participants of this channel switched to using the Jabber server. Jabber is another internet communication tool similar, more sophisticated than IRC. The IRC and Jabber conversations, allowed me to feel connected to others even when alone. They helped pass the time and keep motivated throughout the deployment.

Facts Regarding **the Unauthorized Storage and Disclosure of the SigActs**

As indicated above, I created copies of the CIDNE-I and CIDNE-A SigAct tables as part of the process of backing up information. At the time I did so, I did not intend to use this information for any purpose other than for back-up. However, I later decided to release this information publicly. At that time, I believed and still believe that these tables are two of the most significant documents of our time.

On or around 8 January 2010, I collected the CD-RW I stored in the conference room of the T-SCIF and placed it into the cargo pocket of my army combat uniform. At the end of my shift, I took the CD-RW out of the T-SCIF and brought it to my Containerized Housing Unit of CHU. I copied the data onto my personal laptop.

Later at the beginning of my shift, I returned the CD-RW back to the conference room of the T-SCIF. At the time I saved the SigActs to my laptop, I planned to take them with me on mid-tour leave and decide what to do with them. At some point prior to my mid-tour, I transferred the information from my computer to a Secure Digital memory card from my digital camera. The SD card for the camera also worked on my computer and allowed me to store the SigAct tables in a secure manner for transport.

I began mid-tour leave on 23 January 2010, flying from Atlanta, Georgia, to Regan National Airport in Virginia. I arrived at the home of my aunt, Debra M. Van Alstyne, in Potomac, Maryland, and quickly got into contact with my then boyfriend, Tyler R. Watkins. Tyler-then a student at Brandeis University in Waltham, Massachusetts-and I made plans for me to visit him him in the Boston, Massachusetts area.

I was excited to see Tyler and planned on talking to him about where our relationship was going and about my time in Iraq. However, when I arrived in the Boston area Tyler seemed to become distant. He did not seem very

excited about my return from Iraq. I tried talking to him about our relationship but he refused to make any plans.

I also tried raising the topic of releasing the CIDNE-I and CIDNE-A SigAct tables to the public. I asked Tyler hypothetical questions about what he would do if he had documents that he thought the public needed access to. Tyler really didn t have a specific answer for me. He tried to answer the questions and be supportive, but he seemed confused by the question in this context. Then I tried to be more specific, but he asked too many questions. Rather than try to explain my dilemma, I decided to drop the conversation.

After a few days in Waltham, I began to feel I was overstaying my welcome, and returned to Maryland. I spent the remainder of my time on leave in the Washington, DC, area. During this time a blizzard bombarded the mid-atlantic. I spent a significant period of time essentially stuck in my aunt s house in Maryland.

I began to think about what I knew and the information I still had in my possession. For me, the SigActs represented the on-the-ground reality of the conflicts in both Iraq and Afghanistan. I felt that we were risking so much for people that seemed unwilling to cooperate with us, leading to frustration and [hatred? anger] on both sides.

I began to become depressed with the situation we found ourselves increasingly mired in. The SigActs documented this in great detail and provide a context of what we were seeing on the ground. In attempting to conduct counter-terrorism or CT and counter-insurgency COIN operations we became obsessed with capturing and killing human targets on lists and on being suspicious of and avoiding cooperation with our Host Nation partners, ignoring the second and third order effects of accomplishing

short-term goals and missions.

I believed that if the general public, especially the American public, had access to the information contained within the CIDNE-I and CIDNE-A tables it could spark a domestic debate on the role of the military and our foreign policy in general as it related to Iraq and Afghanistan.

I also believed the detailed analysis of the data over a long period of time by different sectors of society might cause society to reevaluate the need or even the desire to even to engage in counterterrorism and counterinsurgency operations that ignore the complex dynamics of the people living in the affected environment everyday.

At my aunt s house I debated what I should do with the SigActs, in particular whether I should hold on to them or disclose them to a press agency. At this point I decided that it made sense to expose the SigAct tables to an American newspaper. I first called my local newspaper, *The Washington Post*, and spoke with a woman saying that she was a reporter. I asked her if the *Washington Post* would be interested in receiving information that would have enormous value to the American public. Although we spoke for about five minutes concerning the general nature of what I possessed, I do not believe she took me seriously. She informed me that the *Washington Post* would possibly be interested, but that such decisions were made only after seeing the information I was referring to and after consideration by the senior editors.

