In The Matter Of:

United States vs.
PFC Bradley E. Manning

Vol. 5

June 11, 2013

UNOFFICIAL DRAFT - 6/11/13 Morning Session

Provided by Freedom of the Press Foundation

1

1   VOLUME V

2   IN THE UNITED STATES ARMY

3

4   UNITED STATES

5   VS.

6   MANNING, Bradley E., PFC   COURT-MARTIAL

7   U.S. Army, xxx-xx-9504

8   Headquarters and Headquarters Company,

9   U.S. Army Garrison,

10   Joint Base Myer-Henderson Hall,

11   Fort Myer, VA 22211

12   _____/

13

14

15   The Hearing in the above-entitled matter was

16   held on Tuesday, June 11, 2013, commencing at 9:30 a.m.,

17   at Fort Meade, Maryland, before the Honorable Colonel

18   Denise Lind, Judge.

19

20

21

1   DISCLAIMER

2

3   This transcript was made by a court

4   reporter who is not the official Government reporter,

5   was not permitted to be in the actual courtroom where

6   the proceedings took place, but in a media room

7   listening to and watching live audio/video feed, not

8   permitted to make an audio backup recording for

9   editing purposes, and not having the ability to

10   control the proceedings in order to produce an

11   accurate verbatim transcript.

12

13   This unedited, uncertified draft

14   transcript may contain court reporting outlines that

15   are not translated, notes made by the reporter for

16   editing purposes, misspelled terms and names, word

17   combinations that do not make sense, and missing

18   testimony or colloquy due to being inaudible to the

19   reporter.

20

21

1   APPEARANCES:

2

3   ON BEHALF OF THE GOVERNMENT:

4   MAJOR ASHDEN FEIN

5   CAPTAIN ALEXANDER von ELTEN

6

7   ON BEHALF OF THE ACCUSED:

8   DAVID COOMBS

9   MAJOR THOMAS HURLEY

10   CAPTAIN JOSHUA TOOMA

11

12

13

14

15

16

17

18

19

20

21

4

```
 1                      PROCEEDINGS,

 2               THE COURT:  Major Fein, please account

 3   for the parties.

 4               MR. FEIN:  Yes, ma'am.  Your Honor, all

 5   parties in the court from last recess are again present,

 6   exceptions are Captain Overgaard and Captain Morrow are

 7   absent.  Captain von Elten is present.

 8               THE COURT:  Are there any issues we need to

 9   address before we proceed?

10               MR. FEIN:  Yes, ma'am.  A few admin issues.

11   First, this morning United States filed what's been

12   marked as appellate exhibit 566, the witness list order

13   of proposed prosecution witnesses.  That's an updated

14   listing from the previous.

15               THE COURT:  All right.  Thank you.

16               MR. FEIN:  Also, ma'am, as of 0930 this

17   morning there are eleven members of the media in the

18   media operations center.  There are two stenographers.

19   There's no one presently in the trailer, although the

20   trailer is available and the courtroom is not filled to

21   capacity.
```

1   THE COURT: All right. Thank you very much.

2   MR. COOMBS: Ma'am, I would like to put on

3   the record that the government has indicated pretty much

4   from this day forward they'll accommodate the request of

5   the stenographers to have one come in the morning, one

6   come in the afternoon session, and that also the

7   stenographers will be given a dedicated pass for the

8   media operations center.

9   THE COURT: Is that correct?

10   MR. FEIN: Yes, ma'am. Also, the United

11   States' understanding is that the court's preference or

12   directive is that one of the 70 spots for the media will

13   actually become 69 spots and a stenographer will be the

14   70th spot, so it will actually not be a media spot, it

15   will be the stenographer spot. That way the public

16   affairs will credential 69 positions, not 70.

17   THE COURT: That is actually what I did

18   direct you to do. Any objection to that?

19   MR. COOMBS: No objection, Your Honor.

20   THE COURT: Anything else we need to address?

21   MR. COOMBS: No, Your Honor.

 1   MR. FEIN: No, ma'am.

 2   THE COURT: Please call your next witness.

 3   MR. FEIN: Ma'am, prior to that we're going

 4 to read some stipulations.

 5   THE COURT: Can you tell me who those are?

 6   THE WITNESS: Yes, ma'am. Ma'am, the first

 7 stipulation is Mr. Peter Artale, prosecution exhibit

 8 number 70. The next is Mr. Chamberlin, prosecution

 9 exhibit 71.

10   THE COURT: Thank you.

11   MR. FEIN: Your Honor, stipulation of

12 expected testimony of Mr. Peter Artale, dated 9 June

13 2013.

14   It is hereby agreed by the Accused, Defense

15 Counsel, and Trial Counsel, that if Mr. Peter.

16 Artale were present to testify during the merits and

17 pre-sentencing phases of this court-martial, he would

18 testify substantially as follows:

19   One. I am currently employed by the Army

20 Counter-Intelligence Center, ACIC, with the 902nd

21 Military Intelligence Group on Fort Meade, Maryland.

1 ACIC produces finished intelligence products for the

2 intelligence community. It often produces these

3 products by fulfilling requests for information from

4 the Army. It takes finished products and

5 disseminates them on SIPRNET and JWICS.

6   I am a Web Developer and the Team Lead of

7 a team of three software developers. I have worked

8 in this capacity and for ACIC for eight years. Prior

9 to this position, I worked in web development for the

10 Defense Intelligence Agency, DIA, for one year, then

11 with Booz Allen on a one year contract with National

12 Geo-Spatial Agency. I was a software development

13 engineer and programmer in the Air Force for

14 twenty-one years. I retired from the Air Force as a

15 Master Sergeant. I also have an Associate's degree

16 in Computer Science.

17   Two. I first became involved in this

18 case on approximately 17 March 2010 after my Branch

19 Chief, Ms. Jessica Johnson, alerted me to the

20 compromise of U.S. Government information. Ms.

21 Johnson asked if I could use our system to see who

1   had viewed a certain product. I could, as I had

2   developed custom software to track access to

3   particular products. This software captures the

4   viewer credentials by recording the Internet Protocol

5   (IP) address and date/time of access for each user

6   who views our ACIC work product. It then assigns a

7   unique report key to the access event. This occurred

8   before we were contacted by law enforcement in this

9   case, as ACIC was notified of the compromise of one

10 of our products in March 2010.

11   Three. An IP address is part of the

12 Transmission Control Protocol/Internet Protocol

13 (TCP/IP). A protocol is the standard language used

14 to communicate over a network. TCP/IP is the most

15 common "language" that computers use to communicate

16 over the Internet and so an IP address is the method

17 of identifying a specific computer on a network.

18 Only one computer can be assigned a specific IP

19 address at one time. Knowing an IP address allows us

20 to know which computer on a given network used our

21 products.

1   Our software is a custom product which,

2   in capturing this user and access information,

3   produces metrics which can be used to see which of

4   our products are most popular and how our products

5   are used. The software only logged views of the

6   document in the ".asp" format which is the standard

7   way the product would appear on the website. ".asp"

8   is a common file format for web pages. This means

9   that the software only logged views of the web

10 version of the document and not the views of the

11 ".pdf" or ".doc" version of the document. Likewise,

12 the logs do not indicate whether the document was

13 printed or saved, nor do they indicate how long an

14 individual looked at the document, if at all. We

15 collect this data normally so we can analyze it to

16 see where we need to allocate our development and

17 maintenance resources to best support our internal

18 and external customers. The information produced by

19 the tracking software is, therefore, called metrics.

20   Four. The metrics are pulled when an

21 engineer runs a certain query. These queries can be

 1 customized to pull only the information the developer

 2 wants to see. In this case, we were specifically

 3 interested in tracking every access to a product

 4 titled "WikiLeaks.org-An Online Reference to Foreign

 5 Intelligence Services, Insurgents, or Terrorists

 6 Groups?" Therefore, I searched the product by

 7 determining and searching for its product

 8 identification number, which is "RB08-0617". The

 9 product identification number, which is on the

10 document itself and assigned internally by ACIC, is a

11 identifier unique to each ACIC product.

12   Five. This ACIC product "WikiLeaks.org-

13 An Online Reference to Foreign Intelligence Services,

14 Insurgents, or Terrorists Groups?" is housed on our

15 website at "acic.north-inscom.anny.smil.mil" and is

16 accessible only via a classified network, such as

17 SIPRNET. I wrote a custom query, by IP address and

18 visit time, to see every time this particular

19 document was pulled from the web server. A custom

20 query is a method of pulling information from a

21 Database. I pulled these metrics from my own

1   workstation. The data is automatically pulled into a

2   Structured Query Language (SQL) table. SQL is a

3   computer language for extracting and inserting

4   information in a database. It is a standard computer

5   language to interact with databases. Printouts of

6   SQL queries look like an Excel spreadsheet in that it

7   has columns and rows; however, it is not as easy to

8   search and organize as an Excel spreadsheet. I,

9   therefore, digitally cut and pasted the information

10   from the SQL table into an Excel spreadsheet and

11   saved the data to my desktop.

12   I then organized the spreadsheets in two

13   separate manners. The first set is organized by

14   visit date. The second is organized by IP address

15   and then visit date. I did not alter the content of

16   the data in any way when searching for the data,

17   moving it from the SQL table to the Excel

18   spreadsheet, or while in the Excel spreadsheet. I

19   moved the information and organized it in two

20   separate manners because it was easier to read. I

21   then emailed the metric data to my leadership at ACIC

1   as requested.

2   The data is stored securely on our

3   servers and is only accessible to the other three web

4   developers on my team. I have no reason to believe

5   anyone else would have modified the logs in any way.

6   This occurred before we were contacted by

7   investigators involved in this case, as ACIC was

8   notified of the compromise of one of our products in

9   March 2010.

10   Six. In this case, the ACIC document

11   concerned was posted in 2008. I pulled the metric

12   data tracking access to this document on 17 March

13   2010. The most recent access date listed in the

14   metric data is 16 March 2010. The data returned

15   included view hits on the document up until the

16   morning I ran the data query. The logs are broken

17   down by record key, IP address, and visit date.

18   Specifically, the metrics tell me the

19   following about the user IP addresses who opened the

20   website containing the product with a product

21   identification number of RB08-0617 in the web page

1   format: A user with the IP address 22.225.41.40

2   opened the web page on 1 December 2009 at 6:31 PM; a

3   user with the IP address 22.225.41.40 opened the web

4   page on 29 December 2009 at 2:40 PM; a user with the

5   IP address 22.225.41.40 opened the web page on 1

6   March 2010 at 6:40 PM; and a user with the IP address

7   22.225.41.22 opened the web page on 7 March 2010 at

8   11:31 PM.

9   Seven. The data for these metrics is

10 collected by our custom software automatically when

11 someone clicks on one of our links to use our ACIC

12 work product. This system captures the time, date,

13 and IP address as well as which product is being

14 accessed and served out to the requester. We know

15 this data is accurate because there is no human

16 intervention into the process and because views are

17 logged using specific codes and for specific

18 products.

19   Finally, while it is possible to make

20 manual insertions in metric data output, those

21 insertions cannot be backdated or over-written. This

1 means whatever output data the system produces cannot

2 itself be altered. Furthermore, at the time I pulled

3 these logs, I did not know to whom the IP addresses

4 were attached or the reasons for which the data was

5 being pulled. I had neither the motivation nor

6 knowledge required to alter the document. At no

7 point prior to pulling the metric log data, while

8 pulling the information, or after securing it, did I

9 ever alter the data in any way.

10   Eight. My Branch Chief forwarded my

11 email with these metrics to Mr. Winston Budram, S-6

12 and Chief Information Officer of the 902nd MI Group.

13 Mr. Budram forwarded the metrics to investigators

14 after they contacted our office.

15   Prosecution Exhibit (PE) 63 for

16 identification is the paper copy of these logs. PE

17 63 for ID is a printout of the complete logs that I

18 pulled. I put the title "Views of ACIC Product

19 RB08-0617.asp" on the top of the Excel spreadsheet.

20 The title is based on the ACIC product identification

21 number and the format of the document. On the left

1 side of every page are the logs that I pulled and

2 organized by visit date. On the right side of every

3 page are the logs that I pulled and organized by IP

4 address and then visit date.

5   I believe the information on the top of

6 the page ("Views of ACIC Product RB08-0617.asp";

7 "Record Key"; "IP Address"; and "Visit Date"), which

8 is the same as the title and heading information on

9 the spreadsheets that I pulled, was automatically

10 produced by Excel when the spreadsheets were printed.

11   Nine. I am the custodian of the records

12 marked as PE 63 for ID and an employee familiar with

13 the manner and process in which these records are

14 created and maintained, by virtue of my duties and

15 responsibilities. PE 63 for ID was made at or near

16 the time of the occurrences of the matters set forth

17 by or from information transmitted by, people with

18 knowledge of these matters. PE 63 for ID was kept in

19 the course of regularly conducted business activity.

20 It was the regular practice of the business activity

21 to make the records. The records marked as PE 63 for

1   ID are a true, accurate, and complete copy of the

2   original documents.

3   Your Honor, the United States moves to

4   admit PE 63 for ID as PE 63.

5   MR. HURLEY: No objection, ma'am.

6   THE COURT: All right. Prosecution exhibit

7   63 is admitted. May I see it, please?

8   Thank you.

9   MR. FEIN: Ma'am, stipulation of expected

10 testimony of Mr. Shawn Chamberlin dated 9 June 2013.

11   It is hereby agreed by the Accused, Defense

12 Counsel, and Trial Counsel, that if Mr. Sean Chamberlin

13 were present to testify during the merits and

14 pre-sentencing phases of this court-martial, he would

15 testify substantially as follows:

16   One. I am a Systems Administrator for the S6

17 shop of the 902nd Military Intelligence (MI) Group on

18 Fort Meade, Maryland. The 902nd MI Group performs

19 counterintelligence functions. My section is

20 responsible for providing IT support for all unit

21 servers. In this capacity, I build new servers and

1   maintain old ones. I have worked in this capacity

2   for ten years. Before that I was active duty

3   military for nine years and was a Staff Sergeant when

4   I left the Army.

5   For the last five of my nine years of

6   active duty service, I had the Military Occupational

7   Specialty (MOS) 33W, which is Intercept Electronic

8   Warfare Systems Repair. In that capacity, I was a

9   systems administrator. To fulfill my current

10 function, I have received Security Plus training and

11 have certifications in numerous Microsoft server

12 types. I also hold a Bachelor's degree in

13 Information Systems from the University of Phoenix.

14   Two. I first became involved in the

15 present case in July of 2011 when my supervisor Mr.

16 Robert Conner, the Site Lead for Information

17 Technology at the 902nd MI Group, requested that I

18 pull Microsoft Internet Information Services (MIIS)

19 web server audit event logs for the contacting IP

20 addresses 22.225.41.22 and 22.225.41.40 between the

21 dates November 2009 and May 2010. MIIS are

1   application logs that are specific to the web server.

2   Audit logs are a record of the activity that occurs

3   on the server and enable system administrators like

4   me to track what users do on the website. Audit logs

5   contain data that is automatically written to them on

6   a daily basis.

7   Here, the audit logs record file activity

8   on a web server from the United States Government

9   computer assigned to the IP address 199.32.48.154, is

10   a computer dedicated to processing classified

11   information at the SECRET level. This is the IP

12   address for the ACIC website on SIPRNET.

13   Three. This data shows what IP addresses

14   accessed our system within that date range. An IP

15   address is part of the Transmission Control

16   Protocol/Internet Protocol (TCP/IP). A protocol is

17   the standard language used to communicate over a

18   network. TCP/IP is the most common "language" that

19   computers use to communicate over the Internet. An

20   IP address is the method of identifying a specific

21   computer on a network.

 1   Four. An IP address allows us to know

 2   which computer on a given network accessed our

 3   server. In this case, I pulled eighteen log files

 4   for the above IP address and date range. The files

 5   are named the following: ex091119.log; ex091201.log;

 6   ex091214.log; ex091217.log; ex091221.log;

 7   ex091229.log; ex100207.log; ex100209.log;

 8   ex100211.log; ex100214.log; ex100301.log;

 9   ex100302.1og; ex100308.log; ex100315.log;

10   ex100316.log; ex100317.log, which is the automatic

11   naming convention of Microsoft based on date.

12   The files display in text format. The

13   files contain 86 entries for the IP address of

14   22.225.41.22 and 28 entries for the IP address of

15   22.225.41.40. The first entry for 22.225.41.22 or

16   22.225.41.40 is 19 November 2010.

17   Five. These logs are on our external web

18   server, which is one of the servers I am responsible

19   for maintaining. The web server and the logs are

20   located in what is commonly referred to as the

21   "DMZ", which is the area between our internal system

1   and the SIPRNET. I pulled the data using a search

2   window and searching the IP address for the given

3   date range. Then I searched for the two requested IP

4   addresses. I then put the files into an internal

5   investigation folder and had them burned to a disc. I

6   looked at the disc to verify that they were the logs

7   that I pulled.

8   Six. I am familiar with these logs

9   because of my work as a systems administrator. After

10   I pulled the logs, they were burned onto a rewritable

11   disc by another individual. I reviewed the contents

12   of the disc to ensure it contained the logs that I

13   pulled. The disc labeled "Log Files 902nd MI

14   20 11-0006" contain the logs that I pulled.

15   Prosecution Exhibit 64 for Identification is a copy

16   of this disc. I attested to the authenticity of these

17   logs on 21 June 2012, BATES number: 00449439. I

18   pulled the logs from the server and did not alter the

19   content of the logs in any way. I have no reason to

20   believe anyone else would have modified the logs in

21   any way while they are on the server as permissions

1 to the "DMZ" are very limited.

2   Your Honor, the United States moves to

3 admit prosecution exhibit 64 for identification as

4 prosecution exhibit 64.

5   MR. HURLEY: Ma'am, we have no objection to

6 that. May I have a second to speak with Major Fein?

7   THE COURT: Yes.

8   MR. FEIN: Your Honor, the United States

9 requests a brief in place recess.

10   THE COURT: Go ahead. We're not actually

11 recessing the court, I'm going to let you do what you

12 need to do.

13   MR. FEIN: Yes, ma'am.

14   (BRIEF PAUSE.)

15   MR. FEIN: Ma'am, I have retrieved

16 prosecution exhibit 71 and consulted with defense counsel

17 and there has been one modification to the stipulation of

18 expected testimony. I handed the court reporter PE 71

19 and I would direct the court to page two.

20   Your Honor, the top of page two at the end of

21 the first paragraph or the first partial paragraph, the

```
 1  date 19 November 2010 has been modified to 19 November
 2  2009, and the accused's, Major Hurley's and Major Fein's
 3  initials are annotated on that change.
 4                  THE COURT:  All right.  Major Hurley, does
 5  the defense agree with this change?
 6                  MR. HURLEY:  Yes, ma'am.
 7                  THE COURT:  PFC Manning?
 8                  THE ACCUSED:  Yes, ma'am.
 9                  MR. Von ELTEN:  Ma'am, the United States
10  calls Matthew Hosburgh.
11                  THE COURT:  May I see prosecution exhibit 64?
12  I think I still need to admit that.  Is that better done
13  at a recess?
14                  MR. FEIN:  Yes, ma'am, 64.
15                  THE COURT:  Prosecution exhibit 64 for
16  identification is admitted.
17                  Excuse me, Captain von Elten, who is the next
18  witness?
19                  MR. Von ELTEN:  Matthew Hosburgh.
20
21
```

24

1   Whereupon:

2   MATTHEW HOSBURGH,

3   called as a witness, having been first duly sworn

4   according to law, testified as follows:

5   DIRECT EXAMINATION

6   BY MR. Von ELTEN:

7   Q.   For the record, you're Sergeant Matthew

8   Hosburgh of Denver, Colorado?

9   A.   Staff sergeant.

10   Q.   Where do you work?

11   A.   I'm currently working for an oil and gas

12   company in Denver, Colorado.

13   Q.   And what do you do there?

14   A.   I do their IT security.

15   Q.   And what does that entail?

16   A.   It entails monitoring the networks as well as

17   threat and vulnerability research.

18   Q.   And how long have you been in this position?

19   A.   I've been there for about two months now, sir.

20   Q.   And what was your position prior to that?

21   A.   Prior to that I was a government contractor

```
 1   where I did basically the same type of work for

 2   citizenship and immigration.

 3        Q.     And what department does citizenship and

 4   immigration reside in?

 5        A.     Department of Homeland Security.

 6        Q.     And how long were you there?

 7        A.     I was there for three years.

 8        Q.     And how was the work similar; what did you do?

 9        A.     Same type of thing, monitoring networks,

10   looking for threats, vulnerabilities and, yeah, that's

11   basically it.

12        Q.     And what did you do prior to that?

13        A.     Prior to that I was on active duty in the

14   Marine Corps.

15        Q.     And for how long were you on active duty?

16        A.     For eight years.

17        Q.     What was your MOS in the Marine Corps?

18        A.     I was a 2651.

19        Q.     What is that?

20        A.     It's a special intelligence system

21   administrator.
```

1 Q. What training did you receive in that

2 position?

3 A. I received numerous military schools as well

4 as civilian IT security related courses.

5 Q. And what kind of things did that schooling

6 teach you?

7 A. Everything from system administration,

8 servers, networks, to security, basic security and things

9 of that nature.

10 Q. What kind of work did being a 2651 entail?

11 A. Kind of ran the gamut as far as anything from,

12 you know, managing servers and network equipment to

13 information assurance and security accreditation and

14 threat and vulnerability research.

15 Q. What kind of systems did you work on?

16 A. Worked primarily on classified network

17 systems, servers and networks of that nature.

18 Q. And what kind of work did you do on those

19 classified systems?

20 A. Managed the systems, provided access to our

21 users as well as I was in charge of the security of those

1 systems, so we had to basically apply policy to those

2 systems as well as manage the vulnerabilities and risks

3 that the systems faced.

4   Q.   What year did you leave active duty?

5   A.   2010.

6   Q.   What is your current military status?

7   A.   I'm a reservist.

8   Q.   When did you join the reserves?

9   A.   I joined in July of 2012.

10   Q.   What do you do in the reserves?

11   A.   I have the same MOS so I do the same type of

12 general work, but I'm currently working as a network

13 analysis or I'm a network analyst.

14   Q.   Let's talk a little bit about a report you

15 wrote. Where were you stationed in late 2009, early

16 2010?

17   A.   I was in Stuttgart, Germany.

18   Q.   And what were you doing there?

19   A.   I had been stationed there, started out in

20 2006.

21   Q.   Do you remember attending a conference?

1   A.   Yes, sir.

2   Q.   What was the conference called?

3   A.   It was, the title of the conference was called

4 here be dragons.

5   Q.   And who hosted the conference?

6   A.   It was hosted by the Chaos Computer Club.

7   THE COURT: What dragons?

8   THE WITNESS: Here be dragons.

9   Q.   How else is the Chaos Computer Club referred

10 to?

11   A.   It's either known as CCC or C3.

12   Q.   How did you know about C3?

13   A.   Through my research that I was doing just

14 trying to stay ahead of security threats, I noticed that

15 the conference was basically in our neck of the woods and

16 that's how I found out about it.

17   Q.   And where was the conference?

18   A.   It was in Berlin.

19   Q.   And when did the conference occur?

20   A.   It was roughly the 26th of December, 2009

21 through the 30th, if I remember correctly.

```
 1        Q.      What is the C3 conference?

 2        A.      So the C3 conference essentially, what it

 3   actually stands for is the Chaos Communication Congress.

 4   It's a conference that basically combines or brings

 5   together people throughout the hacker community, security

 6   researchers and just random people, brings them all

 7   together and they talk about various topics ranging from

 8   security, hacking, political issues.  I mean you name it

 9   and it's probably there.

10        Q.      And how often is it held?

11        A.      It's held yearly.

12        Q.      And why did you attend?

13        A.      I attended, it was an opportunity to not only

14   attend a conference that could potentially I guess show

15   some security vulnerabilities that we might be able to

16   apply to our command, but is also local and we had some

17   extra funds to go travel and go to that conference, so --

18        Q.      How many days was the conference?

19        A.      I believe it was five days.

20        Q.      And how many days did you attend?

21        A.      I was there for four days.  One day was for
```

```
 1  travel.
 2        Q.      How many people attended the conference?
 3        A.      Roughly about three to 5,000, I believe.
 4        Q.      What kind of facility hosted the conference?
 5        A.      It was your standard just conference center,
 6  multiple rooms that could host various talks and
 7  presentations.
 8        Q.      And where were the featured presentations
 9  given?
10        A.      The featured presentations?  Those were
11  reserved for the bigger rooms of the conference center.
12        Q.      And about how big was the bigger room, how
13  many people did it seat?
14        A.      How many people?  Okay.  Roughly maybe five to
15  a thousand people.
16        Q.      500 to a thousand people?
17        A.      I'm sorry.  500, yes, sir.
18        Q.      What were some of the main presentations?
19        A.      Some of the main presentations I recall
20  offhand they were talking about, one of the big ones was
21  WikiLeaks, they talked about net neutrality, Tor came up.
```

```
 1    They talked about various topics related to GSM cellphone
 2    networks.  A few others, I just can't recall off the top
 3    of my head.
 4         Q.    And what language were the talks given in?
 5         A.     They were given in English and some of them
 6    were also in German.
 7         Q.    Let's talk a little bit about the net
 8    neutrality presentation.  How many speakers gave that
 9    presentation?
10         A.     I recall, I believe there was two speakers for
11    that one.  One main presenter though.
12         Q.    And how long did the presentation last?
13         A.     That was about an hour if I remember that one
14    right.
15         Q.    And what is net neutrality?
16         A.     Well, net neutrality, the way I see it is a
17    way to keep the Internet open and free as far as
18    preventing any issues or ISPs, Internet service providers
19    from regulating it.  So their issue or their whole talk
20    was about we need to keep the Internet open and free
21    instead of having various tiers of regulation on the
```

```
 1   Internet.
 2        Q.      And what was the purpose of the presentation?
 3                MR. HURLEY:  Objection, ma'am.  Hearsay.
 4                THE COURT:  Establish a foundation and his
 5   personal knowledge.
 6                MR. Von ELTEN:  It goes to the effect on
 7   listener.
 8                THE COURT:  What was the question?
 9                MR. Von ELTEN:  What was the purpose of the
10   presentation?
11                THE COURT:  Ask for the foundation of
12   knowledge.  How does he know that?
13   BY MR. Von ELTEN:
14        Q.      How do you know that?
15        A.      How do I know what the purpose is?  Because
16   there's a summary of the talk before I went and I had
17   done some research about that topic.
18        Q.      And where --
19                THE COURT:  Overruled.
20        Q.      Are where did you do your research?
21        A.      Research just on the open Internet.
```

1   Q.   And what was the purpose of the presentation?

2   A.   It was more about awareness, I remember that

3 one. It was in English. The speaker was making a case

4 for global open Internet, but specifically for some of

5 the issues coming up in France at the time.

6   MR. HURLEY: Again, ma'am, hearsay. He's

7 just repeating what the presenter told him.

8   THE COURT: What are you offering it for?

9   MR. Von ELTEN: I'm offering it for, it goes

10 to explain why he wrote his report.

11   THE COURT: Overruled.

12 BY MR. Von ELTEN:

13   Q.   Let's talk about the WikiLeaks presentation.

14 What room was that in?

15   A.   It was in one of the larger conference rooms.

16   Q.   About how many people attended the talk?

17   A.   That one was probably closer to a thousand. I

18 remember it being pretty full.

19   Q.   Who gave the talk?

20   A.   The talk was given by Julian Assange.

21   Q.   And how long did Mr. Assange speak?

1   A.   It was about an hour or so.

2   Q.   And how was the talk relevant to your work at

3   the time in the Marines?

4   A.   It was relevant in the sense that I worked

5   with classified information at the time.

6   Q.   And what was the purpose of the talk?

7   A.   The main purpose of the talk was really to

8   explain what WikiLeaks was and the launch of their,

9   basically their new site is what I got from it. They

10 talked about what their intentions were and then

11 basically what the system provided.

12   Q.   And what were their intentions?

13   A.   The intentions were they basically were

14 eliciting support from the audience and then I guess

15 anybody listening to the conference to leak any type of

16 information, not only classified information but

17 proprietary trade secrets, anything of that nature.

18   Q.   I am retrieving prosecution exhibit 43 for

19 identification, hand this to the witness.

20   Do you recognize the document I've handed

21 you?

1   A.   Yes, sir.

2   Q.   What is it?

3   A.   This is my trip report, after action report I

4 wrote after I came back from the conference.

5   Q.   When did you write it?

6   A.   I wrote it approximately a week after.

7   Q.   How do you know it's your report?

8   A.   Well, it has my name on it and it's in the

9 format I'm used to.

10   Q.   Where did you submit it?

11   A.   Where did I submit it? I submitted it to

12 basically my chain of command when I got back.

13   Q.   Retrieving prosecution exhibit 43 for

14 identification.

15   Retrieving prosecution exhibit 85.

16   Would you please take a minute to review

17 1A12? I believe it's on the second page.

18   A.   Okay.

19   Q.   How often were your reports posted online?

20   A.   How often were they posted? Good question

21 because we had just implemented a new system, so we

1   didn't really have a frequency of necessarily posting

2   them, a standard procedure for that. Since that new

3   system, it was kind of became a de facto practice of

4   posted after the trip.

5   Q.   And where were they posted?

6   A.   We posted to a Sharepoint portal.

7   Q.   And what was the address of that Sharepoint

8   portal?

9   A.   It was something along the lines of M F E dot

10 USMC dot smil dot mil. And then your various section be

11 denoted by a G representing and then a number.

12   Q.   Is that approximately the address (INAUDIBLE)?

13   A.   Yes, sir.

14   MR. Von ELTEN: Retrieving prosecution

15 exhibit 85.

16   Your Honor, the United States would move to

17 enter prosecution exhibit 43 for identification into

18 evidence.

19   MR. HURLEY: No objection, ma'am.

20   THE COURT: May I see it, please?

21   Prosecution exhibit 43 for identification is

 1 admitted.

 2 BY MR. Von ELTEN:

 3   Q.   Let's talk a little bit about this report.

 4 How did you organize the report?

 5   A.   I organized it basically chronologically so

 6 the talks I went to, that's the first talk, and then so

 7 on and so forth throughout the report.

 8   Q.   What information did you put in the summary

 9 section?

10   A.   The summary was generally a description

11 basically from the conference itself, and then if there's

12 anything I needed to add to make it, to make it make more

13 sense to my chain of command.

14   Q.   And what was, how did you construct the

15 sections?

16   A.   The analysis was based off of some of the

17 analytical work I had done in our section and also trying

18 to make that analysis fit within our organization

19 basically.

20   Q.   What was the purpose of the counter measure

21 section?

1   A.   That was basically -- the purpose behind that

2   was to identify if there was a potential threat, security

3   threat that maybe we were vulnerable to, and then to see

4   if we could actually fix it, fix that vulnerability.

5   Q.   What was the purpose of drafting this report?

6   A.   To basically summarize the trip so I could

7   show the command actually what I did there, and then also

8   to raise some awareness as far as what the issues I found

9   there were.

10   MR. Von ELTEN: Thank you.   No further

11   questions, Your Honor.

12   THE COURT: Cross examination.

13   MR. HURLEY: Yes, ma'am.

14   CROSS EXAMINATION

15   BY MR. HURLEY:

16   Q.   Staff Sergeant Hosburgh, good morning.

17   A.   Good morning, sir.

18   Q.   When it comes to the document that you were

19   just discussing with Captain von Elten, that's a document

20   that you wrote?

21   A.   Yes, sir.

```
 1        Q.      By yourself?

 2        A.      Yes, sir.

 3        Q.      And it appears to be a reflection of your time

 4   spent at this conference that you discussed with Captain

 5   von Elten?

 6        A.      Yes, sir.

 7        Q.      It was rendered chronologically?

 8        A.      Yes, sir.

 9        Q.      The first thing that you covered was net

10   neutrality?

11        A.      Yes, sir.

12        Q.      Then WikiLeaks?

13        A.      Yes, sir.

14        Q.      Then you'll forgive my computer ignorance,

15   exposing crypto bugs through reverse engineering?

16        A.      Yes, sir.

17        Q.      And that was followed by some other more

18   technical topics of the conversation?

19        A.      Yes, sir.

20        Q.      And you started with paragraph one, as you

21   were writing you started with paragraph one?
```

```
 1        A.        Yes.

 2        Q.        And you wrote your report chronologically as

 3   well?

 4        A.        Chronologically, yes, sir.

 5        Q.        In your discussion of net neutrality you

 6   mentioned terrorist use of the Internet?

 7        A.        Yes, sir.

 8        Q.        And you mentioned that in paragraph one?

 9        A.        Yes.

10        Q.        In your discussion of WikiLeaks you did not

11   mention terrorism or terrorist use of that site, correct?

12        A.        Correct, sir.

13        Q.        Now, let's talk about WikiLeaks; the presenter

14   you said was Julian Assange?

15        A.        Yes, sir.

16        Q.        And he did not mention terrorism in his

17   presentation?

18        A.        Not that I can recall, sir.

19        Q.        Or a desire to help terrorists?

20        A.        No, sir.

21        Q.        That would have been reflected in your report?
```

```
 1        A.      Yes, sir.

 2        Q.      WikiLeaks was focused on the public and the

 3   public's access to information?

 4        A.      Yes, sir.

 5        Q.      Insuring openness?

 6        A.      Yes, sir.

 7        Q.      And keeping the public well informed?

 8        A.      That's what he said, yes, sir.

 9        Q.      And it wasn't exclusively focused on the

10   United States?

11        A.      It wasn't.  They did mention, there was more

12   of an emphasis for classified information, however.

13        Q.      But it wasn't exclusively focused on

14   classified information?

15        A.      Correct, sir.

16        Q.      They were interested in trade secrets?

17        A.      Yes, sir.

18        Q.      And other corporate information?

19        A.      Yes.

20        Q.      So you mentioned, let's go back to that

21   paragraph one, terrorists and the use of the Internet.
```

1 You indicated that terrorists use the Internet?

2   A.   Yes, sir.

3   Q.   To communicate with each other?

4   A.   Yes.

5   Q.   You indicated that an open Internet allows for

6 hidden communication?

7   A.   I believe I recall that, sir.

8   Q.   It's sort of a, you created this idea that an

9 open network allows for terrorist communication on the

10 Internet.

11   A.   Yes, sir, I did.

12   Q.   Their communication with each other?

13   A.   Yes.

14   Q.   From one terrorist to another, and then

15 potentially from there to yet another terrorist?

16   A.   Yes, sir.

17   Q.   And the point as I understood it -- now, when

18 there was a discussion of net neutrality, did the

19 individual giving the net neutrality talk discuss

20 terrorism?

21   A.   No, sir. That was more of an analytical

1   piece.

2   Q.   Right. And what you were trying to show in

3   your analysis was essentially a cost benefit, right?

4   A.   Trying to show that if it was open, that

5   communication could still exist, yes, sir.

6   THE COURT: What communication?

7   THE WITNESS: Communication between the

8   terrorists. Generally speaking, that's a very general

9   term.

10   BY MR. HURLEY:

11   Q.   Right. And your point was that applying

12   filters to the Internet to make it less unneutral, to use

13   that expression, that would, you weigh what you get from

14   it with limiting terrorist communication against the

15   costs associated with making it less neutral?

16   A.   Not necessarily a cost in my mind. They did

17   talk about costs. It was more along the lines of if it's

18   so restricted, they'll just find another communication

19   medium.

20   Q.   And in your report you did mention that that,

21   this making the net less neutral would cost money?

1   A.   Yes, sir.

2   Q.   And you indicated also in your report that

3 there would be the potential for it impinging on the free

4 flow of speech?

5   A.   Yes, sir.

6   Q.   In your report what you didn't say is that

7 terrorists used the Internet to gather information; is

8 that idea reflected in your report?

9   A.   Not specifically, but maybe more as a

10 (INAUDIBLE), yes, sir.

11   Q.   And you didn't say that they used the Internet

12 to gather information from open source reporting?

13   A.   Not specifically.

14   Q.   And you didn't say that they used the Internet

15 or they use any specific website for this open source

16 collection?

17   A.   Correct.

18   Q.   The thrust of your point as you were talking

19 about net neutrality was terrorists and hiding their

20 communication on the Internet?

21   A.   Yes, sir. Well, generally.

1   Q.   You were involved in military intelligence

2 while you were on active duty in the Marine Corps?

3   A.   Yes, sir.

4   Q.   And how long were you at intel in CO when you

5 were in the Marine Corps?

6   A.   Approximately about three years.

7   Q.   And you're familiar with the term intelligence

8 gaps?

9   A.   Yes, sir.

10   Q.   And an intelligence gap is something we don't

11 know?

12   A.   More or less, yes, sir.

13   MR. HURLEY: No further questions, ma'am.

14   THE COURT: Redirect?

15   MR. Von ELTEN: Nothing, ma'am.

16   THE COURT: All right. Temporary or

17 permanent excusal?

18   MR. Von ELTEN: Temporary.

19   THE COURT: All right. Staff Sergeant

20 Hosburgh, you are temporarily excused. Please don't

21 discuss your testimony or knowledge of the case with

1   anyone other than the accused or the lawyers in the case

2   while the trial is still going on.

3   I do have a question for the government. I'm

4   looking at government exhibits 43 and 44, they appear to

5   be the same thing, one is redacted and one is not.

6   MR. FEIN: Yes, ma'am.

7   THE COURT: I have a motion for prosecution

8   exhibit 43. Is that the intent?

9   MR. FEIN: The intent was to use it as a

10 substitute, yes, ma'am.

11   Ma'am, read a stipulation of expected

12 testimony for Lieutenant Commander Thomas Hoskins, United

13 States Navy Reserve dated 10 June 2013.

14   THE COURT: What exhibit is that?

15   MR. FEIN: Yes, ma'am. Prosecution exhibit

16 111 Bravo, the unclassified redacted version.

17   It is hereby agreed by the Accused, Defense

18 Counsel, and Trial Counsel, that if Lieutenant Commander

19 Thomas Hoskins, United States Navy Reserve, were present

20 to testify during the merits and pre-sentencing phases of

21 this court-martial, he would testify substantially as

47

1 | follows:

2 | One. I am a Lieutenant Commander in the

3 | United States Navy Reserves. As a reservist, I am

4 | currently assigned to United States Pacific Fleet. In

5 | 1997, I obtained a BS in Marine Transportation and a BS

6 | in Environmental Science from the Massachusetts Maritime

7 | Academy. In 2007, I obtained a Masters of Business

8 | Administration from the Naval Postgraduate School.

9 | Two. I entered active duty in the United

10 | States Navy in 1998 and left active duty in 2009.

11 | While on active duty, I was an F-18 pilot. I joined

12 | the United States Navy Reserves in 2009. I have

13 | logged over 1700 hours as a pilot, to include

14 | approximately 320 hours of combat flight time. I

15 | have completed the requisite training, to include six

16 | weeks of ground school, one year of primary training

17 | for preliminary flight instruction, one year of

18 | specialty training after I selected intermediate

19 | training, and eight months of advanced training in

20 | weapons, formation flying, and carrier landing.

21 | After completing that training, I was

1 selected to fly F-18s and received my wings.

2 Thereafter, I completed one year of F-18 training

3 where I received additional training in weapons

4 usage, high and low level deployment of bombs, and

5 carrier flying.

6   As a pilot, I have served as an F-18

7 division combat lead. I have operated weapons while

8 deployed in Afghanistan and conducted reconnaissance

9 while deployed in Iraq. I have deployed three times

10 in 2001-02, 2003-04, and 2008 in support of Operation

11 Enduring Freedom and Operation Iraqi Freedom. I have

12 also served as a flight instructor for three years.

13   Three. As a reservist, I currently work

14 on planning, which involves concept plans, operations

15 plans, and execution orders. After leaving active

16 duty in 2009, I began to work at Booz Allen as a

17 contractor. Today, I work as a maritime planner for

18 Booz Allen. Previously, I worked for Booz Allen on

19 matters related to United States Northern Command

20 USNORTHCOM maritime division. Currently at Booz

21 Allen, I work on USNORTHCOM J6 security cooperation.

1 In my work for the J6, I work on security cooperation

2 between the United States and Mexico. Specifically,

3 I work on command and control of communications,

4 computers, and information, C4I.

5   Four. I have worked with classified

6 information in my career with Booz Allen and as an

7 active duty and reservist pilot. As a pilot, I

8 worked with classified information daily for flights,

9 mission planning, mission briefing, and certain

10 information about the planes. Previously, I worked

11 with classified information in my work at Booz Allen

12 in the J5 pertaining to homeland defense plans, and

13 planning and development of specific plans for

14 maritime activities, to include work with the United

15 States Coast Guard. I have received a one and one

16 half hour PowerPoint training on classification

17 procedures and spent about an hour quarterly on

18 training. I have received derivative classification

19 training. I have also used classification guides in

20 my work; I have used the USNORTHCOM classification

21 guide to determine the classification status of

1   Information. I did not consider the following when

2   making any determination: One. What, if any,

3   Of this material was included in open source

4   reporting and, two, what, if any, of this material

5   was available in unclassified publications, such as

6   Army Regulations or Field Manuals.

7   Five. In 2011, I was mobilized to United

8   States Central Command, USCENTCOM. I was mobilized

9   to the J5 planning office, Yemen Branch. While in

10 this position, I worked on country-to-country action

11 plans and worked with the United States Embassy in

12 Yemen and the Yemeni military on plans and security

13 cooperation.

14   Six. While mobilized at USCENTCOM, I was

15 tasked though the Task Management Tool to conduct a

16 review for classified information. The J5 office

17 plans through the director, who receives taskers.

18 The director passed the tasker to me. I received the

19 submitted documents from the USCENTCOM JAG office.

20 My assignment required me to determine whether the

21 submitted documents contained classified information

1 at the time they were compromised.

2   Seven. In my capacity as the person

3 tasked with reviewing the submitted documents, I

4 reviewed the documents for classified USCENTCOM JS

5 equities. I reviewed approximately 40 documents

6 peliaining to United States v. Private First Class

7 Bradley Manning, which the prosecution provided to

8 USCENTCOM. The documents provided by prosecution,

9 submitted documents, included, among others,

10 documents from the Combined Information Data Network

11 Exchange Afghanistan, CIDNE-A, and other documents

12 related to the AR I 5-6 investigation of the Farah

13 incident.

14   Eight. When conducting the review, I

15 looked at USCENTCOM classification guides and

16 Executive Order 13526 and its predecessors. I

17 reviewed each submitted document line by line for

18 classified information by applying the USCENTCOM

19 classification guides. I annotated the basis for

20 each classification decision in my sworn declaration

21 dated 21 October 2011, Bates numbers:

1   00527378-00527397. Prosecution Exhibit 87 for

2   identification is this declaration. All documents

3   noted in the declaration contained classification

4   markings and were properly classified at least at the

5   SECRET level, hereinafter "reviewed documents".

6   Nine. Based on my military experience, I

7   had prior familiarity with the types of documents and

8   information I reviewed. During my deployments, I

9   worked with similar classified information pertaining

10 to mission planning, mission details, weapons

11 systems, and maps of troop locations.

12   Ten. The reviewed documents consisted of

13 documents collected from CIDNE-A and other documents

14 related to the Farah investigation. The reviewed

15 documents contained military information, to include

16 military plans, weapons systems, or operations;

17 significant activity reports, SigAct; operational

18 code words when identified with mission operations;

19 SigActs related to fact of and general type of

20 improvised explosive device (IED) attack at specific

21 location on specific date, which would have been

1 known by the enemy that was the subject of that

2 report; participating units, and details of movements

3 of US friendly forces; concept of operations

4 (CONOPS), Operation Orders (OPORD), or Fragmentary

5 Orders (FRAGOs); vulnerabilities or capabilities of

6 systems, installations, infrastructures, projects,

7 plans, or protection services relating to national

8 security; and limitations and vulnerabilities of US

9 forces in combat area.

10   CONOPs are properly classified as

11 confidential upon execution and can be declassified

12 one year after completion. Participating units,

13 including types, vulnerabilities, locations,

14 quantities, readiness status, deployments,

15 redeployments, and details of movement of U.S. and

16 friendly forces in operations can be properly

17 declassified upon execution.

18   Eleven. I reviewed and determined that

19 21 SigActs from CIDNE-A contained classified

20 information according to the classification guides

21 and my knowledge and experience. These reviewed

1 | SigAct reports from CIDNE-A were all marked as

2 | Secret. The reviewed SigActs from CIDNE-A contained

3 | multiple forms of military information, to include

4 | information related to deploying quick response

5 | forces and code words, reported the effectiveness of

6 | IED attacks, which would be known to the enemy that

7 | was the subject of that report, report the locations

8 | of IED attacks, which would be known to the enemy

9 | that was the subject of that report, identified IED

10 | tactics, techniques and procedures (TIPs) for

11 | responding to IED attacks, identified TIPs for

12 | identifying and neutralizing IEDs, friendly action

13 | reports of finding and clearing caches, weapons

14 | systems and capabilities, sources and methods of

15 | Intelligence engagement, rules of engagement, CONOPS,

16 | descriptions of United States forces, TIPs for

17 | mission execution, anticipated enemy reaction,

18 | flexible deterrent options, code words, assistance by

19 | local foreign nationals in locating suspects, and

20 | details of enemy attacks.

21 | CONOPs are properly classified as

 1   Confidential upon execution and can be declassified

 2   one year after completion. Participating units,

 3   including types, vulnerabilities, locations,

 4   quantities, readiness status, deployments,

 5   redeployments, and details of movement of U.S. and

 6   friendly forces in operations can be properly

 7   declassified upon execution. The 21 CIDNE-A reports

 8   that contained J5 equities are located in Appellate

 9   Exhibit 501 and have the Bates numbers

10   00377846-00377846 and 00377888-00377910. These

11   CIDNE-A reports are contained within

12   PE 89 for identification.

13   Twelve. Additionally, I reviewed the AR

14   15-6 investigation into a military operation that

15   occurred in Farah province, Afghanistan on or about 4

16   May 2009. The AR 15-6 investigation into the Farah

17   incident was focused on investigating the

18   circumstances surrounding a large-scale civilian

19   casualties (CIVCAS) incident. The incident occurred

20   in Gharani, which is a village in Farah Province,

21   Afghanistan. As noted in PE 90 for identification, I

1 found that 13 of the Farah investigation documents

2 contained classified information I believed to be

3 sensitive and classified because the documents reveal

4 TIPs, troop movements, close air support, troops in

5 combat (TIC), and graphics showing troop movements.

6 The Farah investigation documents that contained J5

7 Equities are located in AE 501 and have the Bates

8 numbers 00377425-00377480, 00377496, 00377627,

9 00377672-00377674 00378029, 00378066, 00378071,

10 00378079, and 00378082. These documents are

11 contained within PE 90 for ID.

12   Thirteen. I reviewed PE 66 for ID, a CD

13 contained the video named "BE22 PAX.wmv". This

14 video, Gharani video, is a video depicting portions

15 of a military operation in Farah Province,

16 Afghanistan, separately from the review I conducted

17 for classified USCENTCOM J5 equities.

18   Fourteen. While on active duty from

19 2007-09, I was the strike operations officer

20 responsible for planning, training, coordinating air

21 wing and air-to-ground operations, which involved

 1   coordinating with the Army ground liaison for mission

 2   coordination of ground targets. In this capacity I

 3   reviewed video recordings of combat missions. The

 4   videos captured flight operations using forward

 5   looking infrared radar (FLIR). I reviewed the videos

 6   to ensure the mission achieved its goal, hit the

 7   target, or reviewed the information captured in a

 8   reconnaissance capacity. I reviewed hundreds of

 9   these videos for validation. The Gharani video is

10   similar to the hundreds of videos I reviewed as a

11   strike operations officer.

12   Fifteen. I reviewed the Gharani video

13   for sensitive military information. I relied on my

14   experience while conducting my review for sensitive

15   and classified information of the Gharani video. In

16   particular, I relied on my training and schooling,

17   experience as a flight instructor, experience with

18   operating FUR systems, and experience reviewing

19   videos that record imagery as presented in the FUR

20   system.

21   After my review of the above referenced

1   documents for USCENTCOM J5 equities, I forwarded my

2   conclusions and recommendations to Deputy Commander,

3   USCENTCOM, an Original Classification Authority for

4   his final determination as to whether the information

5   is properly classified.

6   Your Honor, the United States moves to

7   admit prosecution exhibit 87 for identification as

8   prosecution exhibit 87.

9   MR. HURLEY: No objection.

10   MR. FEIN: And the United States moves to

11 admit prosecution exhibit 66 for identification as

12 prosecution exhibit 66.

13   MR. HURLEY: No objection.

14   THE COURT: All right. Both exhibits are

15 admitted.

16   May I see prosecution exhibit 66, please?

17   All right. Prosecution exhibits 66 and 87

18 are admitted.

19   MR. FEIN: Ma'am, the United States requests

20 a brief comfort break.

21   THE COURT: All right. Any objection?

```
 1              MR. HURLEY:  No, ma'am.

 2              THE COURT:  Court is in recess until 20

 3   minutes to eleven.

 4              (BRIEF RECESS.)

 5              THE COURT:  Is the government ready to call

 6   the next witness?

 7              MR. Von ELTEN:  Yes, ma'am.  United States

 8   recalls Special Agent Mander.

 9              Agent Mander, let me remind you you're still

10   under oath.

11   Whereupon:

12                    MARK MANDER,

13   recalled as a witness, having been previously duly

14   sworn according to law, testified as follows:

15              CONTINUED DIRECT EXAMINATION

16   BY MR. Von ELTEN:

17      Q.     What is an IIR?

18      A.     An IIR, that's an acronym, it stands for

19   intelligence information report.

20      Q.     Who creates an I I R?

21      A.     Various military intelligence-like
```

1 organizations throughout DOD as well as other agencies

2 that deal with intelligence typically create them.

3   Q.   What are some examples of some of those

4 agencies?

5   A.   Army military intelligence, the FBI creates

6 them, NCIS, Air Force Office of Special Investigations.

7 There's others.

8   Q.   What types of information do they contain?

9   A.   They contain all types of intelligence

10 information relating to counter terrorism information,

11 things involving cyber activities, as well as things

12 about foreign militaries, things like that.

13   Q.   And who writes them?

14   A.   Typically individuals who are assigned in

15 military intelligence-like units or other intelligence

16 type units that are designated to produce those types of

17 reports.

18   Q.   What is the basis of the content in an IIR?

19   A.   The basis of the contents can be from sources,

20 people that provide information, it can be from other

21 military or intelligence organizations actually observe

1 activities for themselves and they want to report it and

2 that's essentially the mechanism the intelligence

3 community uses to share that information to other

4 elements.

5   Q.   How are they used broadly?

6   A.   Well, there's a system, and I'm not super

7 familiar with it because I do criminal investigation, but

8 generally speaking, someone will produce a report that

9 contains information or intelligence in it. Other

10 elements will then see that report and they can then

11 generate questions or follow-up questions, which then in

12 turn produce more reports.

13   Q.   And how are they organized?

14   A.   Can you be more specific?

15   Q.   Is it like a fact summary, an analysis

16 section, does it vary?

17   A.   It probably varies. It depends on the nature

18 of the information. Sometimes they're very short, maybe

19 like just one or two pages, sometimes they're very long,

20 multiple pages and they are kind of organized in, they

21 usually have across the top like a classification, shows

1   the section of the distribution of who gives the report.

2   MR. TOOMAN: Your Honor, we'll object based

3   on the record. The witness has said he's not super

4   familiar with this process to use his words, so we would

5   object on personal knowledge.

6   A.   I have seen many intelligence reports, but I

7   don't know all about the process of how they're created.

8   THE COURT: All right. Then stop asking

9   about the process of how they're created. Sustained.

10 BY MR. Von ELDEN:

11   Q.   Where do you find IIRs?

12   A.   There's two systems that I would use to look

13 up IIRs. I believe I can name the two systems here. One

14 of them is called Hot R, H O T R, and I don't know what

15 that acronym stands for or if it stands for anything, and

16 then there's another system called the Multi Media

17 Manager, or they typically call it M3. I know that

18 there's others.

19   Q.   What are some of the others?

20   A.   I don't know the others, I just know that

21 there are others and that certain systems are based on

```
 1   like the organizations that produce the reports.  So, for

 2   example, the DOD reports, most of them are in Hot R, but

 3   if you want to see a report that was published by another

 4   organization such as like the FBI, you would use M3.

 5        Q.     What search engine do you use to search for

 6   IIRs?

 7        A.     Intelink is one of the systems you can use to

 8   search.

 9        Q.     Do you use Intelink to search for IIRs?

10        A.     Occasionally.  Typically you can also log into

11   one of the systems I mentioned and then search for the

12   IIRs that way as well.

13        Q.     How are the results displayed in Intelink?

14        A.     They're typically displayed kind of similar to

15   what Google looks like, somewhat similar.

16        Q.     And when have you used IIRs?

17        A.     Well, specifically in this case we did look

18   for IIRs that related to WikiLeaks, that keyword.

19        Q.     Retrieving prosecution exhibit 99 for

20   identification.  Hand this to the witness.

21                    THE COURT:  Just a minute.  Yes.
```

```
 1   BY MR. Von ELTEN:

 2        Q.       What have I handed you, Agent Mander?

 3        A.       This appears to be, excuse me, declassified

 4   version of an IIR specifically related to the WikiLeaks

 5   organization.

 6        Q.       And what is it numbered?

 7        A.       The number is IIR 5391001408.

 8        Q.       And what is the numbering convention based on

 9   your experience?

10        A.       The numbers are broken by spaces.  The first

11   number, five, I believe that indicates the general

12   organization such as Army, Navy, Air Force.  The second

13   number is a three digit number, 391, would be the

14   specific organization within that service.  The fourth

15   set or, excuse me, third set of numbers, it's a four

16   digit number, 0014, would be the serial number of the

17   report.  And then the last two numbers, 08, would be the

18   year, the two digit year of the report.

19        Q.       Would you please take a moment to review the

20   report?

21        A.       Okay.
```

1   Q.   What's an overview of the content?

2   A.   Generally speaking, the content of this IIR,

3   it more or less spells out that the WikiLeaks

4   organization was established in December 2006. Its point

5   was to encourage the posting of sensitive government and

6   corporate documents. Describes the organization as a

7   uncensorable Wikipedia for untraceable mass document

8   leaking and analysis. And it also goes through, gives

9   more details as well as mentions a large number of what

10   we call mirror sites and it gives a long list of it.

11   MR. TOOMAN: We'll object based on relevance,

12   Your Honor.

13   MR. Von ELTEN: Your Honor, I'm just having

14   him lay foundation for the relevance of the document.

15   THE COURT: What's the relevance?

16   MR. Von ELTEN: I'm going to do that right

17   now.

18   THE COURT: I want you to tell me.

19   MR. Von ELTEN: Sorry, ma'am. The relevance

20   is this document, it was a document searched for by PFC

21   Manning on Intelink.

1   THE COURT: Overruled.

2   MR. Von ELTEN: Retrieving prosecution

3 exhibit 99 for identification from the witness and

4 handing the witness prosecution exhibit 85.

5   THE COURT: That's now for identification,

6 right?

7   MR. Von ELTEN: Yes, ma'am.

8   THE COURT: Just a minute.

9   MR. Von ELTEN: I hand you what is marked as

10 prosecution exhibit 85.

11   THE COURT: For identification?

12   MR. Von ELTEN: No, ma'am.

13   THE COURT: It's admitted?

14 BY MR. Von ELTEN:

15   Q.   Please review line 19.

16   THE COURT: Stop there for just a moment. I

17 want to check with the court reporter for the

18 admissibility, prosecution exhibit 85 admitted?

19   Go ahead.

20   Q.   Where was the search conducted?

21   MR. TOOMAN: Your Honor, the defense is going

```
 1   to object.  I believe that this exhibit is computer logs.

 2   This isn't a computer expert.  The government has not

 3   admitted foundation that this witness can interpret raw

 4   data.

 5                    THE COURT:  Lay a foundation.

 6   BY MR. Von ELTEN:

 7        Q.     Agent Mander, what is your position?

 8        A.     I'm a special agent with the Army CID,

 9   specifically the computer crime investigative unit.

10        Q.     And what type of computer crimes do you

11   investigate?

12        A.     Generally speaking, we investigate network

13   intrusion type incidents.

14        Q.     Do you review computer logs as part of that

15   work?

16        A.     Yes, we do.

17        Q.     And what is a log?

18        A.     A log file is basically a list of activity

19   that is recorded typically by a computer or other types

20   of systems that show what activities occurred.

21        Q.     And what kind of activities are recorded?
```

1   A.   Typically the accesses to a computer system or

2 perhaps maybe traffic that transits Internet device such

3 as a router or switch, stuff like that.

4   Q.   And how often do you review computer logs?

5   A.   I used to review them all the time. Now not

6 so much, but I still see them fairly frequently.

7   Q.   And how familiar are you with computer logs?

8   A.   Fairly familiar.

9   THE COURT: Overruled.

10   MR. TOOMAN: Your Honor, the defense would

11 request the opportunity to voir dire this witness about

12 his knowledge of how computer logs are created.

13   THE COURT: All right. I'll let you go ahead

14 and do it. Are you finished laying the foundation or do

15 you have more foundation questions?

16   MR. Von ELTEN: Just a little more, ma'am.

17   THE COURT: Go ahead.

18 BY MR. Von ELTEN:

19   Q.   What was the source identified in line 19?

20   THE COURT: Wait a minute. Now he's

21 interpreting the logs. Do you have foundation to lay

```
 1   with respect to --

 2   BY MR. Von ELTEN:

 3       Q.      What is the search reflected in the log?

 4               MR. FEIN:  Ma'am, may I have a moment?

 5               THE COURT:  Yes.

 6               (DISCUSSION OFF THE RECORD.)

 7               MR. Von ELTEN:  I'm done laying a foundation.

 8               THE COURT:  Go ahead with the voir dire

 9   respecting foundation.

10                    VOIR DIRE EXAMINATION

11   BY MR. TOOMAN:

12       Q.      Good morning, Agent Mander.

13       A.      Good morning.

14       Q.      Agent Mander, what experience do you have with

15   Intelink?

16       A.      As a user, I've used Intelink to conduct

17   various searches.

18       Q.      Do you know how Intelink was programmed?  Do

19   you know how it operates?

20       A.      Can you be a little more specific?

21       Q.      Do you know how Intelink goes about creating
```

 1 those logs?

 2   A.   I do not know the specifics about that.

 3   Q.   Do you know where Intelink stores its data?

 4   A.   I believe in the local area here in Maryland.

 5   Q.   Okay. Do you have I guess -- what sort of

 6 courses have you taken on computer forensics?

 7   A.   I've taken at least three courses, one offered

 8 by Guidant Software specific to the program that we use,

 9 it's called EnCase, also taken two courses at the Defense

10 Cyber Investigations Training Academy involving some of

11 those same applications as well as other applications.

12   Q.   And -- I'm sorry.

13   A.   I've also taken a large data set acquisition

14 course that involves the acquisition of large amounts of

15 data.

16   Q.   Could you be I guess maybe offer a little more

17 insight into what you learned in the data set acquisition

18 course?

19   A.   Generally speaking, when we conduct

20 investigations there are times where we will need to get

21 information from say a server. Generally a server is a

```
 1  type of computer that will have large amounts of

 2  information on it such as log files as well as storage.

 3  And basically the course taught the students how to

 4  obtain that information and a little bit about how to

 5  interpret it.

 6       Q.     How long was the data set acquisition course?

 7       A.     I'd have to go back and look at my resume.  I

 8  believe it was 40 hours.

 9       Q.     And how much of it was focused on obtaining

10  data from a large data set?

11       A.     I would have to go back and look at the

12  course, what do they call that, the, with, you know, lays

13  out, it's a document that usually lays out how many hours

14  are spent on which thing?  I don't remember.

15       Q.     Syllabus?

16       A.     Yeah, syllabus.  There you go.

17       Q.     Do you recall if the bulk of that course was

18  on how to actually obtain the data?

19       A.     Again, I would have to go back and review the

20  syllabus.

21       Q.     When did you take that course?
```

72

1   A.   I believe that was taken within the last two

2   years.

3   Q.   You talked a little bit at that course you

4   learned about how to interpret data. Did you learn how

5   to interpret Intelink logs?

6   A.   Specifically Intelink logs were not mentioned

7   in the course.

8   Q.   At that course you learned how to interpret

9   logs. Are all logs created equally, that is, do logs for

10 Intelink look the same as logs for Google or logs for

11 ESPN dot com?

12   A.   No. Most logs will have some uniqueness to

13 them, either the formats or the type of data that's

14 contained in the logs. That will be dependent upon where

15 you're obtaining the logs from.

16   MR. TOOMAN: Your Honor, we have no further

17 questions, but we would renew our objection as to this

18 witness's knowledge of Intelink logs and their

19 interpretation.

20   THE COURT: All right. Thank you. It's

21 overruled. Proceed.

```
 1                    CONTINUED DIRECT EXAMINATION
 2   BY MR. Von ELTEN:
 3        Q.     Agent Mander, what document is reflected in
 4   line 19?
 5        A.     In line 19 there's an IP address followed by a
 6   date and time and then followed by what appears to be the
 7   actual raw data of what looks like it's a search on
 8   Intelink.
 9        Q.     What is the first IP address?
10        A.     In line 19 the IP address is 22.225.41.40.
11        Q.     And what was the search for?
12        A.     The search appears to be for an IIR and it
13   looks like the IIR is the same IIR that you previously
14   showed me.
15                MR. Von ELTEN:  Your Honor, the United States
16   moves to admit prosecution exhibit 99 for identification
17   into evidence.
18                MR. TOOMAN:  No objection.
19                THE COURT:  Prosecution exhibit 99 for
20   identification is admitted into evidence.
21                May I see it, please?
```

1   MR. Von ELTEN: Retrieving prosecution

2   exhibit 85 from the witness.

3   THE COURT: Before you do that, what was the

4   date and time on line 19.

5   THE WITNESS: The date here is, it looks like

6   it's 14 February 2010, and the time is 2334 hours, and it

7   appears to be Greenwich Mean Time or Zulu time.

8   THE COURT: Thank you.

9   BY MR. Von ELTEN:

10   Q.   Handing the witness prosecution exhibit 99.

11   Permission to publish.

12   THE COURT: Go ahead.

13   Q.   Agent Mander, can you please read paragraphs

14   three and four?

15   A.   Paragraph three. It's unclassified for

16   official use only paragraph. It read WikiLeaks

17   submission guides states it, quote, accepts classified

18   censored or otherwise restricted material of political,

19   diplomatic or ethical significance, unquote. The website

20   provides suggestions for the anonymous submission of

21   material and several methods of submitting material for

1   inclusion to an online database. Methods include

2   submission via secure upload, email and via discrete

3   postal network.

4   Paragraph four is an unclassified for

5   official use only marked paragraph. Since December '06

6   numerous classified and FOUO documents have been posted

7   and continue to be available on WikiLeaks dot org site

8   and its mirrors. Some of these postings have garnered

9   the attention of major news media outlets, yet

10   intelligence reporting has largely ignored these leaks.

11   This report is being issued in an attempt to raise the

12   awareness of this threat. Some of the documents

13   discovered on the WikiLeaks website are listed below,

14   colon.

15   Q.   Agent Mander, what is a mirror?

16   A.   As we discussed yesterday, a mirror is like an

17   alternate version of a website that generally reflects

18   the content of the original site.

19   Q.   And what is the purpose of a mirror?

20   A.   Well, there's many purposes. Sometimes use

21   that for redundancy in case the primary website goes

 1 down, you'll have an alternate that users can --

 2   THE COURT: Yes.

 3   MR. TOOMAN: We'll renew our objection from

 4 yesterday that this witness doesn't have personal

 5 knowledge of why a website would use a mirror.

 6   THE COURT: Overruled.

 7   THE WITNESS: So redundancy, or generally

 8 redundancy I guess would probably be the best way to say

 9 it.

10   MR. Von ELTEN: Thank you. No further

11 questions.

12   THE COURT: Cross examination.

13   MR. TOOMAN: Yes, ma'am.

14   CROSS EXAMINATION

15 BY MR. TOOMAN:

16   Q.   Agent Mander, you talked about the Intelink

17 logs and you looked at those. From the Intelink logs you

18 can't tell if prosecution exhibit 99 was printed,

19 correct?

20   A.   That would be correct.

21   Q.   You also can't tell if it was saved, a copy

```
 1    was saved by the user?

 2         A.       That would also be correct.

 3         Q.       You really can't tell if the user of that

 4    particular machine even looked at the document, correct?

 5         A.       That's also correct.

 6         Q.       You talked a little bit about the contents of

 7    that document.  I guess the document talked about

 8    WikiLeaks accepting political, diplomatic and ethical

 9    contributions, correct?

10         A.       Yes.

11         Q.       It didn't talk about accepting contributions

12    that would help a military, correct?

13         A.       Can I see the document again?

14         Q.       I'm going to retrieve prosecution exhibit 99

15    and hand that to the witness.

16         A.       Can you repeat your question?

17         Q.       I'm going to go ahead and retrieve the exhibit

18    from the witness.

19         A.       Is it possible that I can keep this while you

20    ask your question?

21         Q.       Sure.
```

```
 1              You were referred to paragraphs two and three

 2   by the prosecution and they talked about WikiLeaks

 3   accepting political, they wanted things that would be of

 4   political significance, correct?

 5        A.     Correct.

 6        Q.     They be wanted things that would be of

 7   diplomatic significance?

 8        A.     Yes.

 9        Q.     And they wanted things that would be of

10   ethical significance, correct?

11        A.     According to that paragraph.

12        Q.     And nothing in that paragraph suggests that

13   WikiLeaks was wanting contributions that would be of

14   military significance, correct?

15        A.     It doesn't mention military, but it does

16   mention governments and corporations of various

17   countries.

18        Q.     Okay.  Governments and corporations?

19        A.     I guess you could infer military is part of

20   the government.

21        Q.     Okay.  Now, that document talks about a number
```

1 of classified materials that were released by WikiLeaks,

2 correct? You talked about that with the prosecution.

3   A.   It does, yes.

4   Q.   And there's nothing in that document that says

5 that the enemy viewed those releases, is there?

6   A.   If you give me a moment here.

7   Q.   Sure.

8   A.   No, it doesn't specifically mention any

9 enemies having access to the documents.

10   MR. TOOMAN: Okay. I'm going to go ahead and

11 retrieve the exhibit from you, Agent Mander. Thank you.

12 And give that back to the court reporter. And no further

13 questions, ma'am.

14   THE COURT: Redirect.

15   MR. Von ELTEN: Nothing, Your Honor.

16   THE COURT: All right. Temporary excusal?

17   MR. Von ELTEN: Yes, ma'am.

18   THE COURT: Once again, Agent Mander, you're

19 temporarily excused. Same rules apply as before. Please

20 don't discuss your testimony or knowledge of the case

21 with anyone other than counsel or the accused.

 1   MR. FEIN: Ma'am, the United States offers to

 2   read a stipulation.

 3   Ma'am, this is prosecution exhibit 112,

 4   stipulation of expected testimony for Lieutenant Colonel,

 5   Retired, Martin Nehring dated 10 June 2013.

 6   It is hereby agreed by the Accused, Defense

 7   Counsel, and Trial Counsel, that if Lieutenant Colonel,

 8   Retired, Martin Nehring were present to testify during

 9   the merits and pre-sentencing phases of this

10   court-martial, he would testify substantially as follows:

11   One. I am a retired lieutenant colonel in

12   the United States Air Force. I have a BS in Petroleum

13   Engineering from New Mexico Institute of Mining and

14   Technology in 1982. I received a Masters of Public

15   Administration from Troy University in 1995. I began

16   serving on active duty in the United States Air Force

17   in 1985 as a second lieutenant. During my career, I

18   spent 12 years on active duty and 16 years in the

19   California Air National Guard. I retired in 2012.

20   I deployed to Kuwait in 2001 with the

21   Third Army. I also deployed to Kosovo in 2002 for

 1 | weather operations. In 2006, I deployed to

 2 | Afghanistan and ran all weather operations in

 3 | Afghanistan. Throughout my career in the Air Force

 4 | as a trained meteorologist, I possessed a Top Secret

 5 | clearance and handled Top Secret information. I

 6 | handled classified information at the beginning of my

 7 | service in 1985 and had training in how to handle and

 8 | identify classified information. I worked with

 9 | classified information at all times during my

10 | military career.

11 | Two. From 2009 to February 2012, I

12 | worked at United States Central Command, USCENTCOM.

13 | I worked in a Sensitive Compartmented Information

14 | Facility, SCIF, at USCENTCOM. Initially, I worked at

15 | the weather desk. After USCENTCOM discontinued the

16 | weather desk, I was reassigned under the USCENTCOM

17 | Directorate of Operations J3 as the J3 subject matter

18 | expert, SME, for identifying J3 classified equities

19 | within United States Government official

20 | documentation. In this capacity, I was primarily

21 | responsible for reviewing documents being processed

1   under the Freedom of Information Act, FOIA, which

2   belonged to or contained information from USCENTCOM

3   J3. For FOIA requests, I reviewed the requested

4   information for classified information to determine

5   whether the document could be released under the

6   FOIA. Additionally, I conducted review for release

7   of information to family members of service members

8   who were killed, wounded, or kidnapped within the

9   USCENTCOM theaters of operations and the media. I

10   also conducted separate reviews for coalition

11   partners because the standards were different for

12   each. Family members and the media could only

13   receive unclassified information. Coalition partners

14   could receive certain classified information.

15   Classified information in a document could not be

16   released under the FOIA even if the remainder of the

17   document contained publicly available information

18   because the information is still protected.

19   Three. In my capacity as the J3 SME, I

20   reviewed documents pertaining to United States v.

21   Private First Class Bradley Manning, which the

 1 prosecution provided to USCENTCOM. The documents

 2 provided by the prosecution, submitted documents,

 3 included, among others, documents from the Combined

 4 Information Data Network Exchange Iraq, CIDNE-I, the

 5 Combined Information Data Network Exchange

 6 Afghanistan, CIDNE-A, other documents related to the

 7 AR 15-6 investigation of the Farah incident, and a

 8 file named "BE22 PAX.zip" containing a video named

 9 "BE22 PAX.wmv" Gharani video.

10   Four. I was tasked though the J3 Task

11 Management Tool. I received the submitted documents

12 from the USCENTCOM JAG office. My assignment

13 required me to determine whether the submitted

14 documents contained classified information at the

15 time they were compromised. I reviewed the documents

16 for classified USCENTCOM J3 equities.

17   Five. To determine whether submitted

18 documents were classified at the time of compromise,

19 I used three classification guides. I used a

20 USCENTCOM classification guide dated before Operation

21 Iraqi Freedom, the updated version of that USCENTCOM

 1   classification guide dated during Operation Iraqi

 2   Freedom, and the version of the USCENTCOM

 3   classification guide that was current at the time I

 4   conducted the classification review.

 5   I did not consider the following in

 6   making any determination: One, what, if any, of this

 7   material was included in open source reporting; two,

 8   what, if any, of this material was available in

 9   unclassified publications, such as Army Regulations

10   or Field Manuals; and, three, what, if any, of this

11   material may have been shared at the tactical level

12   during the key leader engagements described below.

13   Six. I applied a process-oriented

14   approach toward applying the classification guide to

15   each of the submitted documents. First, I would

16   determine the date of the document and use the

17   classification guide appropriate for each document's

18   date. I would determine the document's

19   classification at the time the document was created.

20   Documents I determined that were unclassified were

21   removed from the collection of submitted documents.

1   In fact, I approached the documents with a "FOIA

2   mindset" and tried to ensure each document was not

3   actually classified. I did not presume any document

4   was classified and reviewed each line in each

5   document for classified information.

6   Seven. Second, I reviewed the document

7   to determine if it was classified at the time of it

8   was compromised according to the appropriate security

9   classification guides. I reviewed documents for

10   USCENTCOM J3 equities. Documents containing

11   intelligence were sent to Mr. Louis Travieso for

12   further review for USCENTCOM J2 equities. I

13   conducted a line by line review and reviewed each

14   document for USCENTCOM J3 equities by applying

15   specific paragraphs of the classification guides from

16   the appropriate time period. Where the reviewed

17   document contained USCENTCOM J3 equities as

18   determined by the appropriate USCENTCOM

19   classification guide, I marked the document as

20   containing information I believed to be sensitive and

21   classified. I annotated the basis for each

1 classification decision in my sworn declaration dated

2 19 October 2011, which is Bates numbers

3 00527370-00527377. Prosecution Exhibit 86 for

4 identification is my declaration. All documents

5 noted in the declaration contained classification

6 markings at the Secret level, hereinafter "J3

7 reviewed documents".

8   Eight. The J3 reviewed documents

9 consisted of documents collected from CIDNE-I,

10 CIDNE-A, other documents related to the Farah

11 investigation, and the Gharani video. The reviewed

12 documents contained military information, to include

13 military plans, weapons systems, or operations;

14 foreign government information; significant activity

15 reports (SigActs); operational code words when

16 identified with mission operations; SigActs related

17 to fact of and general type of IED attack at specific

18 location on specific date; participating units,

19 including types of vulnerabilities, locations,

20 quantities, readiness status, deployments,

21 redeployments, and details of movements of US

1 friendly forces; concept of operations (CONOPS),

2 operation orders (OPORD), or fragmentary orders

3 (FRAGOs); vulnerabilities or capabilities of systems,

4 installations, infrastructures, projects, plans, or

5 protection services relating to national security;

6 and limitations and vulnerabilities of US forces in

7 combat area.

8   Nine. CIDNE-I and CIDNE-A contained

9 SigAct reports. The SigActs were marked as Secret.

10 Within the SigActs, several categories appeared

11 multiple times. These categories include key leader

12 engagements, mission report logs, reports on

13 improvised explosive devices, IEDs, and tactics,

14 techniques, and procedures (TIPs) in response to

15 IEDs, and reports and responses for missions focused

16 on duty status-whereabouts unknown (DUSTWUN).

17   Ten. Key leader engagements described

18 interactions of members of the military with local

19 leaders in Iraq and Afghanistan regarding a broad

20 range of topics. Disclosure of the key leader

21 engagements would reveal foreign government

1   activities, the involvement of service members with

2   local foreign leaders, and the identities of local

3   leaders.

4   Eleven. Mission report logs described

5   troop movements, activities, and engagements with

6   hostile forces. The mission report logs describe

7   tactics, troop locations, weapons and military

8   equipment used.

9   Twelve. IED reports detailed the

10   casualties inflicted on service members, the

11   locations of the attacks, and TIPs for detecting and

12   responding to IED attacks. The IED reports recount

13   the attacks of hostile forces, troop locations, and

14   the capabilities of United States forces.

15   Thirteen. DUSTWUN reports stated the

16   names and other personal information of kidnapped

17   service members and the TIPs in response to locate

18   the kidnapped service member. The DUSTWUN reports

19   state troop locations, tactics, encounters by

20   military forces with hostile forces and foreign

21   nationals.

1   Fourteen. The 53 CIDNE-I reports that

2   contained J3 equities are located in Appellate

3   Exhibit 501 and that have the Bates numbers

4   00377912-00377918, 00377921-0377933, 00377935-

5   00333938,00377940-00377949,00377952-00377958,

6   00377960-00377963,00377965-00377980,

7   00377983-00377986, 00377988-00378013, and

8   00378016-00378026. These CIDNE-I reports are

9   contained within PE 88 for ID. The 36 CIDNE-A

10   reports that contained J3 equities are located in AE

11   501 and that have the Bates numbers

12   00377846-00377846, 00377849-00377856,

13   00377860-00377871, 00377874-0037788,

14   00377886-00377905, and 00377907-00377910. These

15   CIDNE-A reports are contained within PE 89 for ID.

16   Fifteen. The J3 reviewed documents

17   contain SigAct reports from CIDNE-I that I determined

18   contained classified information according to the

19   applicable security classification guides. These

20   SigAct reports from CIDNE-I were all marked Secret.

21   Additionally, the J3 reviewed documents contain

 1 SigAct reports from CIDNE-A that I determined

 2 contained classified information according to the

 3 applicable security classification guides. These

 4 SigAct reports from CIDNE-I and CIDNE-A were all

 5 marked Secret. The J3 reviewed documents within

 6 PE 88 for ID and PE 89 for ID contain multiple forms

 7 of military information, to include but not

 8 Limited to the following: One, threat of attack in

 9 an area by a specific group; two, confirmed that a

10 previously reliable source of intelligence provided

11 information; three involved direct and indirect fire

12 reports; four, reported casualties; five reported

13 loss of equipment; six, stated types of weapons

14 encountered in an enemy engagement; seven, reported

15 the effectiveness of IED attacks; eight, reported the

16 locations of IED attacks; nine, identified JED TIPs

17 for responding to JED attacks; ten, identified TIPs

18 for identifying and neutralizing JEDs; eleven,

19 identified by name suspects in investigations;

20 twelve, identified quick response force mobilization

21 TIPs; thirteen, identified code words; fourteen,

```
 1   involved friendly action reports; fifteen, stated

 2   details of military missions; sixteen, named multiple

 3   enemy groups; seventeen, reported lack of casualties;

 4   eighteen, reported lack of loss of equipment;

 5   Nineteen, identified general enemy TIPs; twenty,

 6   involved an enemy small arms fire report; twenty-one,

 7   identified enemy target by name; twenty-two, stated

 8   effectiveness of enemy actions; twenty-three,

 9   described a military raid; twenty-four, identified

10   sources and methods of intelligence collection;

11   twenty-five, identified responses based on

12   intelligence gathered; twenty-six, detailed arrest of

13   a suspect; twenty-seven, stated detention of a

14   suspect would have a significant impact on military

15   operations; twenty-eight, described friendly action

16   of finding and clearing caches; twenty-nine, involved

17   a border operations report; thirty, described a civil

18   disturbance; thirty-one, identified unit locations;

19   thirty-two, reported enemy casualties; thirty-three,

20   stated planned unit movement; thirty-four, stated

21   details of combat patrols; thirty-five, described key
```

1   leader engagement; thirty-six, assessed effectiveness

2   of local outreach programs; thirty-seven, detailed

3   kidnapping of a service member; and thirty-eight,

4   described initiation of DUSTWUN procedures.

5   Sixteen. Additionally, I reviewed

6   documents from the AR 15-6 investigation into a

7   military operation that occurred in Farah province,

8   Afghanistan on or about 4 May 2009. The AR 15-6

9   Investigation into the Farah incident was focused on

10 investigating the circumstances surrounding a

11 large-scale civilian casualties, CIVCAS, incident.

12 The incident occurred in Gharani, which is a village

13 in Farah Province, Afghanistan.

14   The documents from the AR 15-6

15 investigation that contained J3 equities are located

16 in AE 501 and that have the Bates numbers: 00377425-

17 00377492,00377496-00377498,00377627-00377637,

18 00377674-00377675, and 00378029-00378081. These

19 documents are contained within PE 90 for ID. As

20 noted in PE 90 for ID, I found that these documents

21 contained information I believed to be sensitive

 1 classified because they reveal operational

 2 activities, weapons systems, and code words.

 3   Seventeen. As part of my review of the

 4 Farah documents, I reviewed a file named "BE22

 5 PAX.zip" containing a video named "BE22 PAX.wmv"

 6 hereinafter Gharani video. PE 66 for ID is a

 7 CD that contains both files I reviewed. The Gharani

 8 video depicts portions of a military operation in the

 9 Farah Province, Afghanistan. The Gharani video

10 reveals operational code words associated with the

11 mission. The video also reveals operational

12 activities including troop movements and weapons

13 systems. Finally, the video includes specific

14 information contained on the heads-up display.

15   Eighteen. After my review of the above

16 referenced documents for USCENTCOM J3 equities, I

17 Forwarded my conclusions and recommendations to

18 Deputy Commander, USCENTCOM, an Original

19 Classification Authority, for his final determination

20 as to whether the information is properly classified.

21   Your Honor, the United States moves to

 1   admit prosecution exhibits 88 and 89 for

 2   identification as prosecution exhibits 88 and 89.

 3   MR. HURLEY: No objection, ma'am.

 4   THE COURT: All right. Prosecution exhibits

 5   88 and 89 are admitted. May I see them, please?

 6   Plaintiff's exhibits 88 and 89 are admitted.

 7   MR. FEIN: Ma'am, the United States moves to

 8   admit prosecution exhibits 86 and 90 for identification

 9   as prosecution exhibits 86 and 90.

10   MR. HURLEY: No objection, ma'am.

11   THE COURT: All right. Prosecution exhibits

12   86 and 90 are admitted.

13   MR. Von ELTEN: Your Honor, I have

14   prosecution exhibit of Mr. Jacob Grant.

15   THE COURT: That's 106?

16   MR. Von ELTEN: Yes, ma'am.

17   THE COURT: Proceed.

18   MR. Von ELTEN: It is hereby agreed by the

19   accused, defense counsel and trial counsel that if Mr.

20   Jacob Grant were present to testify during the merits and

21   pre-sentencing phases of this court-martial, he would

 1   testify substantially as follows:

 2   One. I currently serve as Contract Task Lead

 3   for CCJ6, assigned to the Active Cyber Defense Branch at

 4   U.S Central Command's Headquarters USCENTCOM on MacDill

 5   Air Force Base in Florida. In this capacity, I am

 6   responsible for conducting various levels of cyber

 7   operations for USCENTCOM and Overseas Areas of

 8   Responsibility including computer network defense

 9   activities, computer network attack planning and

10   analysis, and the analysis and reverse engineering of

11   computer network exploitation activities in order develop

12   effective countermeasures.

13   I am the lead for our "in-house" Computer

14   Emergency Response Team, CERT. In this capacity, I

15   perform in-depth forensic analysis of CND alerts, flow

16   analysis, or interpretation of threat information to

17   include security compromises, network intrusions, and

18   malicious logic outbreaks. I have held this position for

19   four and a half years. At the time of my involvement in

20   this case, I was the Senior INFOSEC Analyst with the

21   Information Assurance Branch of the J6 USCENTCOM. I have

1   also been an IA watch officer, a senior analyst, and a

2   senior engineer. I served for two years as an enlisted

3   airman working in technical control and network

4   engineering.

5   Two. I am a certified information systems

6   security professional, CISSP, 2008. I have a Top

7   Secret/SCI security clearance. I have associate

8   degrees in Electronic Systems Technology and

9   Avionics Systems Technology. I am a Cisco Certified

10   Network Associate, CCNA, 2003, and a CORE Impact

11   Certified Professional, CICP, 2013. Some of the

12   network security and associated training I have

13   received includes: McAfee Network Security Platform

14   Administration, 2013; ArcSight ESM Use Case

15   Foundations, 2012; EnCase Computer Forensics 1, 2012;

16   Arc Sight Logger 5.0 Administration and Operations,

17   2011; Basic Malware Analysis Using Responder

18   Professional, 2010; Ethical Hacking, 2008; McAfee

19   Host-Based Security Systems, 2007; Information

20   Technology Service Management, ITSM, 2007; and Cisco

21   Securing Networks w/ PIX & ASA, SNPA, 2007.

1   Three. I became involved in this case

2 for two reasons. From 19-20 August 2010, I was

3 involved in the collection and transfer of audit logs

4 from the USCENTCOM SharePoint on the USCENTCOM

5 SIPRNET web server. At this time, I was also

6 involved in the identification, collection, and

7 transfer of information housed within that SharePoint

8 site. Our collection focused on the SharePoint

9 because I had identified it as the location of

10 charged documents based upon the SIPRNET web page

11 address of those documents.

12   Further, Special Agent John Wilbur, with

13 whom I was working, was interested in the contents of

14 the USCENTCOM JAG folder.

15   Four. The USCENTCOM SharePoint server is

16 a tool to create an internet interface that allows

17 users with access to the site on SIPRNET to

18 collaborate, for example, by sharing files. The

19 SharePoint itself is only accessible via SIPRNET, so

20 a user must access it via secure systems. At that

21 time, it was identified at IP addresses

1   131.240.47.23, for the SharePoint database cluster,

2   131.240.47.6, and 131.240.47.7, for the web portal

3   front end or the portion accessible by SIPRNET users.

4   The database as a whole occupied several terabytes of

5   space. The server supporting it, from which I pulled

6   the logs and other information at issue, is

7   physically housed on virtual machines within a

8   cluster, in a data center, on a storage area network.

9   Only authorized USCENTCOM Headquarters J-6 personnel

10   are granted access to the facility. The data center

11   is protected by badge access, cipher locks, video

12   surveillance, and an access roster.

13   Five. The audit logs I referenced herein

14   are Internet Information Systems, IIS, or Windows

15   server log files, which capture the IP address of the

16   USCENTCOM SharePoint server. The logs do not capture

17   any remote or external IP addresses. The logs only

18   capture the dates and times documents are accessed on

19   the SharePoint server, as well as related activity on

20   the SharePoint server.

21   Six. For collection as evidence by SA

1   Wilbur, these logs were pulled by the internet server

2   maintenance team. I know this because I was there

3   when they retrieved the information. These logs

4   saved in a standard text file, or .txt format. I

5   burned these logs onto a hard drive and also onto a

6   DVD. I know these devices were clean of data because

7   I personally wiped all information from the hard

8   drive and laptop, and created the image for the hard

9   drive on which the logs were burned. Further, I

10   performed a hash value match to verify that the logs

11   provided were saved accurately onto the disk. The

12   DVD was red. I marked it with the title CIE

13   underscore USR underscore DATA. This DVD contained

14   the files CENTCOM underscore CIE underscore

15   SharePoint dash HASH underscore MDSSHA1.pdf,

16   CENTCOMHQ underscore CIE underscore SharePoint dash

17   HASH underscore MDSSHA1.txt, web1.zip, and web2.zip.

18   The first two files contain the hash

19   value information validating the accuracy of the log

20   information collected. Web1.zip contained the web

21   log data from 1 December 2009 until 30 July 2010,

 1   pertaining to the USCENTCOM server assigned IP

 2   address 131.240.47.6. Web2.zip contained web log

 3   data from 1 April 2010 until 30 July 2010, pertaining

 4   to the USCENTCOM server assigned to IP address

 5   131.240.47.7. Prosecution Exhibit 108 for

 6   Identification are these SharePoint server logs.

 7   Seven. After burning the log information

 8   to the DVD, I signed the evidence to SA Wilbur using

 9   the provided DA Form 4137 Evidence Property Custody

10   Document. The disk was recorded on a DA Form 4137

11   labeled as document number 122-10. I recognize this

12   as Bates number 00411111. I know this because I

13   signed that form and recognize my signature on it. I

14   would recognize the evidence itself because I wrote

15   the label on the disk and burned it. I did not alter

16   the information or the devices on which it was housed

17   in any way.

18   Eight. The information housed on the

19   SharePoint server, mentioned previously, was accessed

20   via SIPRNET and located in the JAG folder on the

21   USCENTCOM SharePoint page. We collected this

 1   information for two reasons. First, collecting this

 2   information shows what content was originally

 3   available on the USCENTCOM server to SIPRNET users.

 4   Second, this information helps put the log data we

 5   collected into context.

 6   Nine. I assisted SA Wilbur in collecting

 7   this information from the SharePoint server. To

 8   retrieve it, we used two blank CCIU SATA hard drives.

 9   I know these are clear hard drives because, in

10   accordance with USCENTCOM policy, I scanned them for

11   malware and viruses before they were used to gather

12   the evidence. Having found none, I knew they were

13   suitable for evidence collection. To collect this

14   information, we also used an approved CCIU laptop. I

15   hooked this laptop to the SIPRNET using a CCIU-issued

16   USB cable and drive dock. We then connected the

17   previously scanned hard drive to the laptop. SA

18   Wilbur used that connection to recover the

19   information at issue.

20   Ma'am, the United States moves to admit

21   prosecution exhibit 108 for identification as

 1 prosecution exhibit 108.

 2   MR. HURLEY: No objection, ma'am.

 3   THE COURT: All right. May I see it, please?

 4   MR. Von ELTEN: Your Honor, if we may mark

 5 this for the next recess.

 6   THE COURT: That's fine.

 7   MR. Von ELTEN: Your Honor, I have

 8 prosecution exhibit 72 which is the stipulated expected

 9 testimony of special agent John Wilbur.

10   THE COURT: Proceed.

11   MR. Von ELTEN: It is hereby agreed by the

12 Accused, Defense Counsel, and Trial Counsel, that if

13 Special Agent John Wilbur were present to testify during

14 the merits and pre-sentencing phases of this

15 court-martial, he would testify substantially as follows:

16   One. I am currently the senior Special Agent

17 at the computer forensic unit in the office of the

18 Special Inspector General for the Troubled Asset

19 Relief Program, TARP, at the Treasury Department. In

20 this position, I collect and examine digital evidence

21 to support criminal investigations. I have held this

1   position since January of 2012. Previously, I was an

2   SA for the Department of the Army's Criminal

3   Investigation Command, CID, Computer Crimes and

4   Investigative Unit, CCIU. I held that position from

5   June of 2010 to January of 2012. As a CCIU SA, I

6   investigated the unauthorized exfiltration of

7   classified and sensitive data and the loss of

8   personally identifiable information, PII, data

9   worldwide. I also investigated intrusions into

10 Army computer systems. I currently have over twenty

11 years of law enforcement experience, fifteen of which

12 have been primarily devoted to conducting complex

13 criminal and administrative cyber-related

14 investigations.

15   Two. I have had substantial training to

16 qualify me for my position. I received Department of

17 State law enforcement training in 2005, CID law

18 enforcement training in 2002, and Police Officer

19 Training in 1990. In addition to the

20 evidence-handling training included in these courses,

21 I also attended the Advanced Crime Scene

1 Investigations course at the Federal Law Enforcement

2 Training Center in Glynco, Georgia, May 2008.

3   At the time of my involvement in this

4 Investigation, my cyber security and forensic

5 evidence experience was extensive. Among other

6 courses, I had attended multiple courses put on by

7 Guidance Software, the makers of the EnCase forensic

8 tool; I had attended the Seized Computer Evidence

9 Recovery Specialist Certification Course, October

10 2001, at the Federal Law Enforcement Training Center;

11 and I had attended FT210, Windows Forensic

12 Examinations through the Defense Cyber Investigations

13 Training Academy, DCITA. Further, I had obtained

14 training in Law Enforcement Technology, April

15 2002, through the University of Pittsburgh; Advanced

16 Data Recovery, March 2001, and Basic Data Recovery,

17 January 2000, at the National White Collar Crime

18 Center; Operational Information Security I and II,

19 July 2000, at the Defense Information Security

20 Agency; and Computer Search and Seizure, June 2000,

21 through the FBI Academy.

1   I have continued to develop my skills and

2   expertise. I have attended training in Windows 7

3   Forensics at Access Data, December 2010, the Computer

4   Incident Response Course, April 2011, and a course on

5   Introduction to Networks and Computer Hardware,

6   December 2010, through DCITA.

7   Three. My role in this case was to

8   assist in witness interviewing and data collection.

9   I collected evidence from the United States Central

10   Command USCENTCOM server and from the Department of

11   State server.

12   In collecting the USCENTCOM materials, I

13   worked with Mr. Jacob Grant to collect both the

14   server logs as well as information from a particular

15   folder.

16   Four. When collecting and handling

17   evidence, I follow several general procedures. After

18   collection, I review the evidence property custody

19   document for the appropriate information. I fill out

20   the date, time, place of collection and describe the

21   evidence collected. I record, for example, serial

 1 numbers, markings for identification, and condition

 2 description matching the associated evidence.

 3 Further, I ensure that the necessary information,

 4 such as date and time, are properly and accurately

 5 recorded.

 6 Lastly, I maintain secure custody of the

 7 evidence prior to transferring it to another

 8 individual. In addition to following these

 9 procedures, when transferring to or receiving

10 evidence from another person, I am also sure to

11 properly sign, date, and note the reason for the

12 transfer.

13 Five. From the USCENTCOM server, Mr.

14 Grant and I collected information from the

15 USCENTCOM SharePoint site as well as the audit logs

16 which track access to the site. I was interested in

17 this information so that investigators could compare

18 compromised information regarding the Farah

19 investigation to information on the USCENTCOM server,

20 and so that investigators could identify computers

21 which were used to retrieve potentially compromised

 1 material. Before Mr. Grant or I accessed, imaged,

 2 searched for, or extracted any information, we needed

 3 special authorization from MG Jones, Chief of Staff,

 4 USCENTCOM. CCIU forwarded a formal written request

 5 through the Office of the Staff Judge Advocate to the

 6 USCENTCOM J6 requesting release of this evidence on 9

 7 August 2010. This request was approved on 19 August

 8 2010. The same day, I worked with Mr. Grant to

 9 prepare for evidence collection by getting in order

10 the equipment we would need for collection. Mr.

11 Grant ensured that the laptop, hard drive, and cables

12 we would need were clean of any data and ready for

13 use.

14   Six. The following day, Mr. Grant

15 collected from the J6 shop a DVD containing the audit

16 logs for the USCENTCOM SharePoint server. The logs

17 show, among other things, the date and time USCENTCOM

18 documents were accessed on the SharePoint server,

19 from December 2009 until August 2010. On 20 August

20 2010, he signed that evidence over to me. I took

21 possession using the evidence handling procedures I

1   describe herein including, but not limited to,

2   documenting it on an Evidence Property Custody

3   Document DA Form 4137, labeled as document number

4   122-10, Bates number 00411111. Later that same day,

5   I properly signed that evidence over to the CCIU

6   Evidence Custodian, Ms. Tamara Mairena. At no point

7   did I alter the DVD or its contents. I have no

8   reason to believe it suffered damage or contamination

9   in any way.

10   Seven. In addition to collecting the

11 logs, I worked further with Mr. Grant to access and

12 collect information from the USCENTCOM SharePoint

13 collaboration space on the USCENTCOM server.

14 SharePoint is a tool produced by the Microsoft

15 Corporation to create an internet interface which

16 allows users with access to a SIPRNET website to

17 collaborate, for example, by sharing files. The

18 USCENTCOM SharePoint itself is only accessible via

19 SIPRNET, so a user must access it via secure systems

20 and a proper security clearance. The server

21 supporting it, from which Mr. Grant pulled the logs,

1   is on virtual machines within a cluster, in a data

2   center, on a storage area network Only authorized

3   USCENTCOM headquarters J6 personnel are granted

4   access to the facility. The data center is protected

5   by badge access, cipher locks, video surveillance,

6   and an access roster. This information was located

7   on SIPRNET in the JAG folder on the USCENTCOM

8   SharePoint page. Mr. Grant assisted me in locating

9   it on the system. We sat at his workstation to pull

10   the folder contents. We knew where to focus our

11   search based on Mr. Grant's SIPRNET web page address

12   identifications of the information at issue and

13   because investigators in the case had cause to

14   suspect the charged information was housed in the

15   USCENTCOM JAG folder.

16   In consultation with investigating

17   forensic examiner SA Dave Shaver, we determined the

18   most forensically sound way to collect the Farah

19   information itself, as well as information about how

20   it was accessible on SharePoint, was to navigate

21   through the series of digital folders to download the

1 Farah file itself. As we navigated through the

2 folder structure on the SharePoint server, we took

3 screenshots of the contents of each folder before we

4 entered the subsequent folder. A screenshot is the

5 process of obtaining a digital copy of the computer

6 screen, similar to a photograph.

7   Eight. During the morning of 20 August

8 2010, I connected, via a USB cable, a CCIU-issued

9 Voyager drive dock to the laptop which accessed the

10 SharePoint server via a USB cable. I connected a

11 400GB Seagate Barracuda, SATA hard drive, serial

12 number 3NFODYJI, to the laptop using the drive dock

13 and assigned that drive the letter X. Using

14 Microsoft's Internet Explorer, I navigated to the

15 SIPRNET web page www.nonrel.cie.centcom.smil.mil.

16 From this screen, I clicked on the Organization link.

17 I created a screen capture of this page and saved it

18 in a folder in the Desktop Directory called screen

19 shots. From this screen, I clicked on the

20 Special Staff link. I created a screen capture of

21 this page and saved it in the screen shots folder.

 1   From this screen, I clicked on the Judge Advocate

 2   link. I created a screen capture of this page and

 3   saved it in the screen shots folder. From this

 4   screen, I clicked on the JA Document Page link. I

 5   created a screen capture of this page and saved it in

 6   the screen shots folder. From this screen, I clicked

 7   on the folder icon Investigations. I created a

 8   screen capture of this page and saved it in the

 9   screen shots folder. From this screen, I clicked on

10   the folder icon Farah. I created a screen capture of

11   this page and saved it in the screen shots folder.

12   The folder Farah contained the following sub-folders:

13   Admin Material, Briefs, Email, Investigations Tabs,

14   Repotis and EXSUMs, Timelines, and Videos. I

15   navigated to each of the sub-folders and created a

16   screen capture for each page then saved it in the

17   screen shots folder. The screen shots showed how the

18   SharePoint portal was arranged and the path to the

19   Farah folder.

20   Nine. Prosecution Exhibit 65 for

21   identification is a computer printout that shows the

1   file names and their associated paths that we

2   navigated. It is a printout of a directory listing

3   showing the filenames of each file and folder

4   contained within the Farah folder on the USCENTCOM

5   Server with individual line numbers printed to the

6   left of the listing. It lists the first level of

7   subfolders within the Farah folder alphabetically,

8   and then lists the filenames of the first subfolder.

9   The document continues this process of listing

10 subfolder names recursively, until all files and

11 their filenames in all subfolders have been listed.

12   Ten. Later in the day on 20 August 2010,

13 I recreated the folder Farah on the Desktop Directory

14 of the laptop and included all of the subfolders that

15 resided in the Farah folder. I then downloaded each

16 individual file contained in the folder Farah into

17 the same location inside the recreated Farah folder

18 on the Desktop Directory of the laptop computer.

19 After verifying that all of the files downloaded

20 correctly, I installed EnCase version 6.14.3 on the

21 laptop computer. Using EnCase, I created a logical

1 evidence file of the folder Farah and all of its

2 sub-folders. The logical evidence file was named

3 JA-Investigations-Farah Folder.LOI. An MD5 hash of

4 46ell229a5d678cabf9c3fa6839f662c was obtained and

5 recorded. The logical evidence file of the folder

6 Farah was placed in a folder named EnCase on the root

7 of the X drive connected to the laptop. I also

8 copied the recreated Farah folder and all of the

9 sub-folders and placed them onto the root of the X

10 drive. Subsequently, the folder Screen Shots was

11 then copied and placed on the root of the X drive as

12 well.

13   Eleven. When beginning the process of

14 navigating through the JAG folder to obtain the Farah

15 contents, I was not required to enter any login or

16 password window on the main page. I was able to

17 navigate to any page and access all folders and

18 documents in the document library, including the SJA

19 Investigations folder and the Farah folder without

20 ever entering any authentication or credential

21 information. In the Farah folder, all of the video

1 files were password protected, including a file named

2 BE22 PAX.zip containing a video named BE22 PAX.wmv.

3 We therefore also requested and received the password

4 to unlock the file named BE22 PAX.zip and the other

5 videos from USCENTCOM. PE 66 for Identification is a

6 CD containing the file named BE22 PAX.zip and the

7 video file named BE22 PAX.wmv. PE 67 for

8 Identification contains the password for the file

9 named BE22 PAX.zip which I received from USCENTCOM.

10   Twelve. Later on 20 August 2010, I

11 connected a second 400GB Seagate Barracuda, SATA hard

12 drive, serial number 3NFOHTG4, to the laptop using

13 the drive dock and assigned that drive the letter Y.

14 I then recreated the process a second time placing

15 the folder EnCase, containing the EnCase logical

16 evidence file for the folder Farah, the recreated

17 folder Farah, and the folder Screen Shots onto the

18 root of the Y drive. The second evidence drive was

19 created as a backup in case the first evidence drive

20 suffered a failure.

21   Thirteen. I later collected as evidence

1 two SATA hard drives. These SATA hard drives each

2 contained images of three folders, EnCase, Farah, and

3 Screen Shots, copied from the USCENTCOM SharePoint

4 server IP address 131.240.47.23, which was documented

5 on Evidence Property Custody Document, Document

6 Number 123-10, identified at Bates number 00411113.

7 In processing this material, I handled and

8 transferred the evidence as I have been trained. At

9 no point did I alter any evidence I collected. I

10 have no reason to believe this evidence was

11 contaminated or damaged in any way. On 20 August

12 2010, I properly signed this evidence over to Ms.

13 Tamara Mairena, the CCIU Evidence Custodian. I did

14 not touch this evidence again.

15   Fourteen. Finally, I took possession of

16 firewall logs from the Department of State from SA

17 Ron Rock. I took possession of this evidence on 15

18 October 2010. He provided this information on a

19 silver CD marked with the words WikiLeaks DoS

20 Firewall Logs 13 October 2010. The CD had a red

21 U.S. Government Secret sticker on it. I recognize it

     1   as an official sticker because I have handled

     2   classified information before. I handled this

     3   evidence consistent with procedures as I have been

     4   trained and previously described.

     5   Upon taking custody, I checked to ensure

     6   the evidence I was receiving matched the description

     7   on the DA Form 4137, labeled as DN 151-10,

     8   Item I, identified at Bates number 00411151. I

     9   checked the date, time, and other collection

    10   information. And finally, I signed in the Received

    11   By column. While in possession of this evidence, I

    12   maintained positive control. I did not alter the

    13   information on the CD. I have no reason to believe

    14   this evidence was damaged or contaminated in any way.

    15   On 18 October 2010, I properly signed this evidence

    16   over to Ms. Mairena, the CCIU evidence custodian. I

    17   did not touch this evidence again. PE 68 for

    18   identification is DN 151-10, Item 1.

    19   And the United States moves to admit

    20   prosecution exhibits 65, 67 and 68 for identification

    21   as prosecution exhibits 65, 67 and 68 respectively.

1   MR. TOOMAN: No objection.

2   THE COURT: May I see them, please?

3   Prosecution exhibits 67 for identification is

4   admitted.

5   Counsel, I have prosecution exhibit 67, but I

6   have a CD and it says 66.

7   MR. FEIN: 66 has already been admitted,

8   ma'am.

9   THE COURT: I know, but there's nothing in

10   67.

11   MR. FEIN: I will retrieve those two exhibits

12   from the court reporter.

13   Ma'am, there is a document marked in this

14   folder. There is a single page document that accompanies

15   the CD.

16   THE COURT: And prosecution exhibit 68 is

17   admitted. 67 is admitted.

18   Now, I have 44 here, is that another one

19   that --

20   MR. FEIN: No, ma'am.

21   Ma'am, also we have found in the bag

```
 1  prosecution exhibit 108 earlier that was to be marked

 2  prior to the recess.

 3              THE COURT:  Prosecution exhibit 108 is

 4  admitted.

 5              I'm looking at the time.  How do the parties

 6  want to proceed?

 7              MR. FEIN:  Ma'am, the United States

 8  recommends we take our lunch recess.

 9              THE COURT:  All right.  How long would you

10  like?

11              MR. FEIN:  Hour and 15 minutes, ma'am.

12              THE COURT:  All right.

13              MR. FEIN:  We're also trying to set up a

14  phone call for the defense to talk to an certain witness.

15  If that happens, we might ask for more time during the

16  recess.

17              THE COURT:  What do you think the likelihood

18  of success is in that?  Do you just want to make it 1:30?

19              MR. COOMBS:  No objection to that, ma'am.

20              THE COURT:  Court is recessed until 1:30.

21                    (LUNCH RECESS.)
```

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

A

able (2)
29:15;113:16
above (3)
20:4;57:21;93:15
absent (1)
5:7
Academy (4)
47:7;70:10;104:13,21
accepting (3)
77:8,11;78:3
accepts (1)
74:17
access (24)
9:2,5,7;10:2;11:3;13:12,
13;26:20;41:3;79:9;97:17,
20;98:10,11,12;105:3;
106:16;108:11,16,19;109:4,
5,6;113:17
accessed (8)
14:14;19:14;20:2;98:18;
100:19;107:1,18;110:9
accesses (1)
68:1
accessible (6)
11:16;13:3;97:19;98:3;
108:18;109:20
accommodate (1)
6:4
accompanies (1)
117:14
accordance (1)
101:10
according (7)
24:4;53:20;59:14;78:11;
85:8;89:18;90:2
account (1)
5:2
accreditation (1)
26:13
accuracy (1)
99:19
accurate (2)
14:15;17:1
accurately (2)
99:11;106:4
Accused (9)
7:14;17:11;23:8;46:1,17;
79:21;80:6;94:19;102:12
accused's (1)
23:2
achieved (1)
57:6
ACIC (16)
7:20;8:1,8;9:6,9;11:10,
11,12;12:21;13:7,10;14:11;
15:18,20;16:6;19:12
acicnorth-inscomannysmilmil (1)
11:15
acquisition (4)
70:13,14,17;71:6

acronym (2)
59:18;62:15
across (1)
61:21
Act (1)
82:1
action (5)
35:3;50:10;54:12;91:1,15
actions (1)
91:8
active (15)
18:2,6;25:13,15;27:4;
45:2;47:9,10,11;48:15;
49:7;56:18;80:16,18;95:3
activities (11)
49:14;60:11;61:1;67:20,
21;88:1,5;93:2,12;95:9,11
activity (8)
16:19,20;19:2,7;52:17;
67:18;86:14;98:19
actual (1)
73:7
actually (10)
6:13,14,17;22:10;29:3;
38:4,7;60:21;71:18;85:3
add (1)
37:12
addition (3)
103:19;106:8;108:10
additional (1)
48:3
Additionally (4)
55:13;82:6;89:21;92:5
address (37)
5:9;6:20;9:5,11,16,19,19;
11:17;12:14;13:17;14:1,3,5,
6,13;16:4,7;19:9,12,15,20;
20:1,4,13,14;21:2;36:7,12;
73:5,9,10;97:11;98:15;
100:2,4;109:11;115:4
addresses (7)
13:19;15:3;18:20;19:13;
21:4;97:21;98:17
admin (2)
5:10;111:13
administration (5)
26:7;47:8;80:15;96:14,16
administrative (1)
103:13
Administrator (4)
17:16;18:9;21:9;25:21
administrators (1)
19:3
admissibility (1)
66:18
admit (10)
17:4;22:3;23:12;58:7,11;
73:16;94:1,8;101:20;
116:19
admitted (17)
17:7;23:16;37:1;58:15,
18;66:13,18;67:3;73:20;
94:5,6,12;117:4,7,17,17;

118:4
advanced (3)
47:19;103:21;104:15
Advocate (2)
107:5;111:1
AE (3)
56:7;89:10;92:16
affairs (1)
6:16
Afghanistan (12)
48:8;51:11;55:15,21;
56:16;81:2,3;83:6;87:19;
92:8,13;93:9
afternoon (1)
6:6
again (7)
5:5;33:6;71:19;77:13;
79:18;115:14;116:17
against (1)
43:14
agencies (2)
60:1,4
Agency (3)
8:10,12;104:20
Agent (17)
59:8,9;64:2;67:7,8;69:12,
14;73:3;74:13;75:15;76:16;
79:11,18;97:12;102:9,13,16
agree (1)
23:5
agreed (6)
7:14;17:11;46:17;80:6;
94:18;102:11
ahead (9)
22:10;28:14;66:19;68:13,
17;69:8;74:12;77:17;79:10
Air (11)
8:13,14;56:4,20;60:6;
64:12;80:12,16,19;81:3;
95:5
airman (1)
96:3
air-to-ground (1)
56:21
alerted (1)
8:19
alerts (1)
95:15
Allen (7)
8:11;48:16,18,18,21;49:6,
11
allocate (1)
10:16
allows (6)
9:19;20:1;42:5,9;97:16;
108:16
along (2)
36:9;43:17
alphabetically (1)
112:7
alter (8)
12:15;15:6,9;21:18;
100:15;108:7;115:9;116:12

altered (1)
15:2
alternate (2)
75:17;76:1
although (1)
5:19
among (4)
51:9;83:3;104:5;107:17
amounts (2)
70:14;71:1
analysis (11)
27:13;37:16,18;43:3;
61:15;65:8;95:10,10,15,16;
96:17
analyst (3)
27:13;95:20;96:1
analytical (2)
37:17;42:21
analyze (1)
10:15
annotated (3)
23:3;51:19;85:21
anonymous (1)
74:20
anticipated (1)
54:17
appear (2)
10:7;46:4
appeared (1)
87:10
appears (5)
39:3;64:3;73:6,12;74:7
appellate (3)
5:12;55:8;89:2
applicable (2)
89:19;90:3
application (1)
19:1
applications (2)
70:11,11
applied (1)
84:13
apply (3)
27:1;29:16;79:19
applying (4)
43:11;51:18;84:14;85:14
approach (1)
84:14
approached (1)
85:1
appropriate (5)
84:17;85:8,16,18;105:19
approved (2)
101:14;107:7
approximately (6)
8:18;35:6;36:12;45:6;
47:14;51:5
April (3)
100:3;104:14;105:4
AR (7)
51:12;55:13,16;83:7;
92:6,8,14
Arc (1)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

96:16
ArcSight (1)
96:14
area (7)
20:21;53:9;70:4;87:7;
90:9;98:8;109:2
Areas (1)
95:7
arms (1)
91:6
Army (11)
7:19;8:4;18:4;50:6;57:1;
60:5;64:12;67:8;80:21;
84:9;103:10
Army's (1)
103:2
arranged (1)
111:18
arrest (1)
91:12
Artale (3)
7:7,12,16
ASA (1)
96:21
asp (2)
10:6,7
Assange (3)
33:20,21;40:14
assessed (1)
92:1
Asset (1)
102:18
assigned (10)
9:18;11:10;19:9;47:4;
60:14;95:3;100:1,4;110:13;
114:13
assignment (2)
50:20;83:12
assigns (1)
9:6
assist (1)
105:8
assistance (1)
54:18
assisted (2)
101:6;109:8
associate (2)
96:7,10
associated (5)
43:15;93:10;96:12;106:2;
112:1
Associate's (1)
8:15
assurance (2)
26:13;95:21
attached (1)
15:4
attack (4)
52:20;86:17;90:8;95:9
attacks (10)
54:6,8,11,20;88:11,12,13;
90:15,16,17
attempt (1)

75:11
attend (3)
29:12,14,20
attended (8)
29:13;30:2;33:16;103:21;
104:6,8,11;105:2
attending (1)
27:21
attention (1)
75:9
attested (1)
21:16
audience (1)
34:14
audit (8)
18:19;19:2,4,7;97:3;
98:13;106:15;107:15
August (9)
97:2;107:7,7,19,19;
110:7;112:12;114:10;
115:11
authentication (1)
113:20
authenticity (1)
21:16
Authority (2)
58:3;93:19
authorization (1)
107:3
authorized (2)
98:9;109:2
automatic (1)
20:10
automatically (4)
12:1;14:10;16:9;19:5
available (6)
5:20;50:5;75:7;82:17;
84:8;101:3
Avionics (1)
96:9
awareness (3)
33:2;38:8;75:12

B

Bachelor's (1)
18:12
back (7)
35:4,12;41:20;71:7,11,
19;79:12
backdated (1)
14:21
backup (1)
114:19
badge (2)
98:11;109:5
bag (1)
117:21
Barracuda (2)
110:11;114:11
Base (1)
95:5
based (11)

15:20;20:11;37:16;52:6;
62:2,21;64:8;65:11;91:11;
97:10;109:11
basic (3)
26:8;96:17;104:16
basically (16)
25:1,11;27:1;28:15;29:4;
34:9,11,13;35:12;37:5,11,
19;38:1,6;67:18;71:3
basis (5)
19:6;51:19;60:18,19;
85:21
BATES (12)
21:17;51:21;55:9;56:7;
86:2;89:3,11;92:16;100:12;
108:4;115:6;116:8
BE22 (11)
56:13;83:8,9;93:4,5;
114:2,2,4,6,7,9
became (4)
8:17;18:14;36:3;97:1
become (1)
6:13
began (2)
48:16;80:15
beginning (2)
81:6;113:13
behind (1)
38:1
belonged (1)
82:2
below (2)
75:13;84:12
benefit (1)
43:3
Berlin (1)
28:18
best (2)
10:17;76:8
better (1)
23:12
big (2)
30:12,20
bigger (2)
30:11,12
bit (6)
27:14;31:7;37:3;71:4;
72:3;77:6
blank (1)
101:8
bombs (1)
48:4
Booz (7)
8:11;48:16,18,18,20;49:6,
11
border (1)
91:17
Both (3)
58:14;93:7;105:13
Bradley (2)
51:7;82:21
Branch (5)
8:18;15:10;50:9;95:3,21

Bravo (1)
46:16
break (1)
58:20
brief (4)
22:9,14;58:20;59:4
briefing (1)
49:9
Briefs (1)
111:13
brings (2)
29:4,6
broad (1)
87:19
broadly (1)
61:5
broken (2)
13:16;64:10
BS (3)
47:5,5;80:12
Budram (2)
15:11,13
bugs (1)
39:15
build (1)
17:21
bulk (1)
71:17
burned (5)
21:5,10;99:5,9;100:15
burning (1)
100:7
business (3)
16:19,20;47:7

C

C3 (4)
28:11,12;29:1,2
C4I (1)
49:4
cable (3)
101:16;110:8,10
cables (1)
107:11
caches (2)
54:13;91:16
California (1)
80:19
call (6)
7:2;59:5;62:17;65:10;
71:12;118:14
called (8)
10:19;24:3;28:2,3;62:14,
16;70:9;110:18
calls (1)
23:10
came (2)
30:21;35:4
Can (24)
7:5;9:18;10:3,15,21;
40:18;53:11,16;55:1,6;
60:19,20;61:10,14;62:13;

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

63:7,10;67:3;69:20;74:13;
76:1;77:13,16,19
capabilities (4)
53:5;54:14;87:3;88:14
capacity (12)
5:21;8:8;17:21;18:1,8;
51:2;57:2,8;81:20;82:19;
95:5,14
Captain (6)
5:6,6,7;23:17;38:19;39:4
capture (10)
98:15,16,18;110:17,20;
111:2,5,8,10,16
captured (2)
57:4,7
captures (2)
9:3;14:12
capturing (1)
10:2
career (4)
49:6;80:17;81:3,10
carrier (2)
47:20;48:5
case (19)
8:18;9:9;11:2;13:7,10;
18:15;20:3;33:3;45:21;
46:1;63:17;75:21;79:20;
95:20;96:14;97:1;105:7;
109:13;114:19
casualties (6)
55:19;88:10;90:12;91:3,
19;92:11
categories (2)
87:10,11
cause (1)
109:13
CCC (1)
28:11
CCIU (8)
101:8,14;103:4,5;107:4;
108:5;115:13;116:16
CCIU-issued (2)
101:15;110:8
CCJ6 (1)
95:3
CCNA (1)
96:10
CD (8)
56:12;93:7;114:6;115:19,
20;116:13;117:6,15
cellphone (1)
31:1
censored (1)
74:18
CENTCOM (1)
99:14
CENTCOMHQ (1)
99:16
center (12)
5:18;6:8;7:20;30:5,11;
98:8,10;104:2,10,18;109:2,
4
Central (4)

50:8;81:12;95:4;105:9
CERT (1)
95:14
certain (6)
9:1;10:21;49:9;62:21;
82:14;118:14
Certification (1)
104:9
certifications (1)
18:11
certified (3)
96:5,9,11
chain (2)
35:12;37:13
Chamberlin (3)
7:8;17:10,12
change (2)
23:3,5
Chaos (3)
28:6,9;29:3
charge (1)
26:21
charged (2)
97:10;109:14
check (1)
66:17
checked (2)
116:5,9
Chief (4)
8:19;15:10,12;107:3
chronologically (4)
37:5;39:7;40:2,4
CICP (1)
96:11
CID (3)
67:8;103:3,17
CIDNE-A (14)
51:11;52:13;53:19;54:1,
2;55:7,11;83:6;86:10;87:8;
89:9,15;90:1,4
CIDNE-I (1)
89:8
CIDNE-I (7)
83:4;86:9;87:8;89:1,17,
20;90:4
CIE (3)
99:12,14,16
cipher (2)
98:11;109:5
circumstances (2)
55:18;92:10
Cisco (2)
96:9,20
CISSP (1)
96:6
citizenship (2)
25:2,3
CIVCAS (2)
55:19;92:11
civil (1)
91:17
civilian (3)
26:4;55:18;92:11

Class (2)
51:6;82:21
classification (28)
49:16,18,19,20,21;51:15,
19,20;52:3;53:20;58:3;
61:21;83:19,20;84:1,3,4,14,
17,19;85:9,15,19;86:1,5;
89:19;90:3;93:19
classified (49)
11:16;19:10;26:16,19;
34:5,16;41:12,14;49:5,8,11;
50:16,21;51:4,18;52:4,9;
53:10,19;54:21;56:2,3,17;
57:15;58:5;74:17;75:6;
79:1;81:6,8,9,18;82:4,14,
15;83:14,16,18;85:3,4,5,7,
21;89:18;90:2;93:1,20;
103:7;116:2
clean (2)
99:6;107:12
clear (1)
101:9
clearance (3)
81:5;96:7;108:20
clearing (2)
54:13;91:16
clicked (6)
110:16,19;111:1,4,6,9
clicks (1)
14:11
close (1)
56:4
closer (1)
33:17
Club (2)
28:6,9
cluster (3)
98:1,8;109:1
CND (1)
95:15
CO (1)
45:4
coalition (2)
82:10,13
Coast (1)
49:15
code (7)
52:18;54:5,18;86:15;
90:21;93:2,10
codes (1)
14:17
collaborate (2)
97:18;108:17
collaboration (1)
108:13
Collar (1)
104:17
collect (6)
10:15;101:13;102:20;
105:13;108:12;109:18
collected (12)
14:10;52:13;86:9;99:20;
100:21;101:5;105:9,21;

106:14;107:15;114:21;
115:9
collecting (5)
101:1,6;105:12,16;
108:10
collection (14)
44:16;84:21;91:10;97:3,
6,8;98:21;101:13;105:8,18,
20;107:9,10;116:9
colon (1)
75:14
Colonel (3)
80:4,7,11
Colorado (2)
24:8,12
column (1)
116:11
columns (1)
12:7
com (1)
72:11
combat (7)
47:14;48:7;53:9;56:5;
57:3;87:7;91:21
Combined (3)
51:10;83:3,5
combines (1)
29:4
comfort (1)
58:20
coming (1)
33:5
command (10)
29:16;35:12;37:13;38:7;
48:19;49:3;50:8;81:12;
103:3;105:10
Commander (5)
46:12,18;47:2;58:2;93:18
Command's (1)
95:4
common (3)
9:15;10:8;19:18
commonly (1)
20:20
communicate (5)
9:14,15;19:17,19;42:3
Communication (10)
29:3;42:6,9,12;43:5,6,7,
14,18;44:20
communications (1)
49:3
community (3)
8:2;29:5;61:3
company (1)
24:12
compare (1)
106:17
Compartmented (1)
81:13
complete (2)
15:17;17:1
completed (2)
47:15;48:2

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

100:9,10;108:3;116:7
daily (2)
  19:6;49:8
damage (1)
  108:8
damaged (2)
  115:11;116:14
dash (2)
  99:15,16
data (52)
  10:15;12:1,11,16,16,21;
  13:2,12,14,14,16;14:9,15,
  20;15:1,4,7,9;19:5,13;21:1;
  51:10;67:4;70:3,13,15,17;
  71:6,10,10,18;72:4,13;73:7;
  83:4,5;98:8,10;99:6,13,21;
  100:3;101:4;103:7,8;
  104:16,16;105:3,8;107:12;
  109:1,4
Database (5)
  11:21;12:4;75:1;98:1,4
databases (1)
  12:5
date (25)
  12:14,15;13:13,17;14:12;
  16:2,4,7;19:14;20:4,11;
  21:3;23:1;52:21;73:6;74:4,
  5;84:16,18;86:18;105:20;
  106:4,11;107:17;116:9
date/time (1)
  9:5
dated (8)
  7:12;17:10;46:13;51:21;
  80:5;83:20;84:1;86:1
dates (2)
  18:21;98:18
Dave (1)
  109:17
day (6)
  6:4;29:21;107:8,14;
  108:4;112:12
days (4)
  29:18,19,20,21
DCITA (2)
  104:13;105:6
de (1)
  36:3
deal (1)
  60:2
December (9)
  14:2,4;28:20;65:4;75:5;
  99:21;105:3,6;107:19
decision (2)
  51:20;86:1
declaration (6)
  51:20;52:2,3;86:1,4,5
declassified (5)
  53:11,17;55:1,7;64:3
dedicated (2)
  6:7;19:10
Defense (18)
  7:14;8:10;17:11;22:16;
  23:5;46:17;49:12;66:21;

68:10;70:9;80:6;94:19;
  95:3,8;102:12;104:12,19;
  118:14
degree (2)
  8:15;18:12
degrees (1)
  96:8
denoted (1)
  36:11
Denver (2)
  24:8,12
department (7)
  25:3,5;102:19;103:2,16;
  105:10;115:16
dependent (1)
  72:14
depends (1)
  61:17
depicting (1)
  56:14
depicts (1)
  93:8
deployed (6)
  48:8,9,9;80:20,21;81:1
deploying (1)
  54:4
deployment (1)
  48:4
deployments (4)
  52:8;53:14;55:4;86:20
Deputy (2)
  58:2;93:18
derivative (1)
  49:18
describe (3)
  88:6;105:20;108:1
described (9)
  84:12;87:17;88:4;91:9,
  15,17,21;92:4;116:4
Describes (1)
  65:6
description (3)
  37:10;106:2;116:6
descriptions (1)
  54:16
designated (1)
  60:16
desire (1)
  40:19
desk (2)
  81:15,16
desktop (4)
  12:11;110:18;112:13,18
detailed (3)
  88:9;91:12;92:2
details (9)
  52:10;53:2,15;54:20;
  55:5;65:9;86:21;91:2,21
detecting (1)
  88:11
detention (1)
  91:13
determination (4)

50:2;58:4;84:6;93:19
determine (8)
  49:21;50:20;82:4;83:13,
  17;84:16,18;85:7
determined (6)
  53:18;84:20;85:18;89:17;
  90:1;109:17
determining (1)
  11:7
deterrent (1)
  54:18
develop (2)
  95:11;105:1
developed (1)
  9:2
Developer (2)
  8:6;11:1
developers (2)
  8:7;13:4
development (4)
  8:9,12;10:16;49:13
device (2)
  52:20;68:2
devices (3)
  87:13;99:6;100:16
devoted (1)
  103:12
DIA (1)
  8:10
different (1)
  82:11
digit (3)
  64:13,16,18
digital (3)
  102:20;109:21;110:5
digitally (1)
  12:9
diplomatic (3)
  74:19;77:8;78:7
dire (3)
  68:11;69:8,10
direct (6)
  6:18;22:19;24:5;59:15;
  73:1;90:11
directive (1)
  6:12
director (2)
  50:17,18
Directorate (1)
  81:17
Directory (4)
  110:18;112:2,13,18
disc (6)
  21:5,6,11,12,13,16
Disclosure (1)
  87:20
discontinued (1)
  81:15
discovered (1)
  75:13
discrete (1)
  75:2
discuss (3)

42:19;45:21;79:20
discussed (2)
  39:4;75:16
discussing (1)
  38:19
discussion (4)
  40:5,10;42:18;69:6
disk (3)
  99:11;100:10,15
display (2)
  20:12;93:14
displayed (2)
  63:13,14
disseminates (1)
  8:5
distribution (1)
  62:1
disturbance (1)
  91:18
division (2)
  48:7,20
DMZ (2)
  20:21;22:1
DN (2)
  116:7,18
doc (1)
  10:11
dock (4)
  101:16;110:9,12;114:13
document (52)
  10:6,10,11,12,14;11:10,
  19;13:10,12,15;15:6,21;
  34:20;38:18,19;51:17;65:7,
  14,20,20;71:13;73:3;77:4,7,
  7,13;78:21;79:4;82:5,15,17;
  84:16,19;85:2,3,5,6,14,17,
  19;100:10,11;105:19;108:3,
  3;111:4;112:9;113:18;
  115:5,5;117:13,14
documentation (1)
  81:20
documented (1)
  115:4
documenting (1)
  108:2
documents (62)
  17:2;50:19,21;51:3,4,5,8,
  9,10,11;52:2,5,7,12,13,13,
  15;56:1,3,6,10;58:1;65:6;
  75:6,12;79:9;81:21;82:20;
  83:1,2,3,6,11,14,15,18;
  84:15,20,21;85:1,9,10;86:4,
  7,8,9,10,12;89:16,21;90:5;
  92:6,14,19,20;93:4,16;
  97:10,11;98:18;107:18;
  113:18
document's (2)
  84:17,18
DOD (2)
  60:1;63:2
done (4)
  23:12;32:17;37:17;69:7
DoS (1)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

115:19
dot (5)
36:9,10,10;72:11;75:7
down (2)
13:17;76:1
download (1)
109:21
downloaded (2)
112:15,19
drafting (1)
38:5
dragons (3)
28:4,7,8
drive (19)
99:5,8,9;101:16,17;
107:11;110:9,11,12,13;
113:7,10,11;114:12,13,13,
18,18,19
drives (4)
101:8,9;115:1,1
duly (2)
24:3;59:13
during (13)
7:16;17:13;46:20;52:8;
80:8,17;81:9;84:1,12;
94:20;102:13;110:7;118:15
DUSTWUN (4)
87:16;88:15,18;92:4
duties (1)
16:14
duty (15)
18:2,6;25:13,15;27:4;
45:2;47:9,10,11;48:16;
49:7;56:18;80:16,18;87:16
DVD (6)
99:6,12,13;100:8;107:15;
108:7

E

earlier (1)
118:1
early (1)
27:15
easier (1)
12:20
easy (1)
12:7
effect (1)
32:6
effective (1)
95:12
effectiveness (4)
54:5;90:15;91:8;92:1
eight (9)
8:8;15:10;25:16;47:19;
51:14;86:8;90:15;100:18;
110:7
eighteen (3)
20:3;91:4;93:15
either (2)
28:11;72:13
ELDEN (1)

62:10
Electronic (2)
18:7;96:8
elements (2)
61:4,10
eleven (6)
5:17;53:18;59:3;88:4;
90:18;113:13
eliciting (1)
34:14
else (4)
6:20;13:5;21:20;28:9
Elten (46)
5:7;23:9,17,19;24:6;32:6,
9,13;33:9,12;36:14;37:2;
38:10,19;39:5;45:15,18;
59:7,16;64:1;65:13,16,19;
66:2,7,9,12,14;67:6;68:16,
18;69:2,7;73:2,15;74:1,9;
76:10;79:15,17;94:13,16,
18;102:4,7,11
email (3)
15:11;75:2;111:13
emailed (1)
12:21
Embassy (1)
50:11
Emergency (1)
95:14
emphasis (1)
41:12
employed (1)
7:19
employee (1)
16:12
enable (1)
19:3
EnCase (9)
70:9;96:15;104:7;112:20,
21;113:6;114:15,15;115:2
encountered (1)
90:14
encounters (1)
88:19
encourage (1)
65:5
end (2)
22:20;98:3
Enduring (1)
48:11
enemies (1)
79:9
enemy (13)
53:1;54:6,8,17,20;79:5;
90:14;91:3,5,6,7,8,19
enforcement (7)
9:8;103:11,17,18;104:1,
10,14
engagement (4)
54:15,15;90:14;92:1
engagements (5)
84:12;87:12,17,21;88:5
engine (1)

63:5
engineer (3)
8:13;10:21;96:2
engineering (4)
39:15;80:13;95:10;96:4
English (2)
31:5;33:3
enlisted (1)
96:2
ensure (5)
21:12;57:6;85:2;106:3;
116:5
ensured (1)
107:11
entail (2)
24:15;26:10
entails (1)
24:16
enter (2)
36:17;113:15
entered (2)
47:9;110:4
entering (1)
113:20
entries (2)
20:13,14
entry (1)
20:15
Environmental (1)
47:6
equally (1)
72:9
equipment (5)
26:12;88:8;90:13;91:4;
107:10
equities (15)
51:5;55:8;56:7,17;58:1;
81:18;83:16;85:10,12,14,
17;89:2,10;92:15;93:16
ESM (1)
96:14
ESPN (1)
72:11
essentially (3)
29:2;43:3;61:2
Establish (1)
32:4
established (1)
65:4
ethical (4)
74:19;77:8;78:10;96:18
even (2)
77:4;82:16
event (2)
9:7;18:19
evidence (48)
36:18;73:17,20;98:21;
100:8,9,14;101:12,13;
102:20;104:5,8;105:9,17,
18,21;106:2,7,10;107:6,9,
20,21;108:2,5,6;113:1,2,5;
114:16,18,19,21;115:5,8,9,
10,12,13,14,17;116:3,6,11,

14,15,16,17
evidence-handling (1)
103:20
ex091119log (1)
20:5
ex091201log (1)
20:5
ex091214log (1)
20:6
ex091217log (1)
20:6
ex091221log (1)
20:6
ex091229log (1)
20:7
ex100207log (1)
20:7
ex100209log (1)
20:7
ex100211log (1)
20:8
ex100214log (1)
20:8
ex100301log (1)
20:8
ex100302.1og (1)
20:9
ex100308log (1)
20:9
ex100315log (1)
20:9
ex100316log (1)
20:10
ex100317log (1)
20:10
EXAMINATION (8)
24:5;38:12,14;59:15;
69:10;73:1;76:12,14
Examinations (1)
104:12
examine (1)
102:20
examiner (1)
109:17
example (4)
63:2;97:18;105:21;
108:17
examples (1)
60:3
Excel (7)
12:6,8,10,17,18;15:19;
16:10
exceptions (1)
5:6
Exchange (3)
51:11;83:4,5
exclusively (2)
41:9,13
excusal (2)
45:17;79:16
Excuse (3)
23:17;64:3,15
excused (2)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

45:20;79:19
execution (6)
48:15;53:11,17;54:17;
55:1,7
Executive (1)
51:16
exfiltration (1)
103:6
exhibit (54)
5:12;7:7,9;15:15;17:6;
21:15;22:3,4,16;23:11,15;
34:18;35:13,15;36:15,17,
21;46:8,14,15;52:1;55:9;
58:7,8,11,12,16;63:19;66:3,
4,10,18;67:1;73:16,19;74:2,
10;76:18;77:14,17;79:11;
80:3;86:3;89:3;94:14;
100:5;101:21;102:1,8;
111:20;117:5,16;118:1,3
exhibits (14)
46:4;58:14,17;94:1,2,4,6,
8,9,11;116:20,21;117:3,11
exist (1)
43:5
expected (6)
7:12;17:9;22:18;46:11;
80:4;102:8
experience (10)
52:6;53:21;57:14,17,17,
18;64:9;69:14;103:11;
104:5
expert (2)
67:2;81:18
expertise (1)
105:2
explain (2)
33:10;34:8
exploitation (1)
95:11
Explorer (1)
110:14
explosive (2)
52:20;87:13
exposing (1)
39:15
expression (1)
43:13
EXSUMs (1)
111:14
extensive (1)
104:5
external (3)
10:18;20:17;98:17
extra (1)
29:17
extracted (1)
107:2
extracting (1)
12:3

F

F-18 (3)

47:11;48:2,6
F-18s (1)
48:1
faced (1)
27:3
facility (4)
30:4;81:14;98:10;109:4
fact (4)
52:19;61:15;85:1;86:17
facto (1)
36:3
failure (1)
114:20
fairly (2)
68:6,8
familiar (7)
16:12;21:8;45:7;61:7;
62:4;68:7,8
familiarity (1)
52:7
family (2)
82:7,12
far (3)
26:11;31:17;38:8
Farah (36)
51:12;52:14;55:15,16,20;
56:1,6,15;83:7;86:10;92:7,
9,13;93:4,9;106:18;109:18;
110:1;111:10,12,19;112:4,
7,13,15,16,17;113:1,6,8,14,
19,21;114:16,17;115:2
FBI (3)
60:5;63:4;104:21
featured (2)
30:8,10
February (2)
74:6;81:11
Federal (2)
104:1,10
Fein (28)
5:2,4,10,16;6:10;7:1,3,11;
17:9;22:6,8,13,15;23:14;
46:6,9,15;58:10,19;69:4;
80:1;94:7;117:7,11,20;
118:7,11,13
Fein's (1)
23:2
few (2)
5:10;31:2
Field (2)
50:6;84:10
Fifteen (4)
57:12;89:16;91:1;103:11
file (19)
10:8;19:7;67:18;83:8;
93:4;99:4;110:1;112:1,3,
16;113:1,2,5;114:1,4,6,7,8,
16
filed (1)
5:11
filenames (3)
112:3,8,11
files (16)

20:3,4,12,13;21:4,13;
71:2;93:7;97:18;98:15;
99:14,18;108:17;112:10,19;
114:1
fill (1)
105:19
filled (1)
5:20
filters (1)
43:12
final (2)
58:4;93:19
Finally (4)
14:19;93:13;115:15;
116:10
find (2)
43:18;62:11
finding (2)
54:13;91:16
fine (1)
102:6
finished (3)
8:1,4;68:14
fire (2)
90:11;91:6
firewall (2)
115:16,20
First (21)
5:11;7:6;8:17;12:13;
18:14;20:15;22:21,21;24:3;
37:6;39:9;51:6;64:10;73:9;
82:21;84:15;99:18;101:1;
112:6,8;114:19
fit (1)
37:18
Five (11)
11:12;18:5;20:17;29:19;
30:14;50:7;64:11;83:17;
90:12;98:13;106:13
fix (2)
38:4,4
Fleet (1)
47:4
flexible (1)
54:18
flight (5)
47:14,17;48:12;57:4,17
flights (1)
49:8
FLIR (1)
57:5
Florida (1)
95:5
flow (2)
44:4;95:15
fly (1)
48:1
flying (2)
47:20;48:5
focus (1)
109:10
focused (8)
41:2,9,13;55:17;71:9;

87:15;92:9;97:8
FOIA (5)
82:1,3,6,16;85:1
folder (42)
21:5;97:14;100:20;
105:15;109:7,10,15;110:2,
3,4,18,21;111:3,6,7,9,10,11,
12,17,19;112:3,4,7,13,15,
16,17;113:1,5,6,8,10,14,19,
19,21;114:15,16,17,17;
117:14
FolderLOI (1)
113:3
folders (3)
109:21;113:17;115:2
follow (1)
105:17
followed (3)
39:17;73:5,6
following (8)
13:19;20:5;50:1;84:5;
90:8;106:8;107:14;111:12
follows (8)
7:18;17:15;24:4;47:1;
59:14;80:10;95:1;102:15
follow-up (1)
61:11
Force (9)
8:13,14;60:6;64:12;
80:12,16;81:3;90:20;95:5
forces (13)
53:3,9,16;54:5,16;55:6;
87:1,6;88:6,13,14,20,20
Foreign (8)
11:4,13;54:19;60:12;
86:14;87:21;88:2,20
forensic (6)
95:15;102:17;104:4,7,11;
109:17
forensically (1)
109:18
forensics (3)
70:6;96:15;105:3
forgive (1)
39:14
Form (5)
100:9,10,13;108:3;116:7
formal (1)
107:4
format (7)
10:6,8;14:1;15:21;20:12;
35:9;99:4
formation (1)
47:20
formats (1)
72:13
forms (2)
54:3;90:6
Fort (2)
7:21;17:18
forth (2)
16:16;37:7
forward (2)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

6:4;57:4
forwarded (5)
15:10,13;58:1;93:17;
107:4
found (6)
28:16;38:8;56:1;92:20;
101:12;117:21
foundation (10)
32:4,11;65:14;67:3,5;
68:14,15,21;69:7,9
Foundations (1)
96:15
FOUO (1)
75:6
Four (12)
10:20;20:1;29:21;49:5;
64:15;74:14;75:4;83:10;
90:12;95:19;97:15;105:16
Fourteen (4)
56:18;89:1;90:21;115:15
fourth (1)
64:14
Fragmentary (2)
53:4;87:2
FRAGOs (2)
53:5;87:3
France (1)
33:5
free (3)
31:17,20;44:3
Freedom (5)
48:11,11;82:1;83:21;84:2
frequency (1)
36:1
frequently (1)
68:6
friendly (7)
53:3,16;54:12;55:6;87:1;
91:1,15
front (1)
98:3
FT210 (1)
104:11
fulfill (1)
18:9
fulfilling (1)
8:3
full (1)
33:18
function (1)
18:10
functions (1)
17:19
funds (1)
29:17
FUR (2)
57:18,19
further (11)
38:10;45:13;72:16;76:10;
79:12;85:12;97:12;99:9;
104:13;106:3;108:11
Furthermore (1)
15:2

G

gamut (1)
26:11
gap (1)
45:10
gaps (1)
45:8
garnered (1)
75:8
gas (1)
24:11
gather (3)
44:7,12;101:11
gathered (1)
91:12
gave (2)
31:8;33:19
general (8)
27:12;43:8;52:19;64:11;
86:17;91:5;102:18;105:17
generally (10)
37:10;43:8;44:21;61:8;
65:2;67:12;70:19,21;75:17;
76:7
generate (1)
61:11
Georgia (1)
104:2
Geo-Spatial (1)
8:12
German (1)
31:6
Germany (1)
27:17
Gharani (11)
55:20;56:14;57:9,12,15;
83:9;86:11;92:12;93:6,7,9
given (8)
6:7;9:20;20:2;21:2;30:9;
31:4,5;33:20
gives (3)
62:1;65:8,10
giving (1)
42:19
global (1)
33:4
Glynco (1)
104:2
goal (1)
57:6
goes (5)
32:6;33:9;65:8;69:21;
75:21
Good (5)
35:20;38:16,17;69:12,13
Google (2)
63:15;72:10
government (14)
6:3;8:20;19:8;24:21;46:3,
4;59:5;65:5;67:2;78:20;
81:19;86:14;87:21;115:21

governments (2)
78:16,18
Grant (11)
94:14,20;105:13;106:14;
107:1,8,11,14;108:11,21;
109:8
granted (2)
98:10;109:3
Grant's (1)
109:11
graphics (1)
56:5
Greenwich (1)
74:7
ground (3)
47:16;57:1,2
Group (6)
7:21;15:12;17:17,18;
18:17;90:9
Groups (3)
11:6,14;91:3
GSM (1)
31:1
Guard (2)
49:15;80:19
guess (7)
29:14;34:14;70:5,16;
76:8;77:7;78:19
Guidance (1)
104:7
Guidant (1)
70:8
guide (7)
49:21;83:20;84:1,3,14,
17;85:19
guides (10)
49:19;51:15,19;53:20;
74:17;83:19;85:9,15;89:19;
90:3

H

hacker (1)
29:5
hacking (2)
29:8;96:18
half (2)
49:16;95:19
hand (4)
34:19;63:20;66:9;77:15
handed (3)
22:18;34:20;64:2
handing (2)
66:4;74:10
handle (1)
81:7
handled (5)
81:5,6;115:7;116:1,2
handling (2)
105:16;107:21
happens (1)
118:15
hard (11)

99:5,7,8;101:8,9,17;
107:11;110:11;114:11;
115:1,1
Hardware (1)
105:5
hash (5)
99:10,15,17,18;113:3
head (1)
31:3
heading (1)
16:8
Headquarters (3)
95:4;98:9;109:3
heads-up (1)
93:14
Hearsay (2)
32:3;33:6
held (5)
29:10,11;95:18;102:21;
103:4
help (2)
40:19;77:12
helps (1)
101:4
hereby (6)
7:14;17:11;46:17;80:6;
94:18;102:11
herein (2)
98:13;108:1
hereinafter (3)
52:5;86:6;93:6
hidden (1)
42:6
hiding (1)
44:19
high (1)
48:4
hit (1)
57:6
hits (1)
13:15
hold (1)
18:12
Homeland (2)
25:5;49:12
Honor (23)
5:4;6:19,21;7:11;17:3;
22:2,8,20;36:16;38:11;
58:6;62:2;65:12,13;66:21;
68:10;72:16;73:15;79:15;
93:21;94:13;102:4,7
hooked (1)
101:15
Hosburgh (6)
23:10,19;24:2,8;38:16;
45:20
Hoskins (2)
46:12,19
host (1)
30:6
Host-Based (1)
96:19
hosted (3)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

28:5,6;30:4
hostile (3)
88:6,13,20
Hot (2)
62:14;63:2
hour (5)
31:13;34:1;49:16,17;
118:11
hours (5)
47:13,14;71:8,13;74:6
housed (6)
11:14;97:7;98:7;100:16,
18;109:14
human (1)
14:15
hundreds (2)
57:8,10
HURLEY (17)
17:5;22:5;23:4,6;32:3;
33:6;36:19;38:13,15;43:10;
45:13;58:9,13;59:1;94:3,
10;102:2
Hurley's (1)
23:2

I

IA (1)
96:1
icon (2)
111:7,10
ID (15)
15:17;16:12,15,18;17:1,
4;56:11,12;89:9,15;90:6,6;
92:19,20;93:6
idea (2)
42:8;44:8
identifiable (1)
103:8
identification (36)
11:8,9;13:21;15:16,20;
21:15;22:3;23:16;34:19;
35:14;36:17,21;52:2;55:12,
21;58:7,11;63:20;66:3,5,11;
73:16,20;86:4;94:2,8;97:6;
100:6;101:21;106:1;
111:21;114:5,8;116:18,20;
117:3
identifications (1)
109:12
identified (19)
52:18;54:9,11;68:19;
86:16;90:16,17,19,20,21;
91:5,7,9,11,18;97:9,21;
115:6;116:8
identifier (1)
11:11
identify (3)
38:2;81:8;106:20
identifying (5)
9:17;19:20;54:12;81:18;
90:18
identities (1)

88:2
IED (11)
52:20;54:6,8,9,11;86:17;
88:9,12,12;90:15,16
IEDs (3)
54:12;87:13,15
ignorance (1)
39:14
ignored (1)
75:10
II (1)
104:18
IIR (9)
59:17,18;60:18;64:4,7;
65:2;73:12,13,13
IIRs (7)
62:11,13;63:6,9,12,16,18
IIS (1)
98:14
image (1)
99:8
imaged (1)
107:1
imagery (1)
57:19
images (1)
115:2
immigration (2)
25:2,4
impact (2)
91:14;96:10
impinging (1)
44:3
implemented (1)
35:21
improvised (2)
52:20;87:13
INAUDIBLE (2)
36:12;44:10
incident (9)
51:13;55:17,19,19;83:7;
92:9,11,12;105:4
incidents (1)
67:13
include (10)
47:13,15;49:14;52:15;
54:3;75:1;86:12;87:11;
90:7;95:17
included (7)
13:15;50:3;51:9;83:3;
84:7;103:20;112:14
includes (2)
93:13;96:13
including (8)
53:13;55:3;86:19;93:12;
95:8;108:1;113:18;114:1
inclusion (1)
75:1
in-depth (1)
95:15
indicate (2)
10:12,13
indicated (4)

6:3;42:1,5;44:2
indicates (1)
64:11
indirect (1)
90:11
individual (6)
10:14;21:11;42:19;106:8;
112:5,16
individuals (1)
60:14
infer (1)
78:19
inflicted (1)
88:10
information (133)
8:3,20;10:2,18;11:1,20;
12:4,9,19;15:8,12;16:5,8,
17;18:13,16,18;19:11;
26:13;34:5,16,16;37:8;41:3,
12,14,18;44:7,12;49:4,6,8,
10,11;50:1,16,21;51:10,18;
52:8,9,15;53:20;54:3,4;
56:2;57:7,13,15;58:4;
59:19;60:8,10,10,20;61:3,9,
18;70:21;71:2,4;81:5,6,8,9,
13;82:1,2,4,4,7,13,14,15,17,
18;83:4,5,14;85:5,20;86:12,
14;88:16;89:18;90:2,7,11;
92:21;93:14,20;95:16,21;
96:5,19;97:7;98:6,14;99:3,
7,19,20;100:7,16,18;101:1,
2,4,7,14,19;103:8;104:18,
19;105:14,19;106:3,14,17,
18,19;107:2;108:12;109:6,
12,14,19,19;113:21;115:18;
116:2,10,13
informed (1)
41:7
INFOSEC (1)
95:20
infrared (1)
57:5
infrastructures (2)
53:6;87:4
in-house (1)
95:13
Initially (1)
81:14
initials (1)
23:3
initiation (1)
92:4
inserting (1)
12:3
insertions (2)
14:20,21
inside (1)
112:17
insight (1)
70:17
Inspector (1)
102:18
installations (2)

53:6;87:4
installed (1)
112:20
instead (1)
31:21
Institute (1)
80:13
instruction (1)
47:17
instructor (2)
48:12;57:17
Insurgents (2)
11:5,14
Insuring (1)
41:5
intel (1)
45:4
Intelink (16)
63:7,9,13;65:21;69:15,16,
18,21;70:3;72:5,6,10,18;
73:8;76:16,17
Intelligence (26)
7:21;8:1,2,10;11:5,13;
17:17;25:20;45:1,7,10;
54:15;59:19;60:2,5,9,15,21;
61:2,9;62:6;75:10;85:11;
90:10;91:10,12
intelligence-like (2)
59:21;60:15
intent (2)
46:8,9
intentions (3)
34:10,12,13
interact (1)
12:5
interactions (1)
87:18
Intercept (1)
18:7
interested (4)
11:3;41:16;97:13;106:16
interface (2)
97:16;108:15
intermediate (1)
47:18
internal (3)
10:17;20:21;21:4
internally (1)
11:10
Internet (26)
9:4,16;18:18;19:19;
31:17,18,20;32:1,21;33:4;
40:6;41:21;42:1,5,10;
43:12;44:7,11,14,20;68:2;
97:16;98:14;99:1;108:15;
110:14
interpret (5)
67:3;71:5;72:4,5,8
interpretation (2)
72:19;95:16
interpreting (1)
68:21
intervention (1)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

14:16
interviewing (1)
105:8
into (16)
12:1,10;14:16;21:4;
36:17;55:14,16;63:10;
70:17;73:17,20;92:6,9;
101:5;103:9;112:16
Introduction (1)
105:5
intrusion (1)
67:13
intrusions (2)
95:17;103:9
investigate (2)
67:11,12
investigated (2)
103:6,9
investigating (3)
55:17;92:10;109:16
investigation (16)
21:5;51:12;52:14;55:14,
16;56:1,6;61:7;83:7;86:11;
92:6,9,15;103:3;104:4;
106:19
Investigations (11)
60:6;70:10,20;90:19;
102:21;103:14;104:1,12;
111:7,13;113:19
investigative (2)
67:9;103:4
investigators (5)
13:7;15:13;106:17,20;
109:13
involved (12)
8:17;13:7;18:14;45:1;
56:21;90:11;91:1,6,16;97:1,
3,6
involvement (3)
88:1;95:19;104:3
involves (2)
48:14;70:14
involving (2)
60:11;70:10
IP (38)
9:5,11,16,18,19;11:17;
12:14;13:17,19;14:1,3,5,6,
13;15:3;16:3,7;18:19;19:9,
11,13,14,20;20:1,4,13,14;
21:2,3;73:5,9,10;97:21;
98:15,17;100:1,4;115:4
Iraq (3)
48:9;83:4;87:19
Iraqi (3)
48:11;83:21;84:1
ISPs (1)
31:18
issue (4)
31:19;98:6;101:19;
109:12
issued (1)
75:11
issues (6)

5:8,10;29:8;31:18;33:5;
38:8
Item (2)
116:8,18
ITSM (1)
96:20

J

J2 (1)
85:12
J3 (19)
81:17,17,18;82:3,19;
83:10,16;85:10,14,17;86:6,
8;89:2,10,16,21;90:5;92:15;
93:16
J5 (7)
49:12;50:9,16;55:8;56:6,
17;58:1
J6 (6)
48:21;49:1;95:21;107:6,
15;109:3
J-6 (1)
98:9
JA (1)
111:4
Jacob (3)
94:14,20;105:13
JAG (7)
50:19;83:12;97:14;
100:20;109:7,15;113:14
JA-Investigations-Farah (1)
113:3
January (3)
103:1,5;104:17
JED (2)
90:16,17
JEDs (1)
90:18
Jessica (1)
8:19
John (3)
97:12;102:9,13
Johnson (2)
8:19,21
join (1)
27:8
joined (2)
27:9;47:11
Jones (1)
107:3
JS (1)
51:4
Judge (2)
107:5;111:1
Julian (2)
33:20;40:14
July (5)
18:15;27:9;99:21;100:3;
104:19
June (7)
7:12;17:10;21:17;46:13;
80:5;103:5;104:20

JWICS (1)
8:5

K

keep (3)
31:17,20;77:19
keeping (1)
41:7
kept (1)
16:18
key (8)
9:7;13:17;16:7;84:12;
87:11,17,20;91:21
keyword (1)
63:18
kidnapped (3)
82:8;88:16,18
kidnapping (1)
92:3
killed (1)
82:8
kind (10)
26:5,10,11,15,18;30:4;
36:3;61:20;63:14;67:21
knew (2)
101:12;109:10
Knowing (1)
9:19
knowledge (11)
15:6;16:18;32:5,12;
45:21;53:21;62:5;68:12;
72:18;76:5;79:20
known (4)
28:11;53:1;54:6,8
Kosovo (1)
80:21
Kuwait (1)
80:20

L

label (1)
100:15
labeled (4)
21:13;100:11;108:3;
116:7
lack (2)
91:3,4
landing (1)
47:20
language (8)
9:13,15;12:2,3,5;19:17,
18;31:4
laptop (12)
99:8;101:14,15,17;
107:11;110:9,12;112:14,18,
21;113:7;114:12
large (5)
65:9;70:13,14;71:1,10
largely (1)
75:10
larger (1)

33:15
large-scale (2)
55:18;92:11
last (5)
5:5;18:5;31:12;64:17;
72:1
Lastly (1)
106:6
late (1)
27:15
Later (4)
108:4;112:12;114:10,21
launch (1)
34:8
law (9)
9:8;24:4;59:14;103:11,
17,17;104:1,10,14
lawyers (1)
46:1
lay (3)
65:14;67:5;68:21
laying (2)
68:14;69:7
lays (2)
71:12,13
Lead (5)
8:6;18:16;48:7;95:2,13
leader (5)
84:12;87:11,17,20;92:1
leaders (3)
87:19;88:2,3
leadership (1)
12:21
leak (1)
34:15
leaking (1)
65:8
leaks (1)
75:10
learn (1)
72:4
learned (3)
70:17;72:4,8
least (2)
52:4;70:7
leave (1)
27:4
leaving (1)
48:15
left (4)
15:21;18:4;47:10;112:6
less (5)
43:12,15,21;45:12;65:3
letter (2)
110:13;114:13
level (6)
19:11;48:4;52:5;84:11;
86:6;112:6
levels (1)
95:6
liaison (1)
57:1
library (1)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

113:18
Lieutenant (7)
  46:12,18;47:2;80:4,7,11,
  17
likelihood (1)
  118:17
Likewise (1)
  10:11
limitations (2)
  53:8;87:6
limited (3)
  22:1;90:8;108:1
limiting (1)
  43:14
line (12)
  51:17,17;66:15;68:19;
  73:4,5,10;74:4;85:4,13,13;
  112:5
lines (2)
  36:9;43:17
link (4)
  110:16,20;111:2,4
links (1)
  14:11
list (3)
  5:12;65:10;67:18
listed (3)
  13:13;75:13;112:11
listener (1)
  32:7
listening (1)
  34:15
listing (4)
  5:14;112:2,6,9
lists (2)
  112:6,8
little (9)
  27:14;31:7;37:3;68:16;
  69:20;70:16;71:4;72:3;77:6
local (7)
  29:16;54:19;70:4;87:18;
  88:2,2;92:2
locate (1)
  88:17
located (8)
  20:20;55:8;56:7;89:2,10;
  92:15;100:20;109:6
locating (2)
  54:19;109:8
location (4)
  52:21;86:18;97:9;112:17
locations (11)
  52:11;53:13;54:7;55:3;
  86:19;88:7,11,13,19;90:16;
  91:18
locks (2)
  98:11;109:5
log (14)
  15:7;20:3;21:13;63:10;
  67:17,18;69:3;71:2;98:15;
  99:19,21;100:2,7;101:4
logged (4)
  10:5,9;14:17;47:13

Logger (1)
  96:16
logic (1)
  95:18
logical (4)
  112:21;113:2,5;114:15
login (1)
  113:15
logs (66)
  10:12;13:5,16;15:3,16,
  17;16:1,3;18:19;19:1,2,4,7;
  20:17,19;21:6,8,10,12,14,
  17,18,19,20;67:1,14;68:4,7,
  12,21;70:1;72:5,6,9,9,9,10,
  10,12,14,15,18;76:17,17;
  87:12;88:4,6;97:3;98:6,13,
  16,17;99:1,3,5,9,10;100:6;
  105:14;106:15;107:16,16;
  108:11,21;115:16,20
long (11)
  10:13;24:18;25:6,15;
  31:12;33:21;45:4;61:19;
  65:10;71:6;118:9
look (6)
  12:6;62:12;63:17;71:7,
  11;72:10
looked (5)
  10:14;21:6;51:15;76:17;
  77:4
looking (4)
  25:10;46:4;57:5;118:5
looks (4)
  63:15;73:7,13;74:5
loss (3)
  90:13;91:4;103:7
Louis (1)
  85:11
low (1)
  48:4
lunch (2)
  118:8,21

M

M3 (2)
  62:17;63:4
ma'am (54)
  5:4,10,16;6:2,10;7:1,3,6,
  6;17:5,9;22:5,13,15;23:6,8,
  9,14;32:3;33:6;36:19;
  38:13;45:13,15;46:6,10,11,
  15;58:19;59:1,7;65:19;
  66:7,12;68:16;69:4;76:13;
  79:13,17;80:1,3;94:3,7,10,
  16;101:20;102:2;117:8,13,
  20,21;118:7,11,19
MacDill (1)
  95:4
machine (1)
  77:4
machines (2)
  98:7;109:1
main (5)

30:18,19;31:11;34:7;
  113:16
maintain (2)
  18:1;106:6
maintained (2)
  16:14;116:12
maintaining (1)
  20:19
maintenance (2)
  10:17;99:2
Mairena (3)
  108:6;115:13;116:16
Major (6)
  5:2;22:6;23:2,2,4;75:9
makers (1)
  104:7
making (5)
  33:3;43:15,21;50:2;84:6
malicious (1)
  95:18
Malware (2)
  96:17;101:11
manage (1)
  27:2
Managed (1)
  26:20
Management (3)
  50:15;83:11;96:20
Manager (1)
  62:17
managing (1)
  26:12
Mander (13)
  59:8,9,12;64:2;67:7;
  69:12,14;73:3;74:13;75:15;
  76:16;79:11,18
manner (1)
  16:13
manners (2)
  12:13,20
Manning (4)
  23:7;51:7;65:21;82:21
manual (1)
  14:20
Manuals (2)
  50:6;84:10
many (10)
  29:18,20;30:2,13,14;
  31:8;33:16;62:6;71:13;
  75:20
maps (1)
  52:11
March (8)
  8:18;9:10;13:9,12,14;
  14:6,7;104:16
Marine (5)
  25:14,17;45:2,5;47:5
Marines (1)
  34:3
Maritime (4)
  47:6;48:17,20;49:14
MARK (2)
  59:12;102:4

marked (14)
  5:12;16:12,21;54:1;66:9;
  75:5;85:19;87:9;89:20;
  90:5;99:12;115:19;117:13;
  118:1
markings (3)
  52:4;86:6;106:1
Martin (2)
  80:5,8
Maryland (3)
  7:21;17:18;70:4
mass (1)
  65:7
Massachusetts (1)
  47:6
Master (1)
  8:15
Masters (2)
  47:7;80:14
match (1)
  99:10
matched (1)
  116:6
matching (1)
  106:2
material (11)
  50:3,4;74:18,21,21;84:7,
  8,11;107:1;111:13;115:7
materials (2)
  79:1;105:12
matter (1)
  81:17
matters (3)
  16:16,18;48:19
Matthew (4)
  23:10,19;24:2,7
May (16)
  17:7;18:21;22:6;23:11;
  36:20;55:16;58:16;69:4;
  73:21;84:11;92:8;94:5;
  102:3,4;104:2;117:2
maybe (6)
  30:14;38:3;44:9;61:18;
  68:2;70:16
McAfee (2)
  96:13,18
MD5 (1)
  113:3
MDSSHA1pdf (1)
  99:15
MDSSHA1txt (1)
  99:17
Meade (2)
  7:21;17:18
mean (2)
  29:8;74:7
means (2)
  10:8;15:1
measure (1)
  37:20
mechanism (1)
  61:2
media (9)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

5:17,18;6:8,12,14;62:16;
75:9;82:9,12
medium (1)
43:19
member (2)
88:18;92:3
members (8)
5:17;82:7,7,12;87:18;
88:1,10,17
mention (7)
40:11,16;41:11;43:20;
78:15,16;79:8
mentioned (6)
40:6,8;41:20;63:11;72:6;
100:19
mentions (1)
65:9
merits (6)
7:16;17:13;46:20;80:9;
94:20;102:14
meteorologist (1)
81:4
method (3)
9:16;11:20;19:20
methods (4)
54:14;74:21;75:1;91:10
metric (5)
12:21;13:11,14;14:20;
15:7
metrics (8)
10:3,19,20;11:21;13:18;
14:9;15:11,13
Mexico (2)
49:2;80:13
MG (1)
107:3
MI (5)
15:12;17:17,18;18:17;
21:13
Microsoft (4)
18:11,18;20:11;108:14
Microsoft's (1)
110:14
might (2)
29:15;118:15
MIIS (2)
18:18,21
mil (1)
36:10
militaries (1)
60:12
Military (35)
7:21;17:17;18:3,6;26:3;
27:6;45:1;50:12;52:6,15,
16;54:3;55:14;56:15;57:13;
59:21;60:5,15,21;77:12;
78:14,15,19;81:10;86:12,
13;87:18;88:7,20;90:7;
91:2,9,14;92:7;93:8
mind (1)
43:16
mindset (1)
85:2

Mining (1)
80:13
minute (4)
35:16;63:21;66:8;68:20
minutes (2)
59:3;118:11
mirror (5)
65:10;75:15,16,19;76:5
mirrors (1)
75:8
mission (13)
49:9,9;52:10,10,18;
54:17;57:1,6;86:16;87:12;
88:4,6;93:11
missions (3)
57:3;87:15;91:2
mobilization (1)
90:20
mobilized (3)
50:7,8,14
modification (1)
22:17
modified (3)
13:5;21:20;23:1
moment (4)
64:19;66:16;69:4;79:6
money (1)
43:21
monitoring (2)
24:16;25:9
months (2)
24:19;47:19
more (17)
33:2;37:12;39:17;41:11;
42:21;43:17;44:9;45:12;
61:12,14;65:3,9;68:15,16;
69:20;70:16;118:15
morning (9)
5:11,17;6:5;13:16;38:16,
17;69:12,13;110:7
Morrow (1)
5:6
MOS (3)
18:7;25:17;27:11
most (7)
9:14;10:4;13:13;19:18;
63:2;72:12;109:18
motion (1)
46:7
motivation (1)
15:5
move (1)
36:16
moved (1)
12:19
movement (3)
53:15;55:5;91:20
movements (6)
53:2;56:4,5;86:21;88:5;
93:12
moves (9)
17:3;22:2;58:6,10;73:16;
93:21;94:7;101:20;116:19

moving (1)
12:17
much (4)
6:1,3;68:6;71:9
Multi (1)
62:16
multiple (7)
30:6;54:3;61:20;87:11;
90:6;91:2;104:6
must (2)
97:20;108:19

N

name (5)
29:8;35:8;62:13;90:19;
91:7
named (15)
20:5;56:13;83:8,8;91:2;
93:4,5;113:2,6;114:1,2,4,6,
7,9
names (3)
88:16;112:1,10
naming (1)
20:11
National (5)
8:11;53:7;80:19;87:5;
104:17
nationals (2)
54:19;88:21
nature (4)
26:9,17;34:17;61:17
Naval (1)
47:8
navigate (2)
109:20;113:17
navigated (4)
110:1,14;111:15;112:2
navigating (1)
113:14
Navy (6)
46:13,19;47:3,10,12;
64:12
NCIS (1)
60:6
near (1)
16:15
necessarily (2)
36:1;43:16
necessary (1)
106:3
neck (1)
28:15
need (9)
5:8;6:20;10:16;22:12;
23:12;31:20;70:20;107:10,
12
needed (2)
37:12;107:2
Nehring (2)
80:5,8
neither (1)
15:5

net (10)
30:21;31:7,15,16;39:9;
40:5;42:18,19;43:21;44:19
network (27)
9:14,17,20;11:16;19:18,
21;20:2;26:12,16;27:12,13;
42:9;51:10;67:12;75:3;
83:4,5;95:8,9,11,17;96:3,
10,12,13;98:8;109:2
networks (7)
24:16;25:9;26:8,17;31:2;
96:21;105:5
neutral (2)
43:15,21
neutrality (9)
30:21;31:8,15,16;39:10;
40:5;42:18,19;44:19
neutralizing (2)
54:12;90:18
new (5)
17:21;34:9;35:21;36:2;
80:13
news (1)
75:9
next (5)
7:2,8;23:17;59:6;102:5
Nine (8)
16:11;18:3,5;52:6;87:8;
90:16;101:6;111:20
Nineteen (1)
91:5
none (1)
101:12
nor (2)
10:13;15:5
normally (1)
10:15
Northern (1)
48:19
note (1)
106:11
noted (4)
52:3;55:21;86:5;92:20
noticed (1)
28:14
notified (2)
9:9;13:8
November (4)
18:21;20:16;23:1,1
number (24)
7:8;11:8,9;13:21;15:21;
21:17;36:11;64:7,11,13,13,
16,16;65:9;78:21;100:11,
12;108:3,4;110:12;114:12;
115:6,6;116:8
numbered (1)
64:6
numbering (1)
64:8
numbers (12)
51:21;55:9;56:8;64:10,
15,17;86:2;89:3,11;92:16;
106:1;112:5

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

numerous (3)
18:11;26:3;75:6

O

oath (1)
59:10
object (4)
62:2,5;65:11;67:1
objection (17)
6:18,19;17:5;22:5;32:3;
36:19;58:9,13,21;72:17;
73:18;76:3;94:3,10;102:2;
117:1;118:19
observe (1)
60:21
obtain (3)
71:4,18;113:14
obtained (4)
47:5,7;104:13;113:4
obtaining (3)
71:9;72:15;110:5
Occasionally (1)
63:10
Occupational (1)
18:6
occupied (1)
98:4
occur (1)
28:19
occurred (7)
9:7;13:6;55:15,19;67:20;
92:7,12
occurrences (1)
16:16
occurs (1)
19:2
October (6)
51:21;86:2;104:9;115:18,
20;116:15
off (3)
31:2;37:16;69:6
offer (1)
70:16
offered (1)
70:7
offering (2)
33:8,9
offers (1)
80:1
offhand (1)
30:20
office (8)
15:14;50:9,16,19;60:6;
83:12;102:17;107:5
Officer (5)
15:12;56:19;57:11;96:1;
103:18
official (4)
74:16;75:5;81:19;116:1
often (5)
8:2;29:10;35:19,20;68:4
oil (1)

24:11
old (1)
18:1
Once (1)
79:18
one (50)
5:19;6:5,5,12;7:19;8:10,
11;9:9,18,19;13:8;14:11;
17:16;20:18;22:17;29:21;
30:20;31:11,11,13;33:3,15,
17;39:20,21;40:8;41:21;
42:14;46:5,5;47:2,16,17;
48:2;49:15,15;50:2;53:12;
55:2;61:19;62:13;63:7,11;
70:7;80:11;84:6;90:8;95:2;
102:16;117:18
ones (2)
18:1;30:20
Online (4)
11:4,13;35:19;75:1
Only (16)
9:18;10:5,9;11:1,16;13:3;
29:13;34:16;74:16;75:5;
82:12;97:19;98:9,17;
108:18;109:2
onto (6)
21:10;99:5,5,11;113:9;
114:17
open (11)
31:17,20;32:21;33:4;
42:5,9;43:4;44:12,15;50:3;
84:7
opened (5)
13:19;14:2,3,5,7
openness (1)
41:5
operated (1)
48:7
operates (1)
69:19
operating (1)
57:18
Operation (10)
48:10,11;53:4;55:14;
56:15;83:20;84:1;87:2;
92:7;93:8
operational (6)
52:17;86:15;93:1,10,11;
104:18
operations (23)
5:18;6:8;48:14;52:16,18;
53:3,16;55:6;56:19,21;57:4,
11;81:1,2,17;82:9;86:13,16;
87:1;91:15,17;95:7;96:16
OPORD (2)
53:4;87:2
opportunity (2)
29:13;68:11
options (1)
54:18
order (4)
5:12;51:16;95:11;107:9
orders (5)

48:15;53:4,5;87:2,2
org (1)
75:7
organization (8)
37:18;63:4;64:5,12,14;
65:4,6;110:16
organizations (3)
60:1,21;63:1
organize (2)
12:8;37:4
organized (9)
12:12,13,14,19;16:2,3;
37:5;61:13,20
original (4)
17:2;58:3;75:18;93:18
originally (1)
101:2
others (8)
31:2;51:9;60:7;62:18,19,
20,21;83:3
otherwise (1)
74:18
out (7)
14:14;27:19;28:16;65:3;
71:13,13;105:19
outbreaks (1)
95:18
outlets (1)
75:9
output (2)
14:20;15:1
outreach (1)
92:2
over (10)
9:14,16;19:17,19;47:13;
103:10;107:20;108:5;
115:12;116:16
Overgaard (1)
5:6
Overruled (6)
32:19;33:11;66:1;68:9;
72:21;76:6
Overseas (1)
95:7
overview (1)
65:1
over-written (1)
14:21
own (1)
11:21

P

Pacific (1)
47:4
page (27)
13:21;14:2,4,5,7;16:1,3,6;
22:19,20;35:17;97:10;
100:21;109:8,11;110:15,17,
21;111:2,4,5,8,11,16;
113:16,17;117:14
pages (3)
10:8;61:19,20

paper (1)
15:16
paragraph (12)
22:21,21;39:20,21;40:8;
41:21;74:15,16;75:4,5;
78:11,12
paragraphs (3)
74:13;78:1;85:15
part (5)
9:11;19:15;67:14;78:19;
93:3
partial (1)
22:21
participating (4)
53:2,12;55:2;86:18
particular (5)
9:3;11:18;57:16;77:4;
105:14
parties (3)
5:3,5;118:5
partners (2)
82:11,13
pass (1)
6:7
passed (1)
50:18
password (4)
113:16;114:1,3,8
pasted (1)
12:9
path (1)
111:18
paths (1)
112:1
patrols (1)
91:21
PAUSE (1)
22:14
PAXwmv (5)
56:13;83:9;93:5;114:2,7
PAXzip (6)
83:8;93:5;114:2,4,6,9
pdf (1)
10:11
PE (23)
15:15,16;16:12,15,18,21;
17:4,4;22:18;55:12,21;
56:11,12;89:9,15;90:6,6;
92:19,20;93:6;114:5,7;
116:17
pe1iaining (1)
51:6
people (10)
16:17;29:5,6;30:2,13,14,
15,16;33:16;60:20
perform (1)
95:15
performed (1)
99:10
performs (1)
17:18
perhaps (1)
68:2

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

period (1)
85:16
permanent (1)
45:17
Permission (1)
74:11
permissions (1)
21:21
person (2)
51:2;106:10
personal (4)
32:5;62:5;76:4;88:16
personally (2)
99:7;103:8
personnel (2)
98:9;109:3
pertaining (5)
49:12;52:9;82:20;100:1,3
Peter (3)
7:7,12,15
Petroleum (1)
80:12
PFC (2)
23:7;65:20
phases (6)
7:17;17:14;46:20;80:9;
94:21;102:14
Phoenix (1)
18:13
phone (1)
118:14
photograph (1)
110:6
physically (1)
98:7
piece (1)
43:1
PII (1)
103:8
pilot (5)
47:11,13;48:6;49:7,7
Pittsburgh (1)
104:15
PIX (1)
96:21
place (2)
22:9;105:20
placed (3)
113:6,9,11
placing (1)
114:14
Plaintiff's (1)
94:6
planes (1)
49:10
planned (1)
91:20
planner (1)
48:17
planning (7)
48:14;49:9,13;50:9;
52:10;56:20;95:9
plans (11)

48:14,15;49:12,13;50:11,
12,17;52:16;53:7;86:13;
87:4
Platform (1)
96:13
please (15)
5:2;7:2;17:7;35:16;
36:20;45:20;58:16;64:19;
66:15;73:21;74:13;79:19;
94:5;102:3;117:2
Plus (1)
18:10
PM (4)
14:2,4,6,8
point (7)
15:7;42:17;43:11;44:18;
65:4;108:6;115:9
Police (1)
103:18
policy (2)
27:1;101:10
political (5)
29:8;74:18;77:8;78:3,4
popular (1)
10:4
portal (4)
36:6,8;98:2;111:18
portion (1)
98:3
portions (2)
56:14;93:8
position (11)
8:9;24:18,20;26:2;50:10;
67:7;95:18;102:20;103:1,4,
16
positions (1)
6:16
positive (1)
116:12
possessed (1)
81:4
possession (4)
107:21;115:15,17;116:11
possible (2)
14:19;77:19
postal (1)
75:3
posted (7)
13:11;35:19,20;36:4,5,6;
75:6
Postgraduate (1)
47:8
posting (2)
36:1;65:5
postings (1)
75:8
potential (2)
38:2;44:3
potentially (3)
29:14;42:15;106:21
PowerPoint (1)
49:16
practice (2)

16:20;36:3
predecessors (1)
51:16
preference (1)
6:11
preliminary (1)
47:17
prepare (1)
107:9
present (9)
5:5,7;7:16;17:13;18:15;
46:19;80:8;94:20;102:13
presentation (8)
31:8,9,12;32:2,10;33:1,
13;40:17
presentations (5)
30:7,8,10,18,19
presented (1)
57:19
pre-sentencing (6)
7:17;17:14;46:20;80:9;
94:21;102:14
presenter (3)
31:11;33:7;40:13
presently (1)
5:19
presume (1)
85:3
pretty (2)
6:3;33:18
preventing (1)
31:18
previous (1)
5:14
Previously (9)
48:18;49:10;59:13;73:13;
90:10;100:19;101:17;
103:1;116:4
primarily (3)
26:16;81:20;103:12
primary (2)
47:16;75:21
printed (4)
10:13;16:10;76:18;112:5
printout (3)
15:17;111:21;112:2
Printouts (1)
12:5
prior (10)
7:3;8:8;15:7;24:20,21;
25:12,13;52:7;106:7;118:2
Private (2)
51:6;82:21
probably (4)
29:9;33:17;61:17;76:8
procedure (1)
36:2
procedures (8)
49:17;54:10;87:14;92:4;
105:17;106:9;107:21;116:3
proceed (5)
5:9;72:21;94:17;102:10;
118:6

PROCEEDINGS (1)
5:1
process (9)
14:16;16:13;62:4,7,9;
110:5;112:9;113:13;114:14
processed (1)
81:21
processing (2)
19:10;115:7
process-oriented (1)
84:13
produce (4)
60:16;61:8,12;63:1
produced (3)
10:18;16:10;108:14
produces (4)
8:1,2;10:3;15:1
product (17)
9:1,6;10:1,7;11:3,6,7,9,
11,12;13:20,20;14:12,13;
15:18,20;16:6
products (10)
8:1,3,4;9:3,10,21;10:4,4;
13:8;14:18
professional (3)
96:6,11,18
program (2)
70:8;102:19
programmed (1)
69:18
programmer (1)
8:13
programs (1)
92:2
projects (2)
53:6;87:4
proper (1)
108:20
properly (12)
52:4;53:10,16;54:21;
55:6;58:5;93:20;106:4,11;
108:5;115:12;116:15
Property (4)
100:9;105:18;108:2;
115:5
proposed (1)
5:13
proprietary (1)
34:17
prosecution (64)
5:13;7:7,8;15:15;17:6;
21:15;22:3,4,16;23:11,15;
34:18;35:13,15;36:14,17,
21;46:7,15;51:7,8;52:1;
58:7,8,11,12,16,17;63:19;
66:2,4,10,18;73:16,19;74:1,
10;76:18;77:14;78:2;79:2;
80:3;83:1,2;86:3;94:1,2,4,8,
9,11,14;100:5;101:21;
102:1,8;111:20;116:20,21;
117:3,5,16;118:1,3
protected (4)
82:18;98:11;109:4;114:1

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

87:12;88:4,6;91:6,17
reported (8)
54:5;90:12,12,14,15;91:3,
4,19
reporter (4)
22:18;66:17;79:12;
117:12
reporting (4)
44:12;50:4;75:10;84:7
reports (29)
35:19;52:17;54:1,13;
55:7,11;60:17;61:12;62:6;
63:1,2;86:15;87:9,12,15;
88:9,12,15,18;89:1,8,10,15,
17,20;90:1,4,12;91:1
Repotis (1)
111:14
representing (1)
36:11
request (4)
6:4;68:11;107:4,7
requested (5)
13:1;18:17;21:3;82:3;
114:3
requester (1)
14:14
requesting (1)
107:6
requests (4)
8:3;22:9;58:19;82:3
required (4)
15:6;50:20;83:13;113:15
requisite (1)
47:15
research (6)
24:17;26:14;28:13;32:17,
20,21
researchers (1)
29:6
Reserve (2)
46:13,19
reserved (1)
30:11
reserves (4)
27:8,10;47:3,12
reservist (4)
27:7;47:3;48:13;49:7
reside (1)
25:4
resided (1)
112:15
resources (1)
10:17
respect (1)
69:1
respecting (1)
69:9
respectively (1)
116:21
Responder (1)
96:17
responding (3)
54:11;88:12;90:17

response (6)
54:4;87:14;88:17;90:20;
95:14;105:4
responses (2)
87:15;91:11
responsibilities (1)
16:15
Responsibility (1)
95:8
responsible (5)
17:20;20:18;56:20;81:21;
95:6
restricted (2)
43:18;74:18
results (1)
63:13
resume (1)
71:7
retired (5)
8:14;80:5,8,11,19
retrieve (6)
77:14,17;79:11;101:8;
106:21;117:11
retrieved (2)
22:15;99:3
retrieving (7)
34:18;35:13,15;36:14;
63:19;66:2;74:1
returned (1)
13:14
reveal (3)
56:3;87:21;93:1
reveals (2)
93:10,11
reverse (2)
39:15;95:10
review (19)
35:16;50:16;51:14;56:16;
57:14,21;64:19;66:15;
67:14;68:4,5;71:19;82:6;
84:4;85:12,13;93:3,15;
105:18
reviewed (36)
21:11;51:4,5,17;52:5,8,
12,14;53:18,21;54:2;55:13;
56:12;57:3,5,7,8,10,12;
82:3,20;83:15;85:4,6,9,13,
16;86:7,8,11;89:16,21;90:5;
92:5;93:4,7
reviewing (3)
51:3;57:18;81:21
reviews (1)
82:10
rewritable (1)
21:10
right (25)
5:15;6:1;16:2;17:6;23:4;
31:14;43:2,3,11;45:16,19;
58:14,17,21;62:8;65:16;
66:6;68:13;72:20;79:16;
94:4,11;102:3;118:9,12
risks (1)
27:2

Robert (1)
18:16
Rock (1)
115:17
role (1)
105:7
Ron (1)
115:17
room (2)
30:12;33:14
rooms (3)
30:6,11;33:15
root (4)
113:6,9,11;114:18
roster (2)
98:12;109:6
roughly (3)
28:20;30:3,14
router (1)
68:3
rows (1)
12:7
rules (2)
54:15;79:19
runs (1)
10:21

S

S6 (1)
17:16
S-6 (1)
15:11
SA (8)
98:21;100:8;101:6,17;
103:2,5;109:17;115:16
same (13)
16:8;25:1,9;27:11,11;
46:5;70:11;72:10;73:13;
79:19;107:8;108:4;112:17
sat (1)
109:9
SATA (5)
101:8;110:11;114:11;
115:1,1
saved (13)
10:13;12:11;76:21;77:1;
99:4,11;110:17,21;111:3,5,
8,11,16
scanned (2)
101:10,17
Scene (1)
103:21
School (2)
47:8,16
schooling (2)
26:5;57:16
schools (1)
26:3
Science (2)
8:16;47:6
SCIF (1)
81:14

screen (25)
110:6,16,17,18,19,20,21;
111:1,2,3,4,5,6,6,8,9,9,10,
11,16,17,17;113:10;114:17;
115:3
screenshot (1)
110:4
screenshots (1)
110:3
Seagate (2)
110:11;114:11
Sean (1)
17:12
search (14)
12:8;21:1;63:5,5,8,9,11;
66:20;69:3;73:7,11,12;
104:20;109:11
searched (4)
11:6;21:3;65:20;107:2
searches (1)
69:17
searching (3)
11:7;12:16;21:2
seat (1)
30:13
second (10)
12:14;22:6;35:17;64:12;
80:17;85:6;101:4;114:11,
14,18
SECRET (10)
19:11;52:5;54:2;81:4,5;
86:6;87:9;89:20;90:5;
115:21
Secret/SCI (1)
96:7
secrets (2)
34:17;41:16
section (7)
17:19;36:10;37:9,17,21;
61:16;62:1
sections (1)
37:15
secure (4)
75:2;97:20;106:6;108:19
securely (1)
13:2
securing (2)
15:8;96:21
Security (31)
18:10;24:14;25:5;26:4,8,
8,13,21;28:14;29:5,8,15;
38:2;48:21;49:1;50:12;
53:8;85:8;87:5;89:19;90:3;
95:17;96:6,7,12,13,19;
104:4,18,19;108:20
Seized (1)
104:8
Seizure (1)
104:20
selected (2)
47:18;48:1
Senior (4)
95:20;96:1,2;102:16

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

sense (2)
  34:4;37:13
sensitive (8)
  56:3;57:13,14;65:5;
  81:13;85:20;92:21;103:7
sent (1)
  85:11
separate (3)
  12:13,20;82:10
separately (1)
  56:16
Sergeant (6)
  8:15;18:3;24:7,9;38:16;
  45:19
serial (4)
  64:16;105:21;110:11;
  114:12
series (1)
  109:21
serve (1)
  95:2
served (4)
  14:14;48:6,12;96:2
server (40)
  11:19;18:11,19;19:1,3,8;
  20:3,18,19;21:18,21;70:21,
  21;97:5,15;98:5,15,16,19,
  20;99:1;100:1,4,6,19;101:3,
  7;105:10,11,14;106:13,19;
  107:16,18;108:13,20;110:2,
  10;112:5;115:4
servers (7)
  13:3;17:21,21;20:18;
  26:8,12,17
service (11)
  18:6;31:18;64:14;81:7;
  82:7;88:1,10,17,18;92:3;
  96:20
Services (5)
  11:5,13;18:18;53:7;87:5
serving (1)
  80:16
session (1)
  6:6
set (9)
  12:13;16:16;64:15,15;
  70:13,17;71:6,10;118:13
Seven (6)
  14:9;51:2;85:6;90:14;
  100:7;108:10
seventeen (2)
  91:3;93:3
several (4)
  74:21;87:10;98:4;105:17
share (1)
  61:3
shared (1)
  84:11
Sharepoint (29)
  36:6,7;97:4,7,8,15,19;
  98:1,16,19,20;99:15,16;
  100:6,19,21;101:7;106:15;
  107:16,18;108:12,14,18;

109:8,20;110:2,10;111:18;
115:3
sharing (2)
  97:18;108:17
Shaver (1)
  109:17
Shawn (1)
  17:10
shop (2)
  17:17;107:15
short (1)
  61:18
shots (11)
  110:19,21;111:3,6,9,11,
  17,17;113:10;114:17;115:3
show (6)
  29:14;38:7;43:2,4;67:20;
  107:17
showed (2)
  73:14;111:17
showing (2)
  56:5;112:3
shows (4)
  19:13;61:21;101:2;
  111:21
side (2)
  16:1,2
SigAct (7)
  52:17;54:1;87:9;89:17,
  20;90:1,4
SigActs (7)
  52:19;53:19;54:2;86:15,
  16;87:9,10
Sight (1)
  96:16
sign (1)
  106:11
signature (1)
  100:13
signed (7)
  100:8,13;107:20;108:5;
  115:12;116:10,15
significance (5)
  74:19;78:4,7,10,14
significant (3)
  52:17;86:14;91:14
silver (1)
  115:19
similar (6)
  25:8;52:9;57:10;63:14,
  15;110:6
single (1)
  117:14
SIPRNET (17)
  8:5;11:17;19:12;21:1;
  97:5,10,17,19;98:3;100:20;
  101:3,15;108:16,19;109:7,
  11;110:15
Site (9)
  18:16;34:9;40:11;75:7,
  18;97:8,17;106:15,16
sites (1)
  65:10

Six (8)
  13:10;21:8;47:15;50:14;
  84:13;90:13;98:21;107:14
sixteen (2)
  91:2;92:5
SJA (1)
  113:18
skills (1)
  105:1
small (1)
  91:6
SME (2)
  81:18;82:19
smil (1)
  36:10
SNPA (1)
  96:21
software (11)
  8:7,12;9:2,3;10:1,5,9,19;
  14:10;70:8;104:7
someone (2)
  14:11;61:8
Sometimes (3)
  61:18,19;75:20
somewhat (1)
  63:15
sorry (3)
  30:17;65:19;70:12
sort (2)
  42:8;70:5
sound (1)
  109:18
source (6)
  44:12,15;50:3;68:19;
  84:7;90:10
sources (3)
  54:14;60:19;91:10
space (2)
  98:5;108:13
spaces (1)
  64:10
speak (2)
  22:6;33:21
speaker (1)
  33:3
speakers (2)
  31:8,10
speaking (5)
  43:8;61:8;65:2;67:12;
  70:19
special (11)
  25:20;59:8;60:6;67:8;
  97:12;102:9,13,16,18;
  107:3;110:20
Specialist (1)
  104:9
Specialty (2)
  18:7;47:18
specific (19)
  9:17,18;14:17,17;19:1,
  20;44:15;49:13;52:20,21;
  61:14;64:14;69:20;70:8;
  85:15;86:17,18;90:9;93:13

specifically (11)
  11:2;13:18;33:4;44:9,13;
  49:2;63:17;64:4;67:9;72:6;
  79:8
specifics (1)
  70:2
speech (1)
  44:4
spells (1)
  65:3
spent (4)
  39:4;49:17;71:14;80:18
spot (3)
  6:14,14,15
spots (2)
  6:12,13
spreadsheet (6)
  12:6,8,10,18,18;15:19
spreadsheets (3)
  12:12;16:9,10
SQL (5)
  12:2,2,6,10,17
Staff (7)
  18:3;24:9;38:16;45:19;
  107:3,5;110:20
standard (7)
  9:13;10:6;12:4;19:17;
  30:5;36:2;99:4
standards (1)
  82:11
stands (4)
  29:3;59:18;62:15,15
started (3)
  27:19;39:20,21
state (4)
  88:19;103:17;105:11;
  115:16
stated (7)
  88:15;90:13;91:1,7,13,20,
  20
States (40)
  5:11;17:3;19:8;22:2,8;
  23:9;36:16;41:10;46:13,19;
  47:3,4,10,12;48:19;49:2,15;
  50:8,11;51:6;54:16;58:6,10,
  19;59:7;73:15;74:17;80:1,
  12,16;81:12,19;82:20;
  88:14;93:21;94:7;101:20;
  105:9;116:19;118:7
States' (1)
  6:11
stationed (2)
  27:15,19
status (5)
  27:6;49:21;53:14;55:4;
  86:20
status-whereabouts (1)
  87:16
stay (1)
  28:14
stenographer (2)
  6:13,15
stenographers (3)

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

5:18;6:5,7

sticker (2)
115:21;116:1

still (6)
23:12;43:5;46:2;59:9;
68:6;82:18

stipulated (1)
102:8

stipulation (7)
7:7,11;17:9;22:17;46:11;
80:2,4

stipulations (1)
7:4

stop (2)
62:8;66:16

storage (3)
71:2;98:8;109:2

stored (1)
13:2

stores (1)
70:3

strike (2)
56:19;57:11

structure (1)
110:2

Structured (1)
12:2

students (1)
71:3

stuff (1)
68:3

Stuttgart (1)
27:17

subfolder (2)
112:8,10

subfolders (3)
112:7,11,14

sub-folders (4)
111:12,15;113:2,9

subject (4)
53:1;54:7,9;81:17

submission (3)
74:17,20;75:2

submit (2)
35:10,11

submitted (12)
35:11;50:19,21;51:3,9,
17;83:2,11,13,17;84:15,21

submitting (1)
74:21

subsequent (1)
110:4

Subsequently (1)
113:10

substantial (1)
103:15

substantially (6)
7:18;17:15;46:21;80:10;
95:1;102:15

substitute (1)
46:10

success (1)
118:18

suffered (2)
108:8;114:20

suggestions (1)
74:20

suggests (1)
78:12

suitable (1)
101:13

summarize (1)
38:6

summary (4)
32:16;37:8,10;61:15

super (2)
61:6;62:3

supervisor (1)
18:15

support (6)
10:17;17:20;34:14;48:10;
56:4;102:21

supporting (2)
98:5;108:21

Sure (3)
77:21;79:7;106:10

surrounding (2)
55:18;92:10

surveillance (2)
98:12;109:5

suspect (3)
91:13,14;109:14

suspects (2)
54:19;90:19

Sustained (1)
62:9

switch (1)
68:3

sworn (4)
24:3;51:20;59:14;86:1

Syllabus (3)
71:15,16,20

system (16)
8:21;14:12;15:1;19:3,14;
20:21;25:20;26:7;34:11;
35:21;36:3;57:20;61:6;
62:16;68:1;109:9

Systems (35)
17:16;18:8,9,13;21:9;
26:15,17,19,20;27:1,2,3;
52:11,16;53:6;54:14;57:18;
62:12,13,21;63:7,11;67:20;
86:13;87:3;93:2,13;96:5,8,
9,19;97:20;98:14;103:10;
108:19

T

table (3)
12:2,10,17

Tabs (1)
111:13

tactical (1)
84:11

tactics (4)
54:10;87:13;88:7,19

talk (19)
27:14;29:7;31:7,19;
32:16;33:13,16,19,20;34:2,
6,7;37:3,6;40:13;42:19;
43:17;77:11;118:14

talked (9)
30:21;31:1;34:10;72:3;
76:16;77:6,7;78:2;79:2

talking (2)
30:20;44:18

talks (4)
30:6;31:4;37:6;78:21

Tamara (2)
108:6;115:13

target (2)
57:7;91:7

targets (1)
57:2

TARP (1)
102:19

Task (3)
50:15;83:10;95:2

tasked (3)
50:15;51:3;83:10

tasker (1)
50:18

taskers (1)
50:17

taught (1)
71:3

TCP/IP (4)
9:13,14;19:16,18

teach (1)
26:6

Team (5)
8:6,7;13:4;95:14;99:2

technical (2)
39:18;96:3

techniques (2)
54:10;87:14

Technology (6)
18:17;80:14;96:8,9,20;
104:14

temporarily (2)
45:20;79:19

Temporary (3)
45:16,18;79:16

ten (5)
18:2;52:12;87:17;90:17;
112:12

terabytes (1)
98:4

term (2)
43:9;45:7

terrorism (4)
40:11,16;42:20;60:10

terrorist (6)
40:6,11;42:9,14,15;43:14

Terrorists (8)
11:5,14;40:19;41:21;
42:1;43:8;44:7,19

testified (2)
24:4;59:14

testify (12)
7:16,18;17:13,15;46:20,
21;80:8,10;94:20;95:1;
102:13,15

testimony (8)
7:12;17:10;22:18;45:21;
46:12;79:20;80:4;102:9

theaters (1)
82:9

Thereafter (1)
48:2

therefore (4)
10:19;11:6;12:9;114:3

third (2)
64:15;80:21

Thirteen (4)
56:12;88:15;90:21;
114:21

thirty (1)
91:17

thirty-eight (1)
92:3

thirty-five (1)
91:21

thirty-four (1)
91:20

thirty-one (1)
91:18

thirty-seven (1)
92:2

thirty-six (1)
92:1

thirty-three (1)
91:19

thirty-two (1)
91:19

Thomas (2)
46:12,19

though (3)
31:11;50:15;83:10

thousand (3)
30:15,16;33:17

threat (7)
24:17;26:14;38:2,3;
75:12;90:8;95:16

threats (2)
25:10;28:14

three (22)
8:7;9:11;13:3;19:13;
25:7;30:3;45:6;48:9,12,13;
64:13;70:7;74:14,15;78:1;
82:19;83:19;84:10;90:11;
97:1;105:7;115:2

throughout (4)
29:5;37:7;60:1;81:3

thrust (1)
44:18

TIC (1)
56:5

tiers (1)
31:21

Timelines (1)
111:14

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

89:13
00377886-00377905 (1)
89:14
00377888-00377910 (1)
55:10
00377907-00377910 (1)
89:14
00377912-00377918 (1)
89:4
00377921-0377933 (1)
89:4
00377935- (1)
89:4
00377960-00377963,00377965-00377980 (1)
89:6
00377983-00377986 (1)
89:7
00377988-00378013 (1)
89:7
00378016-00378026 (1)
89:8
00378029 (1)
56:9
00378029-00378081 (1)
92:18
00378066 (1)
56:9
00378071 (1)
56:9
00378079 (1)
56:10
00378082 (1)
56:10
00411111 (2)
100:12;108:4
00411113 (1)
115:6
00411151 (1)
116:8
00449439 (1)
21:17
00527370-00527377 (1)
86:3
00527378-00527397 (1)
52:1
06 (1)
75:5
08 (1)
64:17
0930 (1)
5:16

1

1 (6)
14:2,5;96:15;99:21;
100:3;116:18
1:30 (2)
118:18,20
10 (2)
46:13;80:5
106 (1)
94:15

108 (5)
100:5;101:21;102:1;
118:1,3
11:31 (1)
14:8
11-0006 (1)
21:14
111 (1)
46:16
112 (1)
80:3
12 (1)
80:18
122-10 (2)
100:11;108:4
123-10 (1)
115:6
13 (2)
56:1;115:20
131.240.47.23 (2)
98:1;115:4
131.240.47.6 (2)
98:2;100:2
131.240.47.7 (2)
98:2;100:5
13526 (1)
51:16
14 (1)
74:6
15 (2)
115:17;118:11
151-10 (2)
116:7,18
15-6 (6)
55:14,16;83:7;92:6,8,14
16 (2)
13:14;80:18
17 (2)
8:18;13:12
1700 (1)
47:13
18 (1)
116:15
19 (11)
20:16;23:1,1;66:15;
68:19;73:4,5,10;74:4;86:2;
107:7
19-20 (1)
97:2
1982 (1)
80:14
1985 (2)
80:17;81:7
199.32.48.154 (1)
19:9
1990 (1)
103:19
1995 (1)
80:15
1997 (1)
47:5
1998 (1)
47:10

1A12 (1)
35:17

2

2:40 (1)
14:4
20 (7)
21:14;59:2;107:19;110:7;
112:12;114:10;115:11
2000 (3)
104:17,19,20
2001 (3)
80:20;104:10,16
2001-02 (1)
48:10
2002 (3)
80:21;103:18;104:15
2003 (1)
96:10
2003-04 (1)
48:10
2005 (1)
103:17
2006 (3)
27:20;65:4;81:1
2007 (4)
47:7;96:19,20,21
2007-09 (1)
56:19
2008 (5)
13:11;48:10;96:6,18;
104:2
2009 (14)
14:2,4;18:21;23:2;27:15;
28:20;47:10,12;48:16;
55:16;81:11;92:8;99:21;
107:19
2010 (32)
8:18;9:10;13:9,13,14;
14:6,7;18:21;20:16;23:1;
27:5,16;74:6;96:18;97:2;
99:21;100:3,3;103:5;105:3,
6;107:7,8,19,20;110:8;
112:12;114:10;115:12,18,
20;116:15
2011 (6)
18:15;50:7;51:21;86:2;
96:17;105:4
2012 (8)
21:17;27:9;80:19;81:11;
96:15,15;103:1,5
2013 (6)
7:13;17:10;46:13;80:5;
96:11,14
21 (4)
21:17;51:21;53:19;55:7
22.225.41.22 (4)
14:7;18:20;20:14,15
22.225.41.40 (7)
14:1,3,5;18:20;20:15,16;
73:10
2334 (1)

74:6
2651 (2)
25:18;26:10
26th (1)
28:20
28 (1)
20:14
29 (1)
14:4

3

30 (2)
99:21;100:3
30th (1)
28:21
320 (1)
47:14
33W (1)
18:7
36 (1)
89:9
391 (1)
64:13
3NFODYJI (1)
110:12
3NFOHTG4 (1)
114:12

4

4 (2)
55:15;92:8
40 (2)
51:5;71:8
400GB (2)
110:11;114:11
4137 (4)
100:9,10;108:3;116:7
43 (6)
34:18;35:13;36:17,21;
46:4,8
44 (2)
46:4;117:18
46ell229a5d678cabf9c3fa6839f662c (1)
113:4

5

5,000 (1)
30:3
5.0 (1)
96:16
500 (2)
30:16,17
501 (5)
55:9;56:7;89:3,11;92:16
53 (1)
89:1
5391001408 (1)
64:7
5-6 (1)
51:12

United States vs.
PFC Bradley E. Manning

UNOFFICIAL DRAFT
6/11/13 Morning Session

- Vol. 5
June 11, 2013

566 (1)
5:12

6

6.14.3 (1)
112:20
6:31 (1)
14:2
6:40 (1)
14:6
63 (9)
15:15,17;16:12,15,18,21;
17:4,4,7
64 (6)
21:15;22:3,4;23:11,14,15
65 (3)
111:20;116:20,21
66 (9)
56:12;58:11,12,16,17;
93:6;114:5;117:6,7
67 (7)
114:7;116:20,21;117:3,5,
10,17
68 (4)
116:17,20,21;117:16
69 (2)
6:13,16

7

7 (2)
14:7;105:2
70 (3)
6:12,16;7:8
70th (1)
6:14
71 (3)
7:9;22:16,18
72 (1)
102:8

8

85 (6)
35:15;36:15;66:4,10,18;
74:2
86 (5)
20:13;86:3;94:8,9,12
87 (4)
52:1;58:7,8,17
88 (6)
89:9;90:6;94:1,2,5,6
89 (7)
55:12;89:15;90:6;94:1,2,
5,6

9

9 (3)
7:12;17:10;107:6
90 (7)
55:21;56:11;92:19,20;

94:8,9,12
902nd (6)
7:20;15:12;17:17,18;
18:17;21:13
99 (7)
63:19;66:3;73:16,19;
74:10;76:18;77:14