

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

STIPULATION OF
EXPECTED TESTIMONY

Mr. Patrick Hoeffel

10 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Patrick Hoeffel were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows.

1. I am a software engineer at Intelligent Software Solutions, Inc., Colorado Springs, Colorado. I design and write software systems, such as the Combined Information Data Network Exchange (CIDNE) database, and manage eight other individuals who also write software code for CIDNE. In 1989, I earned my Bachelor of Science degree in Computer Science from Catholic University in Washington, DC. During the time I was attending school, I worked from 1987 to 1989 in the school computer lab as student help desk support. Also, in 1989, I worked for a rent control apartment management company writing software. From 1989 to 1997, I worked in Columbus, Ohio, as a software engineer for a company called Compuserve, which was bought by America Online (AOL). From 1997 to 1998, I additionally worked as a consultant for Compuware, contracted to MCI, which is now Verizon.

2. In 2000, I received 80 hours of course instruction on the Design and Maintenance of Structured Query Language (SQL) Server Databases and Systems. This instruction provided foundational knowledge for my work as a software and database engineer. From 1998 to 1999, I worked at software start-up company called TribalVoice. At TribalVoice, I was a software engineer.

3. From 1999 to 2006, I worked at a software startup company called ConfigureSoft, in Colorado Springs, Colorado. I worked at ConfigureSoft as a software engineer with an emphasis on the design of database systems. I also designed databases and software systems to be used by systems administrators. As a database and software designer, I became familiar with systems administration.

4. I have worked at Intelligent Software Solutions, Inc. since September 2006. During my time at Intelligent Software Solutions, I have spent two years as the lead CIDNE engineer in theater and at corporate headquarters. I have been responsible for the management of day-to-day CIDNE engineering operations. I have managed approximately 20 individuals that range from software engineers, to database engineers, testers, and system administrators.

5. I have no military experience, but I have deployed as a contractor with Intelligent Software Solutions, Inc. I deployed to Victory Base Complex (VBC), Iraq from September 2007 to December 2007 as a software engineer working on the CIDNE database. I deployed again from

PROSECUTION EXHIBIT 111 for identification
PAGE OFFERED: PAGE ADMITTED:
PAGE 1 OF 4 PAGES

May 2009 to September 2009 to the VBC, Iraq, working as a software engineer on the CIDNE database. From May 2010 to August 2010, I deployed to Kabul, Afghanistan as a theater technical lead working on the CIDNE database. I last deployed from May 2011 to September 2011 to Kabul, Afghanistan as a theater technical lead working on the CIDNE database. I have over 25 years of computer science expertise developed through courses and experience.

6. I am familiar with the CIDNE software and the database in particular because I developed the database. CIDNE is a centralized database that stores information about events, people, organizations, and facilities, and makes that information available to users throughout Iraq, Afghanistan, and the United States. There are different CIDNE databases for Iraq and Afghanistan. The Iraq server at United States Central Command (USCENTCOM) Headquarters (HQ) is physically distinct from the Afghanistan server. The two do not share data with each other. The Iraq data is stored in a series of servers that are positioned at various locations in Iraq, with all data being constantly copied back to a CIDNE-Iraq server at USCENTCOM HQ in Tampa, Florida, for use by interested entities. All data is the same across all Iraq servers. Afghanistan data is stored in a series of servers that are positioned at various locations in Afghanistan, with all data copied back to a CIDNE-Afghanistan server in Tampa. This setup was created to make data available as broadly as possible.

7. CIDNE can be accessed through one of the seven different classified networks, including SIPRNET and JWICS. CIDNE is only available on classified networks. CIDNE data is accessed using a CIDNE web site. To see Afghanistan data, one must open a CIDNE-A web page on a CIDNE-Afghanistan server. Likewise, Iraq data must be accessed via a CIDNE-I server through a CIDNE-I web site. During the 2009-2010 timeframe one could access a database by logging in as self-registered or as a guest user to browse. As of today, capabilities were developed to see who views data and an enhanced log-in system was designed for access to the CIDNE database. One can no longer browse the database without logging in as a self-registered user. Prior to the recent log-in requirements, the CIDNE databases did not track individual users' access by IP address or otherwise.