I then decided to contact the largest and most popular newspaper, *The New York Times*. I called the public editor number on the *New York Times* website. The phone rang and was answered by a machine. I went through the menu section for news tips. I was routed to an answering machine. I left a message stating I had access to information about Iraq and Afghanistan

that I believed was very important. However, despite leaving my Skype phone number and personal email address, I never received a reply from *The New York Times*.

I also briefly considered dropping into the office for the political commentary blog Politico, however the weather conditions during my leave hampered my efforts to travel. After these failed efforts I ultimately decided to submit the materials to the WLO. I was not sure if the WLO would even actually publish the SigAct tables. I was concerned that they might not be noticed by the American media. However, based upon what I had read about the WLO through my research described above, this seemed to be the best medium for publishing this information to the world within my reach.

At my aunt s house I joined in on an IRC conversation and stated I had information that needed to be shared with the world. I wrote that the information would help document the true cost of the wars in Iraq and Afghanistan. One of the individuals in the IRC asked me to describe the information. Before I could describe the information another individual pointed me to the link for the WLO web site online submission system. After ending my IRC connection, I considered my options one more time. Ultimately, I felt that the right thing to do was to release the SigActs.

On 3 February 2010, I visited the WLO website on my computer and clicked on the submit documents link. Next I found the submit your information online link and decided to submit the SigActs via the router or TOR anonymizing network by special link. TOR is a system intended to provide anonymity online. The software routes internet traffic through a network of servers and other TOR clients to conceal the user s location and identity.

I was familiar with TOR and had it previously installed on a computer to anonymously monitor the social media website of militia groups operating within central Iraq. I followed the prompts and attached the compressed data files of CIDNE-I and CIDNE-A SigActs. I attached a text file I drafted while preparing to provide the documents to the *Washington Post*. I provided rough guidelines saying, "It s already been sanitized of any source identifying information. You might need to sit on this information-perhaps 90 to 100 days-to figure out how best to release such a large amount of data and to protect its source. This is possibly one of the more significant documents of our time removing the fog of war and revealing the true nature of twenty-first century asymmetric warfare. Have a good day."

After sending this, I left the SD card in a camera case at my aunt s house in the event I needed it again in the future. I returned from mid-tour leave on 11 February 2010. Although the information had not yet been published by the WLO, I felt this sense of relief by them having it. I felt I had accomplished something that allowed me to have a clear conscience based upon what I had seen and what I had read about and knew were happening in both Iraq and Afghanistan everyday.

Facts Regarding the Unauthorized Storage and Disclosure of 10 Reykjavik 13

I first became aware of the diplomatic cables during my training period in the AIT. I later learned about the Department of State or DoS netcentric Diplomacy NCD portal from the 2/10 Brigade Combat Team S2, Captain Steven Lim. Captain Lim sent a section-wide email to the other analysts and officer in late December 2009 containing the SIPRnet link to the portal, along with the instructions to look at the cables contained within them and incorporate them into our work product.

Shortly after this I also noticed the diplomatic cables were being reported to in products from the corp level US Forces Iraq or US-I. Based on Captain Lim s direction to become familiar with its contents, I read virtually every published cable concerning Iraq.

I also began scanning the database and reading other random cables that piqued my curiosity. It was around this time, in early to mid-January of 2010, that I began searching the database for information on Iceland. I became interested in Iceland due to the IRC conversations I viewed in the WLO channel discussing an issue called Icesave. At this time I was not very familiar with the topic, but it seemed to be a big issue for those participating in the conversation. This is when I decided to investigate and conduct a few searches on Iceland to find out more.

At the time, I did not find anything discussing the Icesave issue either directly or indirectly. I then conducted an open source search for Icesave. I then learned that Iceland was involved in a dispute with the United Kingdom and the Netherlands concerning the financial collapse of one or more of Iceland s banks. According to open source reporting much of the public controversy involved the UK s use of anti-terrorism legislation against Iceland in order to freeze Icelandic access for payment of the guarantees for UK depositors that lost money.

Shortly after returning from mid-tour leave, I returned to the Net Centric Diplomacy portal to search for information on Iceland and Icesave as the topic had not abated on the WLO IRC channel. To my surprise, on 14 February 2010, I found the cable 10 Reykjavik 13, which referenced the Icesave issue directly.

The cable, published on 13 January 2010, was just over two pages in length. I read the cable and quickly concluded that Iceland was

essentially being bullied diplomatically by two larger European powers. It appeared to me that Iceland was out viable options and was coming to the US for assistance. Despite the quiet request for assistance, it did not appear that we were going to do anything.

From my perspective it appeared that we were not getting involved due to the lack of long term geopolitical benefit to do so. After digesting the contents of 10 Reykjavik 13 I debated whether this was something I should send to the WLO. At this point the WLO had not published or acknowledged receipt of the CIDNE-I or CIDNE-A tables. Despite not knowing if the SigActs were a priority for the WLO, I decided the cable was something that could be important. I felt that I might be able to right a wrong by having them publish this document. I burned the information onto a CD-RW on 15 February 2010, took it to my CHU, and saved it on my personal laptop.

I navigated to the WLO website via a TOR connection like before and uploaded the document via the secure form. Amazingly, the WLO published 10 Reykjavik 13 within hours, proving the form worked and that they must have received the SigAct tables.

Facts Regarding the Unauthorized Storage and Disclosure of the 12 July 2007 Aerial Weapons Team (AWT) Video

During the mid-February 2010 time-frame, the 2nd Brigade Combat Team, 10th Mountain Division targeting analysts, then Specialist [Jihrleah?] W. Showman and others discussed a video that Ms. Showman had found on the T-drive.

The video depicted several individuals being engaged by an aerial weapons team. At first I did not consider the video very special, as I have viewed

countless other "war porn"-type videos depicting combat. However, the recording and audio comments by the aerial weapons team and the second engagement in the video of an unarmed bongo truck troubled me. As Showman and a few other analysts and officers in the T-SCIF commented on the video and debated whether the crew violated the rules of engagement or ROE in the second engagement, I shied away from this debate, and decided to conduct some research on the event. I wanted to learn what happened and whether there was any background to the events of the day that the event occurred, 12 July 2007.

Using Google I searched for the event by date by its general location. I found several new accounts involving two Reuters employees who were killed during the aerial weapon team engagement. Another story explained how Reuters had requested for a copy of the video under the Freedom of Information Act or FOIA. Reuters wanted to view the video in order to understand what had happened and to improve their safety practices in combat zones. A spokesperson for Reuters was quoted saying that the video might help avoid the re-occurrence of the tragedy and believed there was a compelling need for the immediate release of the video.

Despite the submission of the FOIA request, the news account explained that CENTCOM replied to Reuters, stating that they could not give a time frame for considering a FOIA request and that the video might no longer exist. Another story I found written a year later said that even though Reuters was still pursuing the request, they still did not receive a formal response or written determination in accordance with FOIA.

The fact neither CENTCOM or Multi National Forces Iraq or MNF-I would not voluntarily release the video troubled me further. It was clear to me that the event happened because the aerial weapons team mistakenly identified Reuters employees as a potential threat and that the people in the bongo

truck were merely attempting to assist the wounded. The people in the van were not a threat but merely "good Samaritans." The most alarming aspect of the video to me, however, was the seemly delightful blood-lust the Aerial Weapons Team seemed to have.

They dehumanized the individuals they were engaging and seemed to not value human life, and referred to them as quote-unquote "dead bastards," and congratulated each other on their ability to kill in large numbers. At one point in the video there is an individual on the ground attempting to crawl to safety. The individual is seriously wounded. Instead of calling for medical attention to the location, one of the aerial weapons team crew members verbally asks for the wounded person to pick up a weapon so that he can have a reason to engage. For me, this seemed similar to a child torturing ants with a magnifying glass.

While saddened by the aerial weapons team crew s lack of concern about human life, I was disturbed by the response of the discovery of injured children at the scene. In the video, you can see a bongo truck driving up to assist the wounded individual. In response the aerial weapons team crew assumes the individuals are a threat. They repeatedly request for authorization to fire on the bongo truck, and once granted, they engage the vehicle at least six times.

Shortly after the second engagement, a mechanized infantry unit arrives at the scene. Within minutes, the aerial weapons team crew learns that children were in the van. Despite the injuries the crew exhibits no remorse. Instead, they downplay the significance of their actions, saying quote Well, it s their fault for bringing their kids into a battle."

The aerial weapons team crew members sound like they lack sympathy for the children or the parents. Later, in a particularly disturbing manner, the

aerial weapons team crew vocalizes enjoyment at the sight of one of the ground vehicles driving over one of the bodies.

As I continued my research, I found an article discussing a book, *The Good Soldiers*, written by *Washington Post* writer David Finkel.

In Mr. Finkel book, he writes about the aerial weapons team attack. As I read an online excerpt in Google Books, I followed Mr. Finkel s account of the event belonging to the video. I quickly realize that Mr. Finkel was quoting, I feel verbatim, the audio communications of the aerial weapons team crew.

It is clear to me Mr. Finkel obtained access and a copy of the video during his tenure as an embedded journalist. I was aghast at Mr. Finkel s portrayal of the incident. Reading his account, one would believe the engagement was somehow justified as payback for an earlier attack that lead to the death of a soldier. Mr. Finkel ends his account of the engagement by discussing how a soldier finds an individual still alive from the attack. He writes the soldier finds him and sees him gesture with his two forefingers together-a common method in the Middle East to communicate that they are friendly. However, instead of assisting him, the soldier makes an obscene gesture with his middle finger.

The individual apparently dies shortly thereafter. Reading this, I can only think of how this person was simply trying to help others, and then quickly finds he needs help as well. To make matter worse, in the last moments of his life, he continues to express his friendly intent only to find himself receiving this well known gesture of unfriendliness. For me it s all a big mess. I was left wondering what these things mean, and how it all fits together. It burdens me emotionally.

I saved a copy of the video on my workstation. I searched for and found the rules of engagement, the rules of engagement annexes, and a flow chart from the 2007 time period, as well as an unclassified Rules of Engagement smart card from 2006. On 15 February 2010 I burned these documents onto a CD-RW at the same time I burned the 10 Reykjavik 13 cable onto a CD-RW. At the time, I placed the video and rules for engagement information onto my personal laptop in my CHU. I planned to keep this information there until I re-deployed in Summer 2010. I planned on providing this to the Reuters office in London to assist them in preventing events such as this in the future.

However, after the WLO published 10 Reykjavik 13, I altered my plans. I decided to provide the video and the rules of engagement to them so that Reuters would have this information before I re-deployed from Iraq. On about 21 February 2010, as described above, I used the WLO submission form and uploaded the documents. The WLO released the video on 5 April 2010. After the release, I was concern about the impact of the video and how it would been received by the general public. I hoped that the public would be as alarmed as me about the conduct of the aerial weapons team crew members. I wanted the American public to know that not everyone in Iraq and Afghanistan were targets that needed to be neutralized, but rather people who were struggling to live in the pressure cooker environment of what we call asymmetric warfare. After the release I was encouraged by the response in the media and general public who observed the aerial weapons team video. As I hoped, others were just as troubled-if not more troubled-that me by what they saw.

At this time, I began seeing reports claiming that the Department of Defense an CENTCOM could not confirm the authenticity of the video. Additionally, one of my supervisors, Captain Casey Fulton, stated her belief that the video was not authentic. In her response, I decided to

ensure that the authenticity of the video would not be questioned in the future. On 25 February 2010, I emailed Captain Fulton a link to the video that was on our T-drive, and a copy of the video published by WLO that was collected by the open source center so she could compare them herself.

Around this time frame, I burned a second CD-RW containing the aerial weapons team video. In order to make it appear authentic, I placed a classification sticker and wrote "Reuters FOIA Req" on its face. I placed the CD-RW in one of my personal CD cases containing a set of "Starting Out in Arabic" CDs. I planned on mailing out the CD-RW to Reuters after our re-deployment so they could have a copy that was unquestionably authentic.

Almost immediately after submitting the air weapons team video and rules of engagement documents, I notified the individuals in the WLO IRC to expect an important submission. I received a response from an individual going by the handle of "Office." At first our conversations were general in nature, but over time as our conversations progressed, I assessed this individual to be an important part of the WLO. Due to the strict adherence of anonymity by the WLO, we never exchanged identifying information, however, I believe the individual was likely Mr. Julian Assange [pronounced "Ah-sang-hee"], Mr. Daniel Schmidt, or a proxy representative of Mr. Assange ["Ah-sang-hee"] and Schmidt. As the communications transferred from IRC to the Jabber client, I gave "Office" and later "Press Association" the name of Nathaniel Frank in my address book, after the author of a book I read in 2009.

After a period of time, I developed what I felt was a friendly relationship with Nathaniel. Our mutual interest in information technology and politics made our conversations enjoyable. We engaged in conversation often. Sometimes as long as an hour or more. I often looked forward to my conversations with Nathaniel after work. The anonymity provided by TOR and

the Jabber client and the WLO s policy allowed me to feel I could just be myself, free of the concerns of social labeling and perceptions that are often placed upon me in real life.

In real life, I lacked a closed friendship with the people I worked with in my section, the S2 section. In my section, the S2 section supported battalions and the 2nd Brigade Combat Team as a whole. For instance, I lacked close ties with my roommate to his discomfort regarding my perceived sexual orientation.

Over the next few months, I stayed in frequent contact with Nathaniel. We conversed on nearly a daily basis, and I felt we were developing a friendship. The conversations covered many topics and I enjoyed the ability to talk about pretty much everything-not just the publications that the WLO was working on. In retrospect, I realize that these dynamics were artificial and were valued more by myself than Nathaniel. For me, these conversations represented an opportunity to escape from the immense pressures and anxiety that I experienced and built up through out the deployment. It seems that as I tried harder to fit in at work, the more I seemed to alienate my peers and lose the respect, trust, and support I needed.

Facts Regarding the Unauthorized Storage and Disclosure of Documents Related to the Detainments by the Iraqi Federal Police or FP, Detainee Assessment Briefs and the USACIC United States Army Counter Intelligence Center report:

On 27 February 2010, a report was received from a subordinate battalion. The report described an event in which the Federal Police, or FP, detained 15 individuals for printing anti-Iraqi literature. On 2 March 2010, I received instructions from an S3 section officer in the 2nd Brigade Combat

Team, 10th Mountain Division Tactical Operation Center or TOC to investigate the matter and figure out who the quote "bad guys" unquote were and how significant this event was for the Federal Police.

Over the course of my research I found that none of the individuals had previous ties to anti-Iraqi actions or suspected terrorist militia groups. A few hours later, I received several photos from the scene from the subordinate battalion. They were accidentally sent to an officer on a different team in the S2 section, and she forwarded them to me.

These photos included picture of the individuals, [pallets?] of unprinted paper and seized copies of the final, printed document, and a high-resolution photo of the printed material itself. I printed out one copy of a high resolution photo. I laminated it for ease of use and transfer. I then walked to the TOC and delivered the laminated copy to our Category 2 interpreter.

She reviewed the information and about a half and hour later delivered a rough written transcript in English to the S2 section. I read the transcript and followed up with her, asking her for her take on the content. She said it was easy for her to transcribe verbatim since I blew up the photograph and laminated it. She said the general nature of the document was benign. The document, as I had assessed as well, was merely a scholarly critique of the then current Iraqi Prime Minister Nouri al-Maliki.

It detailed corruption within the cabinet of al-Maliki s government and the financial impact of his corruption on the Iraqi people. After discovering this discrepancy between the Federal Police s report and the interpreter s transcript, I forwarded this discovery to the top OIC and the battle NCOIC. The top OIC and the [unavailable] battle captain

informed me they didn't want or need to know this information anymore. They told me to quote "drop it" unquote and to just assist them and the Federal Police in finding out where more of these print shops creating quote "anti-Iraqi literature" unquote might be.

I couldn't believe what I heard, and I returned to the T-SCIF and complained to the other analysts in my section NCOIC about what happened. Some were sympathetic, but no one wanted to do anything about it.

I am the type of person who likes to know how things work, and as an analyst, this means I always want to figure out the truth. Unlike other analysts in my section or other sections within the 2nd Brigade Combat Team, I was not satisfied with just scratching the surface and producing canned or cookie-cutter assessments. I wanted to know why something was the way it was, and what we could to correct or mitigate the situation.

I knew if I continued to assist the Baghdad Federal Police in identifying the political opponents of Prime Minister al-Maliki, those people would be arrested and in the custody of the Special Unit of the Baghdad Federal Police and very likely tortured and not seen again for a very long time-if ever.

Instead of assisting the Special Unit of the Baghdad Federal Police, I decided to take the information and expose it to the WLO, before the upcoming 7 March 2010 election, hoping they could generate some immediate press on the issue and prevent this unit of the Federal Police from continuing to crack down in political opponents of al-Maliki. On 4 March 2010, I burned the report, the photos, the high-resolution copy of the pamphlet, and the interpreter's hand-written transcript onto a CD-RW. I took the CD-RW [... copies to his personal computer]. Unlike the times before, instead of uploading the information through the submission form,

I used a Secure File Transfer Protocol, or SFTP connection, to a [cloud? file?] drop box operated by the WLO. The drop box contained a folder that allowed me to upload directly into it. Saving files into this directory allowed me or anyone with log-in access to server to view and download them. After uploading these files to the WLO, on 5 March 2010, I notified Nathaniel over Jabber. Although sympathetic, he said that the WLO needed more information to confirm the event in order for it to be published or to gain interest in the international media.

I attempted to provide the specifics but to my disappointment, the WLO website chose not to publish this information. At the same time, I began sifting through information from ... SOUTHCOM and Joint Task Force Guantanamo, Cuba or JTF-GTMO. The thought occurred to me, although unlikely ... the individual detained by the Federal Police might be turned over into US custody, ending up in the custody of Joint Task Force Guantanamo.

As I digested through the information on Joint Task Force Guantanamo, I quickly found the Detainee Assessment Briefs, or DABs. I previously came across the documents before in 2009 but did not think much about them. However, this time I was more curious in this search and I found them again.

The DABs were written in standard DoD memorandum format and addressed the commander of US SOUTHCOM. Each memorandum gave basic background information about detainees held at some point by Joint Task Force Guantanamo. I have always been interested in the issue of the moral efficacy of our actions surrounding Joint Task Force Guantanamo. On the one hand, I have always understood the need to detain and interrogate individuals who might wish to harm the United States and our allies, however, the more I became educated on the topic, it seemed that we found

ourselves holding an increasing number of individuals indefinitely that we believed or knew to be innocent, low-level foot soldiers that did not have useful intelligence and would ve been released if they were held in theater.

I also recall that in early 2009 the then newly elected president, Barack Obama, stated he would close Joint Task Force Guantanamo, and that the facility compromised our standing over all, and diminished our quote-unquote "moral authority." After familiarizing myself with the DABs, I agreed.

Reading through the Detainee Assessment Briefs, I noticed they were not analytical products. Instead they contained summaries of [unavailable] versions of interim intelligence reports that were old or unclassified. None of the DABs contained names of sources or quotes from tactical interrogation reports or TIRs. Since the DABs were being sent to the US SOUTHCOM commander, I assessed they were intended to provide general background information on each detainee-not a detailed assessment.

In addition to the manner [in which] the DABs were written, I recognized they were at least several years old, discussing detainees already released from Joint Task Force Guantanamo. Based on this, I determined that the DABs were not very important from either an intelligence or national security standpoint. On 7 March 2010, during my Jabber conversation with Nathaniel, I asked him if he thought the DABs might be of any use to anyone. Nathaniel indicated although he did not believe that they were of political significance, he did believe that they could be used to merge into the general historical account of what occurred at JTF Guantanamo. He also thought the DABs might be helpful to the legal counsel of those currently or previously held at Gitmo.

After this discussion, I decided to download the data. I used an application called Wget to download the DABs. I downloaded Wget off the NIPRnet laptop in the T-SCIF, like other programs. I saved that on a CD-RW and placed the executable in my documents directory on my user profile for the D6-A SIPRnet workstation.

On 7 March 2010, I took a list of links for the DABs, and used Wget to download them sequentially. I burned the data onto a CD-RW, and took it into my CHU, and copied them onto my personal computer. On 8 March 2010, I combined the Detainee Assessment Briefs with the United States Army Counterintelligence Center reports on the WLO into a compressed Zip file. Zip files contain multiple files, compressed to reduce their size.

After creating the zip file, I uploaded the file onto their [cloud? file?] drop box via Secure File Transfer Protocol. Once these were uploaded, I notified Nathaniel this information was in the X directory, designated for my own use.

Earlier that day, I downloaded the USACIC report on WLO. As discussed above, I previously reviewed the report on numerous occasions and although I saved the document onto the workstation before, I could not locate it. After I found the document again, I downloaded it to my workstation, and saved it onto the same CD-RW as the Detainee Assessment Briefs described above.

Although my access included a great deal of information, I decided I had nothing else to send to WLO after sending the Detainee Assessment Briefs and the USACIC report.

Up to this point I had sent them the following:

- the CIDNE-I and -A SigActs tables
- the Reykjavik 13 Department of State Cable
- the 12 July 2007 aerial weapons team video
- the 2006-2007 Rules of Engagement documents
- the SigAct report and supporting documents concerning the 15 individuals detained by the Baghdad Federal Police
- the US SOUTHCOM and Joint Task Force Guantanamo Detainee Assessment Briefs.
- a USACIC report on the WikiLeaks website and organization.

Over next few weeks I did not send any additional information to WLO. I continued to converse with Nathaniel over the Jabber client and in the WLO IRC channel. Although I stopped sending documents to WLO, no one associated with WLO pressured me into giving more information.

The decisions I made to send documents and information to WLO and the website were my own decisions, and I take full responsibility for my actions.

Facts Regarding the Unauthorized Disclosure of Other Government Documents

On 22 March 2010, I downloaded two documents. I found these documents over the course of my normal duties as an analyst. Based on my training and the possible guidance of my superiors, I looked at as much information as possible. Doing so provided me with the ability to make connections that others might miss. On several occasions throughout March, I accessed information from a government entity. I read several documents from a section within this government entity. The content of two of these documents upset me greatly, and I had difficulty believing what this section was doing.

On 22 March 2010, I downloaded the two documents that I found troubling and compressed them into a zip file named "Blah.zip," and burned them onto a CD-RW. I took the CD-RW to my CHU and copied the files to my personal computer. I uploaded the information to the WLO website using the designated prompts.

Facts Regarding the Unauthorized Storage and Disclosure of the Net Centric Diplomacy Department of State Cables

In late March 2010, I received a warning over Jabber from Nathaniel, that the WLO website would be publishing the aerial weapons team video. He indicated that the WLO would be very busy and the frequency and intensity of our Jabber conversations might decrease significantly.

During this time, I had nothing but work to distract me. I read more of the diplomatic cables published on the Department of State Net Centric Diplomacy server. With my insatiable curiosity and interest in geopolitics, I became fascinated. I read not only the cables on Iraq, but also about countries and events I found interesting. The more I read, the more I was fascinated by the way we dealt with other nations and organizations. I soon began to think the documented backdoor deals and seemingly criminal activity didn t seem characteristic of the de facto leader of the free world.

Up to this point during the deployment, I had issues I struggled with and difficulty at work. Of the documents released, the cables were the only ones I was not absolutely certain couldn t harm the United States. I conducted research on the cables published on Net Centric Diplomacy, as well as how Department of State cables worked in general.

In particular, I wanted to know how each cable was published on SIRPnet

via the Net Centric Diplomacy. As part of my open source research, I found a document published by the Department of State on its official website. The document provided guidance on caption markings for individual cables and handling instructions for their distribution. I quickly learned the caption markings clearly detailed the sensitivity of Department of State cables. For example, NODIS or No Distribution was used for messages at the highest sensitivity and were only distributed to the authorized recipients.

The SIPDIS or SIPRnet distribution caption applied only to [unavailable verbatim: he describes information and messages "deemed appropriate for" release and "a wide number of individuals"]. According to the Department of State guidance, for a cable to have the SIPDIS caption, it could not include other captions limiting distribution.

The SIPDIS caption was only for information [to be] shared with anyone [authorized to] access SIPRnet. I was aware that thousands of military personnel, DoD, DoS, and other civilian agencies had easy access to the tables. The fact the SIPDIS caption was for wide distribution made sense to me given how the vast majority of the Net Centric Diplomacy Cables were not classified.

The more I read the cables, the more I came to the conclusion this was the type of information that should become public. I once read [unavailable] a quote on open diplomacy written after the First World War [about how] the world would be a better place if states would avoid making secret pacts and deals with or against each other. I thought these cables were a prime example of the need for more open diplomacy.

Given all of the DoS info I read, the fact most of these cables were unclassified, and that all the cables have a SIPDIS caption, I believed

the public release of these cables would not damage the United States. I did believe that the cables might be embarrassing since they represent very honest opinions and statements behind the backs of other nations and organizations. In many ways these cables are a catalogue of cliques and gossip. I believed exposing this information might make some within the DoS, and other government entities, unhappy.

On 22 March 2010, I began downloading a copy of the SIPDIS cables using the program wget, described above. I used instances of the Wget application to download the Net Centric Diplomacy cables in the background. As I worked on my daily tasks, the Net Centric Diplomacy cables were downloaded from 28 March 2010 to 9 April 2010. After downloading the cables, I saved them to a CD-RW.

These cables went from the earliest dates in Net Centric Diplomacy to 28 February 2010. I took the CD-RW to my CHU on 10 April 2010. I sorted the cables on my personal computer, compressed them using the [bzip2?] compression algorithm described above, and uploaded them to the WLO via designated drop box.

On 3 May 2010, I used wget to download and update cables for the months of March 2010 and April 2010. I saved the information onto a Zip file and burned it to a CD-RW. I then took the CD-RW to my CHU and saved those to my computer. I later found that the file was corrupted during the transfer. I intended to save another copy of these cables, but was removed from the T-SCIF on 8 May 2010 after an altercation.

Facts Regarding the Unauthorized Storage and Disclosure of Garani, Farah Province, Afghanistan 15-6 Investigation and Videos

In late March 2010, I discovered a US CENTCOM directory on a 2009

air-strike in Afghanistan. I was searching CENTCOM for information I could use as an analyst. This is something myself and other officers did on a frequent basis. As I reviewed the documents, I recalled the incident and what happened. The airstrike occurred in the Garani village in the Farah Province, Northwestern Afghanistan. It received worldwide press coverage at the time as it was reported that up to 100-150 Afghan civilians, mostly women and children, were accidentally killed during the airstrike.

After going through the report and annexes, I began to review the incident as being similar to the 12 July 2007 aerial weapons team engagements in Iraq, however, this event was noticeably different in that it involved a significantly higher number of individuals, larger aircraft and much heavier munitions. The conclusions of the report are more disturbing than those of the July 2007 incident. I did not see anything in the 15-6 report or its annexes that gave away sensitive information. Rather, the investigation and its conclusions help explain how the incident occurred and what those involved should of done to avoid an event like this occurring again.

After investigating the report and annexes, I downloaded the 15-6 investigation, PowerPoint presentations and supporting documents to my workstation. I also downloaded three zip files containing the videos of the incident. I burned this information onto a CD-RW and transfered it to the personal computer in my CHU. Later that day or the next, I uploaded the information to the WLO website using a new version of the submission form. Unlike other times using the submission form above, I did not activate the TOR anonymizer.

Your Honor, this concludes my statement and facts for this providence inquiry.