8. CIDNE reports are individual reports of specific unit actions. CIDNE is the USCENTCOM directed reporting tool for the majority of operational reporting in Iraq and Afghanistan. It is a structured collection of data with over 100 different types of reports, including Significant Activity reports (SIGACTs). SIGACTs are only one report type in CIDNE, but it is one of the most frequently used type of report along with Human Intelligence (HUMINT) and Counter-IED (C-IED) reports. SIGACTs are often used because of their content. SIGACTs are summaries of actual events created at the time of those events. The reports state the who, what, when, and where of events encountered by the unit.

9. A user can create a report only if the user's unit administrator grants the authority to populate reports on the system. Any user with access to CIDNE on a classified network could browse the information. During the 2009-2010 timeframe, the CIDNE database did not record who looked at the data. Instead, CIDNE only recorded who was creating reports and what types of reports were being created. As the theater technical lead in Afghanistan, I frequently worked with users who created reports and the types of reports the users created. CIDNE requires reports have certain fields completed. The database will not accept a report unless the required fields are

completed. Classification is a mandatory field with unclassified, confidential, and secret as the options. Thus, all reports, including all SIGACTs, are marked with a classification. Once a report is entered into CIDNE, the database assigns a unique value called a "report key" that is used by the database to identify individual reports and allows the user to quickly query the database.

10. In August 2010, I was tasked to participate in the Information Review Task Force (IRTF) at the Defense Intelligence Agency (DIA) based on my CIDNE expertise. My original task was to verify and confirm that the compromised data came from the CIDNE-A database, and later I also was tasked to review the CIDNE-I database. As a part of the IRTF, I identified the source of the compromised data, the time frame in which the data was taken based on examination of the released data, and data in the source database. Using computer software, I compared the compromised CIDNE-A report keys to the report keys in the original database. Based on my comparison, I concluded the hundreds of thousands of compromised report keys and the original report keys on the CIDNE-A database were identical. I spent about two weeks on the IRTF initially. I returned to the IRTF in November 2010 after the CIDNE-I database was released. I repeated the comparison procedures for CIDNE-I. Using computer software, I compared the compromised CIDNE-I report keys to the original report keys in the database. Based on my comparison, I concluded the tens of thousands of compromised report keys and the original report keys on the CIDNE-I database were identical.

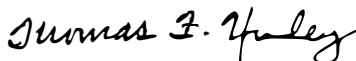
11. At the bottom of the CIDNE database search query results screen, CIDNE allows a user to export SIGACTS into a ".csv" format. CIDNE only exports one month at a time. This export function is available for users to download specific information in order to use the information with other programs or systems. During my investigation, I determined that the last of the compromised CIDNE-A data was pulled from the CIDNE-A System in the 57 seconds between 11:51:30Z and 11:52:27Z (Zulu time). Afghanistan servers are all set to Zulu time, and thus the reported dates are all in Zulu time. The compromised data from CIDNE-A was pulled before 7 Jan 2010 11:52:27Z because that is the date and time of the first update made to a report where the update did not appear in the compromised data. The compromised data was pulled from the CIDNE-A system after 7 Jan 2010 11:51:30Z because that is the date and time of the last update made to a report where the update appeared in the compromised data. Every modification prior to that time appears in the compromised data.

12. The compromised Iraq data was pulled from the CIDNE-I system in the 14 minutes and 51 seconds between 04:39:13C and 04:54:04C (Iraq time). Iraq servers are set to local time and record their dates in local time, which is Zulu+3 on 3 Jan 2010. The compromised data from CIDNE-I was pulled before 3 Jan 2010 04:54:04C. The first data modification that does not appear in the compromised data occurred at 3 Jan 2010 04:54:04C. Every modification prior to that time appears in the compromised data, while all modifications at this point and following do not appear in the compromised data. The compromised data from CIDNE-I had to have been pulled after 3 Jan 2010 04:39:13C. The last modification to appear in the compromised data occurred at 3 Jan 2010 04:39:13C. Every modification including and prior to that time appears in the compromised data.

13. At no time was the SIGACT information charged in this case unavailable for access on the CIDNE database. Those that accessed the SIGACT database before May of 2010 did so in the same manner after May of 2010. We continue to use the SIGACTs charged in this case in the CIDNE database. To the best of my knowledge, the United States Government has never made these databases publicly available.



ALEXANDER VON ELTEN
CPT, JA
Assistant Trial Counsel



THOMAS F. HURLEY
MAJ, JA
Military Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused