

V.

**Government Response
to Defense Motion for
Directed Verdict:
Charge II, Specifications
4, 6, 8, 12, and 16
(18 U.S.C. § 641)**

11 July 2013

LEGAL AUTHORITY AND ARGUMENT

The United States submitted evidence relevant to the § 641 specifications that was admitted. The Defense argues that the United States has failed to satisfy the standard set forth in RCM 917(d). The admitted evidence establishes a reasonable inference that the accused stole and converted the databases and records listed in the § 641 specifications. The Defense argues that the § 641 specifications constitute fatal variances lack merit because the evidence proves the contents of the databases and the records were stolen or converted. The evidence does not constitute a material variance. Additionally, the Defense had adequate notice and ability to prepare the accused's defense for trial.

I. EVIDENCE ADMITTED AT TRIAL RELEVANT TO § 641 SPECIFICATIONS

A. R.C.M. 917 Background

"The military judge, on motion by the accused or *sua sponte*, shall enter a finding of not guilty of one or more offenses charged after the evidence on either side is closed and before findings on the general issue of guilt are announced if the evidence is insufficient to sustain a conviction of the offense affected." RCM 917(a). The motion by the accused shall state with specificity where the evidence is insufficient to enable the trial counsel to respond to the motion, and the Court shall give each party an opportunity to be heard on the matter. *See* RCM 917(b); RCM 917(c); RCM 917(c), discussion (stating that the military judge ordinarily should permit the trial counsel to reopen the case as to the insufficiency specified in the motion).

A motion for a finding of not guilty "shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." RCM 917(d). The Court shall view the evidence "in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id*; *United States v. Perez*, 40 M.J. 373 (C.M.A. 1994) (upholding the military judge's decision not to enter a finding of not guilty because the testimony of three witnesses, construed in the light most favorable to the prosecution, could reasonably tend to establish the overt act). The standard of "some evidence" required to survive a motion for a finding of not guilty is a low one. *See United States v. Escochea-Sanchez*, 2013 WL 561356 (N-M. Ct. Crim. App. 2013) (concurring with the military judge who "noted repeatedly while hearing argument on the RCM 917 motion [that] the standard for surviving such a motion is very low"); *United States v. Jenkins*, 59 M.J. 893, 898 (A. Ct. Crim. App. 2004) (encouraging trial judges to view the standard used to decide whether to grant a motion for a finding of guilty as a mirror image of the standard used to decide whether to give an instruction on an affirmative defense); *United States v. Athearn*, 1994 WL 711894 (A.F. Ct. Crim. App. 1994) (noting that "[t]he military judge was obviously correct in denying the motion for a finding of not guilty under the low, 'some evidence' standard set out in R.C.M. 917(d)") (quoting RCM 917(d)). Direct or circumstantial evidence satisfies the "some evidence" standard. *See United States v. Parker*, 59 M.J. 195 (C.A.A.F. 2003); *United States v. Varkonyi*, 645 F.2d 453, 458 (5th Cir. 1981).

B. Relevant Evidence Admitted

Relevant evidence is evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence. Military Rule of Evidence (hereinafter "MRE") 401. Relevant evidence is necessary when it is not cumulative and when it would contribute to a party's presentation of the case in some positive way in a matter at issue. The military judge has the initial responsibility to determine whether evidence is relevant under MRE 401. *See United States v. White*, 69 M.J. 236 (C.A.A.F. 2010). Elements of charged offenses are relevant and defined by the specification. *See* Rule for Courts-Martial 307(c)(3) (defining a specification as a plain, concise, and definite statement of the essential facts constituting the offense charged).

In the Defense Motions, the Defense does not dispute that the Combined Information Database Network Exchange (hereinafter "CIDNE")-Iraq database, CIDNE-Afghanistan database, United States Southern Command (hereinafter "USSOUTHCOM") database, Department of State Net-Centric Diplomacy (NCD) database, and United States Forces- Iraq Microsoft Outlook/SharePoint Exchange Server global address list (hereinafter "USF-I GAL") belonged to the United States or a department or agency thereof. Further, the Court took judicial notice that 18 U.S.C. § 641 was in existence on the dates alleged in Specifications 4, 6, 8, 12 and 16. *See* AE DLXXXVIII; AE DLXXXVIII(a).

The accused was not authorized to give classified information to the WikiLeaks organization. *See, e.g.*, PE 59; PE 60; Testimony of CPT Fulton; Testimony of Special Agent (hereinafter "SA") Mander; Testimony of Ms. Glenn; Testimony of SSgt Hosburgh. The Court took judicial notice that WikiLeaks posted records from the CIDNE-Iraq database, CIDNE-Afghanistan database, and USSOUTHCOM database. AE DLXXXVIII. SA Bettencourt confirmed that WikiLeaks posted the purported Department of State records from the NCD database. *See* PE 76.

1. Specification 4 of Charge II

The United States presented evidence that "at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: the Combined Information Data Network Exchange Iraq database containing more than 380,000 records." *See* AE CDX. SA David Shaver testified that the accused stole, purloined, or knowingly converted more than 380,000 records from the CIDNE-Iraq database on a Secure Digital (SD) card. *See* Testimony of SA Shaver. SA Shaver testified that these records were stored in a folder entitled "yada.tar.bz2.nc" with the filename "irq_events.csv." *See id.* The folder entitled "yada.tar.bz2.nc" and its contents were admitted into evidence. *See* Prosecution Exhibit (hereinafter "PE") 92. On 2 November 2010, SA Mark Mander collected this SD card from the home of Ms. Debra Van Alystne, the aunt of the accused. *See* PE 78; PE 113. On 3 November 2010, Ms. Tamara Mairena received this SD card from SA Mander and, on 10 December 2010, released the SD card to SA Shaver for examination. *See* PE 29. This SD card contained a picture of the accused, in addition to more than 380,000 records from the CIDNE-Iraq database. *See* PE 40; PE 113. The SD card was admitted into evidence. *See* PE 92.

The accused admitted to this misconduct to Mr. Adrian Lamo. *See* PE 30. When asked “(04:34:14 PM) info@adrianlamo.com: what do you consider the highlights?[,]” the accused admitted “(04:35:31 PM) bradass87: The Gharani airstrike videos and full report, Iraq war event log, the “Gitmo Papers”, and State Department cable database . . .” *See id.* at 46.

The United States presented evidence that “the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records.” *See* AE CDX. The SD card with which the accused stored the records from the CIDNE-Iraq database contained a document entitled “README.txt.” *See* Testimony of SA Shaver. The “README.txt” document was last written on 9 January 2010. *See id.* With this document, the accused identified the contents of the SD card to include the “Iraq and Afghanistan Significant Activities (SIGACTs) between 0000 on 01 JAN 2004 and 2359 on 31 DEC 2009.” *See* PE 42. The accused also recommended that the recipient “might need to sit on this information, perhaps 90-180 days, to figure out how best to release such a large amount of data, and to protect source.” *See* PE 42. Mr. Troy Moul, the accused’s instructor at Advanced Individual Training (AIT), testified that, during AIT, the accused received substantial training on the definition, marking, and proper handling of classified information. *See* Testimony of Mr. Moul. The PowerPoint slides that the accused received at AIT were admitted into evidence. *See* PE 52. The accused also executed several Non-Disclosure Agreements (NDAs), whereby the accused acknowledged his responsibility not to disclose classified information to unauthorized persons. These NDAs were admitted into evidence. *See* PE 59; PE 60. Every member of the accused’s unit, who testified, stated that Soldiers were not authorized to remove classified information from the Sensitive Compartmented Information Facility (SCIF). *See* Testimony of CPT Casey Fulton; Testimony of CW2 Kyle Balonek; Testimony of COL David Miller.

Executive Order (EO) 13526, which the Court took judicial notice of, verifies that classified information may not be removed from official premises without proper authorization. *See* EO 13526 § 4.1(d); AE CDX. EO 13526 also states that “[i]nformation may be originally classified only if...(2) the information is owned by, produced by or for, or is under the control of the United States Government.” *See* EO 13526 §1.1. Army Regulation (AR) 380-5, paragraph 2-8, which the Court took judicial notice of, also states that “U.S. classification can only be applied to information that is owned by, produced by or for, or is under the control of, the United States Government.” *See* AR 380-5 at ¶ 2-8.

The accused made many admissions to Mr. Lamo that establish a reasonable inference that the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records. A sampling of the relevant statements, in chronological order, is set forth below:

- i. “(12:22:49 PM) bradass87: the air gap has been penetrated , . . =L[.]” PE 30, at 8.
- ii. “(12:26:09 PM) bradass87: lets just say *someone* i know intimately well, has been penetrating US classified networks, mining data like the ones described... and been transferring that data from the classified networks over the “air gap” onto a commercial network computer... sorting the data, compressing it, encrypting it, and

uploading it to a crazy white haired aussie who can't seem to stay in one country very long =L[.]” PE 30, at 8.

- iii. “(1:34:11 PM) bradass87: waiting to redeploy to the US, be discharged... and figure out how on earth im going to transition
(1:34:45 PM) bradass87: all while witnessing the world freak out as its most intimate secrets are revealed[.]” PE 30, at 10.
- iv. “(03:07:01 PM) bradass87: i just... couldnt let these things stay inside of the system... and inside of my head...[.]” PE 30, at 26.
- v. “(02:23:25 PM) bradass87: i could’ve sold to russia or china, and made bank?
(02:23:36 PM) info@adrianlamo.com: why didn’t you?
(02:23:58 PM) bradass87: because it’s public data
(02:24:15 PM) info@adrianlamo.com: i mean, the cables
(02:24:46 PM) bradass87: it belongs in the public domain
(02:25:15 PM) bradass87: information should be free
(02:25:39 PM) bradass87: it belongs in the public domain[.]”

PE 30 (ellipses in original).

The United States presented evidence that “the records were of a value greater than \$1,000.” See AE CDX. The parties entered into a stipulation of expected testimony for Mr. Wyatt Bora. See PE 115. This evidence confirms the following:

- i. “In 2007, the program spent approximately \$900,000 on data management in Iraq. In 2008, the program spent approximately \$1,000,000 on data management in Iraq. In 2009, the program spent approximately \$4,200,000 on data management in Afghanistan and \$1,800,000 on data management in Iraq. In 2010, the program spent approximately \$3,600,000 on data management in Afghanistan. In 2011, the program spent approximately \$3,000,000 on data management in Afghanistan and \$570,000 on data management in Iraq. In 2012, the program spent approximately \$5,000,000 on data management in Afghanistan. These data management costs are directly associated with keeping the data useable on the classified networks.”
- ii. “In 2005, the program spent approximately \$1,100,000 for development and testing in Iraq and \$1,800,000 in development and testing in the Continental United States (CONUS). In 2006, the program spent approximately \$1,770,000 for development and testing in Iraq and \$790,000 in development and testing in CONUS. In 2007, the program spent approximately \$1,320,000 for development and testing in Iraq and \$1,810,000 in development and testing in CONUS. In 2008, the program spent approximately \$950,000 for development and testing in Afghanistan, \$2,690,000 for development and testing in Iraq, and \$3,610,000 in development and testing in CONUS. In 2009, the program spent approximately \$2,760,000 for development and testing in Afghanistan, \$3,280,000 for development and testing in Iraq, and \$5,500,000 in development and testing in CONUS. In 2010, the program spent

approximately \$4,200,000 for development and testing in Afghanistan, \$2,650,000 for development and testing in Iraq, and \$4,980,000 in development and testing in CONUS.”

- iii. “In 2007, the program spent approximately \$720,000 on hardware in Iraq. In 2008, the program spent \$560,000 on hardware in Afghanistan and \$190,000 on hardware in Iraq. In 2009, the program spent approximately \$1,660,000 on hardware in Afghanistan and \$520,000 on hardware in Iraq. In 2010, the program spent \$760,000 on hardware in Afghanistan. In 2011, the program approximately spent \$180,000 on hardware in Afghanistan. In 2012, the program spent approximately \$3,680,000 on hardware in Afghanistan.”
- iv. “In 2005, the program spent approximately \$1,100,000 for Iraq training. In 2006, the program spent approximately \$1,180,000 for Iraq training and \$480,000 for CONUS training. In 2007, the program spent approximately \$2,570,000 for Iraq training and \$200,000 for CONUS training. In 2008, the program spent approximately \$1,850,000 for Afghanistan training, \$5,220,000 for Iraq training, and \$1,550,000 for CONUS training. In 2009, the program spent approximately \$5,360,000 for Afghanistan training, \$6,370,000 for Iraq training, and \$3,660,000 for CONUS training. In 2010, the program spent approximately \$8,140,000.00 for Afghanistan training, \$5,150,000 for Iraq training, and \$3,320,000 for CONUS training. In 2011, the program spent approximately \$18,410,000 for Afghanistan training, \$2,650,000 for Iraq training, and \$6,150,000 for CONUS training. In 2012, the program spent approximately \$8,790,000 for Afghanistan training and \$2,740,000 for CONUS training.”
- v. “From 2005 through 2012, the CIDNE program spent approximately \$181,160,000 on contracted support required to run the program, to include development, training, data management, and hardware. In addition, from 2005 through 2012, the program spent approximately \$5,434,800.00 on program management support, to include government testing, administrative oversight, and research and development.”

See id. Mr. Danny Lewis also testified that the value of these records is greater than \$1,000. *See* Testimony of Mr. Lewis.

The United States presented evidence that “under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.” *See* AE CDX. COL Miller, the Brigade Commander for 2d Brigade Combat Team (BCT), 10th Mountain Division, testified that he was “stunned” when he learned of the accused’s misconduct because the last thing he anticipated was an internal security breach from one of their own. *See* Testimony of COL Miller. COL Miller testified that the impact to the brigade’s morale was significantly affected. *See id.* Before learning of the accused’s misconduct, COL Miller explained that the brigade’s morale was at its highest point since he took command because many of the Soldiers assigned to the unit had deployed multiple times and, having been tasked as the first BCT responsible for drawdown in Iraq, the Soldiers were seeing the fruits of their labor over the past ten years coming to fruition. *See id.* COL Miller testified that the accused’s misconduct was prejudicial to good order and

discipline because the atmosphere throughout the brigade as a result of the accused's misconduct was like that of a "funeral" –full of anger, sadness, grief, and frustration. *See id.* COL Miller also testified that the impact to the brigade's trust with one another was significantly affected. *See id.* COL Miller testified that trust is critical in theater and, similar to how Soldiers must trust one another in a combat patrol, trust is crucial among Soldiers in the S-2 section for safeguarding classified information. *See id.* The accused's acts as described by COL Miller, to include, *inter alia*, the harm to trust among Soldiers, caused discredit. Furthermore, the accused's admission of the world's awareness of the records he compromised caused discredit. *See* PE 30.

Lastly, Mr. Jason Milliman testified that having a large amount of information stored on one's desktop caused problems with the Distributed Common Ground System-Army (DCGS-A) computers in theater. *See* Testimony of Mr. Milliman. Mr. Chad Madaras, a former Soldier who worked on the day shift and shared a classified government computer with the accused in theater, testified that he observed the size of the accused's desktop and testified that it was large and filled with many items. *See* Testimony of Mr. Madaras. Mr. Madaras testified that he experienced many problems with his computer after the accused's shift completed. Mr. Madaras testified that he lost about two hours of work each time he experienced problems with his computer. *See id.*

2. Specification 6 of Charge II

The United States presented evidence that "at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 8 January 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: the Combined Information Network Exchange Afghanistan database containing more than 90,000 records." *See* AE CDX. SA Shaver testified that the accused stole, purloined, or knowingly converted more than 90,000 records from the CIDNE-Afghanistan database on a SD card. *See* Testimony of SA Shaver. SA Shaver testified that these records were stored in a folder entitled "yada.tar.bz2.nc" with the filename "afg_events.csv." *See* Testimony of SA Shaver. The filename "afg_events.csv" was last written on 8 January 2010. *See id.* This SD card contained a picture of the accused, in addition to more than 90,000 records from the CIDNE-Afghanistan database. *See* PE 40; PE 113. The SD card was admitted into evidence. *See* PE 92.

The United States presented evidence that "the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records." *See* AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

The United States presented evidence that "the records were of a value greater than \$1,000." *See* AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II. Mr. Lewis also testified that the value of these records is greater than \$1,000. *See* Testimony of Mr. Lewis.

The United States presented evidence that "under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature

to bring discredit upon the armed forces.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

3. Specification 8 of Charge II

The United States presented evidence that “at or near Contingency Operating Station Hammer, Iraq, on or about 8 March 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else’s use, to wit: a United States Southern Command database containing more than 700 records.” See AE CDX. SA Shaver testified that PE 83 consists of a summary of Intelink logs showing that the accused, on 8 March 2010, used Wget to retrieve more than 700 records from the United States Southern Command database accessible through the Joint Task Force–Guantanamo (JTF-GTMO) Detainee Assessment Branch website on Intellipedia. See Testimony of SA Shaver; PE 82; PE 83. SA Shaver explained that the number “200” in PE 83 means that the accused successfully executed Wget to retrieve the “DocumentID” of records relating to JTF-GTMO detainees. Mr. Jeffrey Motes confirmed that the records in the United States Southern Command database were stored by “DocumentID” and that the above database consisted of over 700 records. See PE 131.

The accused further admitted to his misconduct to Mr. Lamo. See PE 30. When asked “(04:34:14 PM) info@adrianlamo.com: what do you consider the highlights?[,]” the accused admitted “(04:35:31 PM) bradass87: The Gharani airstrike videos and full report, Iraq war event log, the “Gitmo Papers”, and State Department cable database[.]” See *id.* at 46.

The United States presented evidence that “the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

The United States presented evidence that “the records were of a value greater than \$1,000.” See AE CDX. The stipulation of Mr. Motes explained, in detail, the steps necessary to prepare the records from the United States Southern Command database. See PE 131. Mr. Motes confirmed that it took, on average, 80-90 working hours to create each of the 700 records the accused stole and that the most detainee assessments created in one year was approximately 520. See *id.* Mr. Motes also confirmed that the lowest ranking Servicemember responsible for creating these records was E-4 and the lowest ranking government employee responsible for creating these records was GS-12. The Court took judicial notice of the salaries for persons of these ranks. See AE DLXXXVIII. Mr. Lewis also testified that the value of these records is greater than \$1,000. See Testimony of Mr. Lewis.

The United States presented evidence that “under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

4. Specification 12 of Charge II

The United States presented evidence that “at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else’s use, to wit: the Department of State NCD database containing more than 250,000 records.” See AE CDX. The Department of State firewall server logs show an incredible amount of activity between the accused’s classified government computer and the NCD database. See PE 159. SA Shaver testified that he recovered a folder from the accused’s computer with Department of State cables. See Testimony of SA Shaver; See PE 12. SA Shaver explained how the accused converted the cables into Comma Separated Value (CSV) format with Base64 encryption. See Testimony of SA Shaver. The excel spreadsheet retrieved from the accused’s computer shows that the accused was cataloguing the theft of 251,287 Department of State diplomatic cables and was admitted into evidence. See PE 102. SA Bettencourt retrieved 251,287 purported Department of State diplomatic cables from WikiLeaks. See PE 76. The accused admitted this misconduct in chats with Mr. Lamo, stating: “(02:16:48 AM) info@adrianlamo.com: embassy cables? (02:16:54 AM) bradass87: yes (02:17:00 AM) bradass87: 260,000 in all[.]” See PE 30, at 34.

The United States presented evidence that “the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records.” See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II. Additionally, Mr. Charley Wisecarver testified that each diplomatic cable in the NCD database displayed a warning banner. See Testimony of Mr. Wisecarver. See PE 169(c); PE 170(c); PE 171(c); PE 172(c); PE 173(c); PE 175(c); PE 176(c); PE 177(c). Further, and in addition to those statements listed in Specification 4 of Charge II, the accused made many additional admissions to Mr. Lamo establish a reasonable inference that the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records. These admissions, in chronological order, are set forth below:

- i. “(12:52:33 PM) bradass87: Hilary Clinton, and several thousand diplomats around the world are going to have a heart attack when they wake up one morning, and finds an entire repository of classified foreign policy is available, in searchable format to the public... =L”
- ii. “(01:52:30 PM) bradass87: funny thing is... we transffered so much data on unmarked CDs...
(01:52:42 PM) bradass87: everyone did... videos... movies... music
(01:53:05 PM) bradass87: all out in the open
(01:53:53 PM) bradass87: bringing CDs too and from the networks was/is a common phenomeon
(01:54:14 PM) info@adrianlamo.com: is that how you got the cables out?
(01:54:28 PM) bradass87: perhaps
(01:54:42 PM) bradass87: i would come in with music on a CD-RW
(01:55:21 PM) bradass87: labelled with something like “Lady Gaga”... erase the music... then write a compressed split file
(01:55:46 PM) bradass87: no-one suspected a thing

(01:55:48 PM) bradass87: =L kind of sad
(01:56:04 PM) info@adrianlamo.com: and odds are, they never will
(01:56:07 PM) bradass87: i didnt even have to hide anything
(02:00:12 PM) bradass87: everyone just sat at their workstations... watching music videos / car chases / buildings exploding... and writing more stuff to CD/DVD... the culture fed opportunities"

- iii. "(04:34:14 PM) info@adrianlamo.com: what do you consider the highlights?
(04:35:31 PM) bradass87: The Gharani airstrike videos and full report Iraq war event log the "Gitmo Papers" and State Department cable database"

PE 30 (ellipses in original) (emphasis added).

The United States presented evidence that "the records were of a value greater than \$1,000." See AE CDX. Mr. Wisecarver testified that the technicians responsible for maintaining the NCD database earned approximately \$70,000 annually and that the yearly maintenance of the database "well" exceeded \$1,000. See Testimony of Mr. Wisecarver. Mr. Lewis also testified that the value of these records is greater than \$1,000. See Testimony of Mr. Lewis.

The United States presented evidence that "under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces." See AE CDX. Evidence supporting this element is listed above in Specification 4 of Charge II.

5. Specification 16 of Charge II

The United States presented evidence that "at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010; the accused did steal, purloin, or knowingly convert records to his own use or someone else's use, to wit: the United States Forces- Iraq Microsoft Outlook/SharePoint Exchange Server global address list." See AE CDX. On 7 May 2010, WikiLeaks requested via Twitter email addresses for military personnel. See PE 31. SA Alfred Williamson confirmed that the accused, on 11 May 2010, searched Google for "global address list Microsoft excel macro." See PE 143. The accused conducted this search on the unclassified government computer in the supply office at Forward Operating Base (FOB) Hammer, Iraq. See *id.* SA Williamson found the accused's profile on this government computer, and SSG Peter Bigelow, the other user of this computer, confirmed that he "did not know what the Global Address List was." See PE 142. SA Williamson found the text file entitled "blah.txt" on this computer which contained 74,000 exchange-formatted email addresses and names of unit, ranks, and sections of personnel. See PE 143.

The United States presented evidence that "the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records." See AE CDX. SA Williamson confirmed that "on login to the computer by a user, the computer was set to display a Department of Defense warning banner and legal notice." PE 143. Further, Mr. Moul testified that the accused received Operational Security (OPSEC) training at AIT, which instructed the accused not to disclose this type of information to unauthorized persons. See

Testimony of Mr. Moul. The tasker created by the accused to “exfiltrate” the global address list further supports that the accused acted knowingly and willfully and with the intent to deprive the government of the use and benefit of the records. *See* Testimony of Mr. Johnson; PE 122. Digital remnants of the USF-I GAL were located on the accused’s personal computer. *Id.*

The United States presented evidence that “the records were of a value greater than \$1,000.” *See* AE CDX. Mr. Lewis also testified that the value of these records is greater than \$1,000. *See* Testimony of Mr. Lewis. CW4 Nixon testified that the software and hardware pieces required to operate the USF-I GAL cost between tens of thousands and over a million dollars. *See* Testimony of CW4 Nixon. CW4 Nixon also testified that the USF-I GAL could not operate without the software and hardware. *See id.*

The United States presented evidence that “under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.” *See* AE CDX. Evidence supporting this element came from the testimony of COL Miller, as set forth above in Specification 4 of Charge II. The Defense does not allege that the United States has failed to provide evidence that the accused’s conduct is prejudicial to good order and discipline. *See* Defense GAL Motion ¶ 21. The analysis for a finding of prejudice to good order and discipline is conducted separately from the analysis of whether conduct is service discrediting. *See, e.g., United States v. Davis*, 26 M.J. 445, 448 (C.M.A. 1988). Evidence of both prejudice to good order and discipline and discredit to the service has been admitted. *See* Part I.B.1, *supra*.

Therefore, based on the above evidence and all reasonable inferences drawn therefrom, the United States satisfied the requirements of RCM 917(d).

C. Relevance Objection Forfeited Where Not Timely Made

In order to preserve an objection when “the ruling is one admitting evidence” the objecting party must make a “timely objection or a motion to strike” and must state the specific ground of the objection. MRE 103(a)(1); *United States v. Reynoso*, 66 M.J. 208, 210 (C.A.A.F. 2008). Application of 103 and its requirement for a timely objection should be applied practically, not formulaically. *See Reynoso*, 66 M.J. at 210.

In the instant case, the Defense did not object to the evidence detailed in Part I.B as irrelevant. To the extent the Defense believed the admitted evidence regarding the stolen databases did not relate to the § 641 specifications, the Defense should have raised an objection to the evidence’s relevance. The Defense declined to object. Having thus conceded the evidence’s relevance, the Defense cannot claim that “the Government has failed to adduce evidence that [the accused] stole or converted the databases in question.” The Defense Motions’ arguments are not a timely objection because the Defense remained silent about the relevance of the evidence detailed in Part I.B upon its introduction into evidence. *Ford ex rel. Estate of Ford v. Garcia*, 289 F.3d 1283, 1296 (11th Cir. 2002) (“Where a party has the opportunity to object, but remains silent or fails to state the grounds for objection, objections . . . will be waived . . .”) (quotations and citations omitted); *United States v. Wong*, 40 F.3d 1347, 1378-79 (2d Cir. 1994) (holding objection waived where not raised during a sidebar conference despite ample

opportunity); *see also* *United States v. White*, 25 M.J. 50, 52 (C.M.A. 1987) (deciding the defense forfeited any objection to assailant's identity where defense elicited the identity of the assailant on cross-examination). Therefore, the Defense forfeited any objection about the relationship of the evidence to the *res* of the § 641 specifications.

II. VARIANCE

The Defense also avers that the admitted evidence constitutes a fatal variance because "information" was not specifically charged. *See* Defense 641 Motion ¶ 9 ("If the Government in this case intended to charge theft of the *information* itself or theft of a *copy* of a record, instead of theft of the database, such a charge must appear in the Charge Sheet.") (emphasis in original). The Defense claim lacks merit because no variance exists. The United States charged that the accused compromised databases, to include the records contained in the databases. *See* Charge Sheet. The United States admitted evidence to provide a reasonable inference the records were stolen and converted. Furthermore, the accused himself referred to the records he asported as "databases" in his chats.

"A variance between pleadings and proof exists when evidence at trial establishes the commission of a criminal offense by the accused, but the proof does not conform strictly with the offense alleged in the charge." *United States v. Allen*, 50 M.J. 84, 86 (C.A.A.F. 1999) (citing *United States v. Lee*, 1 M.J. 15, 16 (C.M.A. 1975)). To prevail on its claim of a fatal variance, the Defense must demonstrate that the variance is material and substantially prejudicial. *United States v. Finch*, 64 M.J. 118, 121 (C.A.A.F. 2006). A variance is material where it "substantially changes the nature of the offense, increases the seriousness of the offense, or increases the punishment of the offense." *United States v. Marshall*, 67 M.J. 418, 420 (C.A.A.F. 2009) (citing *Finch*, *supra*). A variance is prejudicial where it puts the accused at risk of another prosecution for the same conduct, misleads to the extent that the accused is unable to prepare adequately for trial, or denies the accused the opportunity to defend against the charge. *Id.* (citing *United States v. Tefteau*, 58 M.J. 62, 66 (C.A.A.F. 2003)).

A. US Charged Databases and Records, and those charges include the info in the records

1. Plain meaning of charged terms "database" and "records" includes information

For all § 641 specifications, the accused has been charged with stealing, purloining, or converting a database, to include its records, or the USF-I GAL.¹ The Charge Sheet specifies that the CIDNE-Iraq database contained more than 380,000 records, the CIDNE-Afghanistan database contained more than 90,000 records, the USSOUTHCOM database contained more than 700 records, and the NCD database contained more than 250,000 records. The Defense opines that the United States did not charge the accused with stealing or converting information.

¹ In this motion, the United States uses the term "steal" and its variations as synonymous with "stealing" and "purloining." The element of stealth required for "purloining" is not necessary under the specifications at issue because the accused has been charged with stealing, purloining, or converting certain databases and information. *See* Charge Sheet. However, the United States has offered evidence of the stealthiness employed by the accused in compromising the databases. *See* PE 30.

Defense 641 Motion at ¶ 5-6 (stating that a database is “not any way synonymous with the information or records contained therein” and that the United States could have charged the accused with stealing “information”).² By the plain meanings of the § 641 specifications, the records include the information contained therein. A database is “a compilation of information arranged in a systematic way and offering a means of finding specific elements it contains, often today by electronic means.” Black’s Law Dictionary (9th ed. 2009). Similarly, a record is “information that is inscribed on a tangible medium or that, having been stored in an electronic or other medium, is retrievable in perceivable form.” Black’s Law Dictionary (9th ed. 2009). The Charge Sheet informed the accused of the stolen *res* because the Charge Sheet described stolen records, which, by definition, includes the information in those records. *See* Part III, *infra*; *see, e.g.*, Testimony of Mr. Lewis, Testimony of CW4 Nixon; Testimony of CW4 Rouillard.

The Defense’s reliance on its filing cabinet analogy is misplaced. The United States charged the accused with stealing or converting the databases, which consisted of a collection of records. The databases were contained in servers. In the instant case, the servers are more appropriately comparable to a filing cabinet. While the servers are relevant to valuation as instruments that support the use of the databases, the servers are not the charged databases.

2. The accused agrees that “database” and “records” includes information

Moreover, the accused repeatedly referred to the records he compromised as “databases.” *See* PE 30. The accused also describes the information contained in these databases, writing, “(12:21:24 PM) bradass87: [S]ay . . . a database of half a million events during the Iraq war . . . from 2004 to 2009 . . . with reports, date time groups, lat-lon locations, casualty figures . . . ? or 260,000 state department cables from embassies and consulates all over the world, explaining how the first world exploits the third, in detail, from an internal perspective?” *Id.* at 8 (ellipses in original); *see also id.* at 9 (describing the 9/11 pager messages as a database). The accused further connected a database to the information it contains, noting, “(7:44:01 AM) bradass87: [B]ut once a single piece of information is found . . . then the database can be sifted and sifted and sifted some more, for refinement, so other intelligence functions can get in the act.” *Id.* at 17 (ellipsis in original).

3. Information as part of records comports with precedent

Charging records and the information contained therein comports with applicable precedent in criminal law. The contents and information contained in government records determines the criminality of the theft of the records more than the form of the records. *See United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966), *cert. denied*, 385 U.S. 974 (1966) (“When the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owners should be deemed immaterial.”); *United States v. Lambert*, 446 F.Supp. 890, 894 (D.C. Conn. 1978). Under § 641, the transmission of the information contained in documents is just as larcenous as theft of the documents themselves. *United States*

² Specific records, to include birth records and marriage records, are also defined to include information. Black’s Law Dictionary (9th ed. 2009).

v. *Rosner*, 352 F.Supp. 915, 922 (D.C.N.Y. 1972) (noting that the importance of information in documents described in *Bottone* applies to § 641 charges).

B. United States Presented Evidence of Theft and Conversion

The accused both stole and converted the information he compromised. Relying on dicta, the Defense argues that the United States must prove conversion and demonstrate a serious and substantial interference with its rights in the databases. Defense 641 Motion ¶ 11. The Defense's theory ignores the statutory terms of § 641 and the Charge Sheet's use of the statutory theories of stealing or conversion. See *United States v. Morissette*, 342 U.S. 246, 271 (1952) ("What has concerned codifiers of the larceny-type offense is that gaps or crevices have separated particular crimes of this general class and guilty men have escaped through the breaches. . . . The codifiers wanted to reach all such instances."). The Defense further argues that *Marshall* sets forth a precedent for a fatal variance. See Defense 641 Motion ¶¶ 27-30. In *Marshall*, the identity of the accused's custodian as charged was not proven. See *Marshall*, 67 M.J. at 420-21. Accordingly, the substitution of a different custodian changed the identity of the offense. *Id.* In this case, however, the identity of the records remains the same because the evidence relates to the charged databases and records. Thus, *Marshall* is not pertinent.³

Here, to "steal" means to wrongfully take money or property belonging to the United States Government with the intent to deprive the owner of the use and benefit temporarily or permanently. AE CDX. A conversion may include the misuse or abuse of United States property and may reach use in an unauthorized manner or to an unauthorized extent of property. *Id.* The misuse must seriously and substantially interfere with the United States Government's property rights. *Id.*

1. Accused's acts constitute theft of United States Government Records

Theft of records occurs where copies of the records are transmitted to an unauthorized party even though the records remain in the custody and control of the United States. *United States v. DiGilio*, 538 F.2d 972, 977 (2d Cir. 1976). A copy of a record does not alter its character as a record under the ambit of § 641. *Id.* ("A duplicate copy is a record for purposes of the statute, and duplicate copies belonging to the government were stolen.") (citations omitted). Furthermore, the accused remains criminally liable under § 641 even where the United States retains possession of the original records. See *id.* (rejecting the accused's argument that § 641 does not apply where the United States, at most, loses exclusive possession of information contained in confidential records); see also *Flores-Figueroa v. United States*, 556 U.S. 646, 647 (2009) (upholding criminal liability for knowing transfer, possession, or use, without lawful authority, a means of identifying another person). Indeed, § 641 makes criminal the asportation of records owned by the United States. *DiGilio*, 538 F.2d at 977.

In his chat logs, the accused admitted to asporting the data from a United States Government computer system onto his personal computer and compromising the data by conveying it to Mr. Julian Assange. The accused stated, "[L]et's just say *someone* I know

³ Changing the identity of the custodian prevents the accused from confronting the custodian. Here, the accused has been able to confront the custodians of the charged databases and records.

intimately well, has been penetrating US classified networks, mining data like the ones described . . . and has been transferring that data from the classified network over the "air gap" onto a commercial network computer . . . sorting the data, compressing it, encrypting it, and uploading it to a crazy white haired aussie who can't seem to stay in one country very long =L." PE 30 at 8 (ellipses in original). The accused admitted to compromising CIDNE-Iraq, CIDNE-Afganistan, and NCD. *Id.* at 8. The accused also admitted to compromising the USSOUTHCOM database, stating that Mr. Assange has "the 'Gitmo Papers.'" *Id.* at 46. The accused's admission provides a reasonable inference of his intent to deprive the United States Government permanently of the records and information contained therein.

Additionally, these statements corroborate the accused's intent to steal the USF-I GAL. The accused removed the USF-I from a United States Government computer system. CW4 Nixon testified that the only United States Government personnel had access to the USF-I GAL on NIPR system. The accused extracted the USF-I GAL from the United States Government system to his personal computer. This act constituted stealing. Moreover, the accused removed the USF-I GAL from the possession of the United States Government and placed it in his private possession after WikiLeaks posted a tweet specifically requesting military email addresses. *See* PE 31. The accused had the ability to view the USF-I GAL but did not possess the capability to export the USF-I GAL. *See* Testimony of CW4 Nixon. The accused searched for a macro, which is a computer program, that removed the USF-I GAL from a United States Government system. *See* PE 143. The accused also created a tasker to "exfiltrate" the USF-I GAL. *See* Testimony of Mr. Johnson; PE 122. Thus, the theft was complete the moment the accused took the USF-I GAL from the possession of the United States Government into his personal possession with the intent to deprive the United States of the stolen property. *See* AE CDX.

After-the-fact deletion of the record does not render innocent an already completed criminal act. The Defense's proffered argument regarding contradictory evidence is not appropriate under RCM 917. *See* 917(a) (stating that Defense may offer evidence if its request for a finding of not guilty is denied). Similarly, any evidence of transmission would only enhance the criminality of the already completed theft, but the lack of enhancement also does not render innocent a completed criminal act.

2. Accused's acts constitute conversion of United States Government records

The existence of a property in the contents of confidential information has long been judicially recognized. *See Carpenter v. United States*, 484 U.S. 19, 25 (1987) (recognizing as worthy of protection a property right in confidential business information); *United States v. Girard*, 601 F.2d 69, 71 (2d Cir. 1979) (recognizing a property right in unpublished writings) (citations omitted). The United States Government is responsible for the accountability and dissemination of classified information and has set up certain procedures and precautions to protect classified documents and the information contained therein. *United States v. Zettl*, 889 F.2d 51, 53. The United States Government has created the systems for protecting classified information to protect its rights to confidentiality and exclusivity in the information it elects to classify. *See id.* (holding that authority to determine whether a document should be transferred is a function of the United States Government, not the holder of the document). Accordingly, the United States has a property interest in its classified records which it may protect by statute as a

thing of value under § 641. See *Girard*, 601 F.2d at 71. (citing *United States v. Friedman*, 445 F.2d 1076, 1087 (9th Cir. 1971)). Conversion of computerized records as a “misuse or abuse of property its use in an unauthorized manner” occurs where an accused transfers information to an unauthorized party. See *id.* (holding that sale of information contained in computerized Drug Enforcement Agency records could be found to violate § 641 as a conversion of the computerized records) (citation and quotation marks omitted).

Conveyance of United States Government records to an unauthorized party constitutes conversion under § 641. See *DiGilio*, 538 F.2d at 976. In *DiGilio*, the defendants created unauthorized copies documents related to an investigation of alleged criminal activity and delivered the copies to unauthorized persons. *DiGilio*, 538 F.2d at 976. Based on these acts, the defendants were charged with converting to their own use “records of the United States; that is, photocopies of official files of the Federal Bureau of Investigation . . .” *DiGilio*, 538 F.2d at 976. Here, the accused converted the United States Government records by conveying them to WikiLeaks. WikiLeaks lacked the authority to possess this information. See Testimony of SA Mander; Testimony of Ms. Glenn; Testimony of Mr. Hosburgh. Defense’s reliance on *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995), is inapposite because *Collins* involved an infringement on computer systems within the possession on the United States Government and not the United States Government’s proprietary interest in its United States Government information. In the instant case, the accused stole and converted United States Government records by transferring them to an unauthorized party or onto his personal computer. Additionally, this conveyance harmed the United State’s interest in exclusive possession of the information in the records, thereby further adding to the conversion caused by the accused.

Furthermore, disclosure of United States Government proprietary information creates criminal liability for converting that information. See *Carpenter*, 484 U.S. at 26-27; *United States v. Fowler*, 932 F.2d 306, 309-10 (4th Cir. 1991). Specifically, misappropriating information confidentially held by one party by giving it to an unauthorized party constituted interference with the right to exclusive use of the compromised information. See *id.* In *Carpenter*, the author of an investment column entered into an agreement to give his co-conspirators advance information as to the content and timing of the article. *Id.* at 23. The contents of the articles were not affected and the owner of the information did not suffer a monetary loss. *Id.* at 23, 26. Nevertheless, the defendants’ conviction for wire and mail fraud under 18 U.S.C. § 1341 and 18 U.S.C. § 1343, each of which carried a potential sentence of up to five years, was upheld. See *id.* at 22 nn. 3-4. Deprivation of the right to exclusive use of the information established a sufficient basis for criminal liability because exclusivity was an important aspect of the confidential information. Accord *DiGilio*, 538 F.3d at 978 (finding merit to the Government’s argument that a misappropriation of information under § 641 but declining to so hold where a technical larceny was proven).

Here, the accused compromised classified, other United States Government information, or PII. This information had value because it was closely held. See Testimony of Mr. Lewis. The United States Government classifies information, *inter alia*, to protect it from adversaries. See *id.* Adversaries seek United States Government information to attack the United States. See PE 183. Thus, the accused substantially interfered with United States Government information by compromising it to WikiLeaks.

B. Copies Do Not Constitute a Material or Prejudicial Variance

The Defense asserts a fatal variance on two bases. First, the Defense states that the distinction between “information,” “database,” and “copy” affects valuation and any preparation for the valuation element of the § 641 specification. Defense 641 Motion ¶ 26. As discussed in Part III, *infra*, this Defense argument ignores established precedent for determining valuation. Second, the Defense maintains that the distinction between stealing a “database,” “information,” or “copies of records” alters the substance of the § 641 specification and harms the accused’s ability to present a defense to the § 641 specifications. Defense 641 Motion ¶ 30.

The accused stole and converted records maintained on United States Government computer systems. The Defense argues that a fatal variance exists because the Charge Sheet specifies records and not copies of records. *See* Defense 641 Motion ¶ 4. The records compromised by the accused are the records maintained by the United States. The United States maintained copies of the records because they were digitally stored on United States Government computer systems. In this case, any distinction between copies of the records is feckless because the records were stored digitally. *See DiGilio*, 538 F.2d at 978 (referring to theft of copies as “an asportation of records owned by the United States”) (emphasis added). This distinction cannot be a material variance because it does not change the nature of the offense, let alone substantially change the nature of the offense, increase the seriousness of the offense, or the punishment of the offense. Thus, any variance is not material.

Moreover, any variance between a digital record and a digital copy of the same record is not prejudicial. The distinction does not place the accused at risk of another prosecution because the accused is charged with stealing and converting the actual records, which he in fact stole and converted. Nor did the distinction affect the accused’s ability to prepare his defense because the United States charged the accused with stealing and converting the records using a term, “database,” the accused himself used to describe the records he compromised.

C. No Variance Regarding USF-I GAL

The United States admitted evidence that the accused stole the USF-I GAL, and the Defense allegation that the property stolen by the accused was not, in fact, the USF-I GAL lacks merit. CW4 Nixon testified that the USF-I GAL had approximately 160,000 users. *See* Testimony of CW4 Nixon. CW4 Nixon testified that the USF-I GAL contained, *inter alia*, names and email addresses connected to the “iraq.centcom.mil” domain. *Id.* CW4 Nixon further testified that he identified names in PE 47 he personally knew existed in the USF-I GAL and that the “iraq.centcom.mil” domain was associated with the names, to include GEN Odierno and then-LTG Austin in PE 47. *Id.* CW4 Nixon testified that the USF-I GAL was distributed by organization, to include by division at the division level. *See id.* CW4 Nixon testified that the domain control of USF-I GAL at the division level established distributional control of the USF-I GAL. *See id.* CW4 Nixon testified that the USF-I GAL was also distributed at the Corps and brigade levels. *See id.* CW4 Nixon testified that PE 47 and PE 48 constituted a USF-I GAL pool for a USF-I server. *Id.* CW4 Nixon identified the contents of PE 47 and PE 48 as reflecting the contents of the USF-I GAL. CW4 Nixon also testified that PE 147 and PE 148 were representative of the contents of PE 47 and PE 48, respectively.

CW4 Nixon testified that a user would not have the ability to download the USF-I GAL or its subordinate portions without a special program or access privileges. *See id.* CW4 Nixon testified that downloading the USF-I GAL as a whole or in part was not a function. CW4 Nixon distinguished between a user being able to view the entire USF-I GAL and accessing the USF-I GAL; accessing the USF-I GAL entailed the ability to remove the USF-I GAL from the United States Government systems. CW4 Nixon testified that a user could cut and paste the information from the USF-I GAL but that such a process would not be effective. *See id.* CW4 Nixon also testified that removing the contents of the USF-I GAL would not be easy without outside software or programming. *See id.* SA Williamson testified that he found the contents of a Microsoft GAL on the accused's computer. *See* PE 143. SA Williamson also testified that the accused searched for a macro to export a GAL. *See* PE 143. Also, the accused created a tasker to "exfiltrate" the USF-I GAL. *See* Testimony of Mr. Johnson; PE 122.

Assuming, *arguendo*, that the United States has not adduced evidence that the accused stole the entire USF-I GAL but only a large portion of it, no fatal variance exists for Specification 16 of Charge II. Any such variance is minor because it does not change the nature of the offense. *See United States v. Lovett*, 59 M.J. 230, 235-36 (C.A.A.F. 2004) (citations omitted). At a minimum, the evidence establishes that the accused stole the USF-I GAL as distributed at the division level. *See* Testimony of CW4 Nixon.

The Defense was fully aware of the United States Government property at issue. Furthermore, the admitted evidence constitutes at least part of the USF-I GAL as charged in Specification 16 of Charge II. Evidence that a portion of the charged property was stolen does not constitute a fatal variance. *See United States v. Kubel*, 5 C.M.R. 73, 75-76 (C.M.A. 1952) (upholding substitutions and exceptions that reduced the number and value of stolen items); *United States v. Lee*, 1 M.J. 15, 16-17 (C.M.A. 1975) (holding defense counsel was not misled where the Government submitted evidence that marijuana plants were part of the quantities covered in the specification); *England v. United States*, 174 F.2d 466, 468 (5th Cir. 1949) (holding no fatal variance between "check" and "an incomplected draft on the Treasurer of the United States"); *see also United States v. Thomas*, 65 M.J. 132, 135-36 (amending specification to change a specifically charged quantity to "some quantity"). The Defense contends that *United States v. Wilkins*, 45 C.M.R. 638 (A.C.M.R. 1972), demonstrates that the alleged variance is fatal. However, *Wilkins* held that a variance is fatal where it completely changes the stolen *res* from an amount of currency to a wallet. *See Wilkins*, 45 C.M.R. at 639-40. Here, the accused is charged with stealing the USF-I GAL and its contents, and the evidence demonstrates, at a minimum, that a large portion of the contents of the USF-I GAL were stolen. Thus, any variance regarding the amount of the USF-I GAL that was stolen is not fatal.

III. VALUATION IS PROVEN BY INFORMATION

A. Information Is Intrinsic to Compromised Records

Defense claims about prejudice stemming from valuation disregard the methods of proving valuation. Under § 641, valuation may be demonstrated by face value, par value, market value, or cost price. § 641. § 641 protects "a thing of value." *Id.* A thing of value includes

tangible and intangible items. *See Fowler*, 932 F.2d 306, 309-310 (4th Cir. 1991) (determining that records and the information contained in the records qualify as a thing of value under § 641) (citing *Carpenter*, 484 U.S. at 25; *Morison*, 844 F.2d at 1076-77). Information is an intangible thing of value protected by § 641. *See id.*; cf. *United States v. Schwartz*, 785 F.2d 673 (9th Cir. 1986) (interpreting “thing of value” under § 641 to “include . . . intangibles, such as providing assistance in arranging the merger”); *United States v. Croft*, 750 F.2d 1354, 1362 (7th Cir. 1984) (holding that § 641 applies to research services as a thing of value); *Burnette v. United States*, 222 F.2d 426 (6th Cir. 1955) (holding services and labor performed by government employees are punishable under § 641). Indeed, proprietary information in United States Government records is a thing of value under § 641. *See Fowler*, 932 F.2d at 310 (noting that information is a species of property and a thing of value); *United States v. Jeter*, 775 F.2d 670, 680-82 (6th Cir. 1985); *Girard*, 601 F.2d at 70-71.

Valuation for a § 641 specification may be demonstrated, *inter alia*, by the item’s market value, thieves’ market value, or cost of production. Market value is “approximately what it would cost to purchase the same or similar property in the marketplace.” *United States v. 50 Acres of Land*, 469 U.S. 24 (1984); *see Muser v. Magone*, 155 U.S. 240 (1894) (defining market value as the “price at which the owner of the goods, or the producer, holds them for sale; the price at which they are freely offered in the market to all the world; such prices as dealers in the goods are willing to receive, and purchasers are made to pay, when the goods are bought and sold in the ordinary course of trade”). The thieves’ market value is the price at which the good may be sold on the illegal black market. *See, e.g., United States v. Hood*, 12 M.J. 890, 891-92 (A.C.M.R. 1982); *see also United States v. Ligon*, 440 F.3d 1182 (9th Cir. 2006) (defining the market value approach to include the thieves’ market). The cost of production is the price the producer incurred to create or produce the good. *See, e.g., United States v. Walter*, 43 M.J. 879, 885 (N-M. Ct. Crim. App. 1996). The cost of production has been applied to calculate the value of deleted database files for which “no readily ascertainable market value” existed. *Id.*

Additionally, the cost of production includes costs producing and supporting the use of the records. *See Zettl*, 889 F.2d at 54 (noting that cost price includes the cost of photocopying, transportation, and other actual costs of the documents); *Walter*, 43 M.J. at 884-85 (deciding that the personnel or labor costs of producing and reproducing the files was reasonable). The Defense relies on *Zettl* to argue that the scope of valuation should be narrowed. *See* Defense 641 Motion ¶ 44. However, the accused is charged with stealing or converting databases, to include the records contained therein, and not documents as charged in *Zettl*. *See* Charge Sheet; *Zettl*, *supra*. Given the infrastructure necessary to support the databases and the records contained therein, the costs of producing and maintaining the databases are relevant under § 641. *See, e.g.,* PE 115; PE 116; PE 131; Testimony of CW4 Nixon; Testimony of Mr. Wisecarver.

The basis of establishing a market value, to include the thieves market, requires an analysis of the characteristics of the actual goods. *See, e.g., Hood*, 12 M.J. at 891-92 (comparing values of stolen goods to values received on black market of similar goods). The market value is determined by the value the participants place on the record, to include its information. *See Ligon*, 440 F.3d at 1184 (“[P]roperty value is determined by market forces This gives § 641 its obvious, and certainly its practical, meaning, namely the amount the goods may bring to the thief.”).

The contents of the record dictate its value. *See* Testimony of Mr. Lewis. No open market for United States Government information exists. *See id.* Further, bulk amounts of information have increased value in comparison to smaller collections of records. *See id.* Where valuation can be proven by the value of the goods in a market, evidence that the records are valuable to adversaries based on their contents does not prejudice the accused. *See United States v. May*, 625 F.2d, 186, 191-92 (6th Cir. 1980) (deciding that a determination of a thing of value can rely on the readily ascertainable and quantifiably components of the stolen or converted thing of value). Similarly, evidence of the cost of production for the databases and records contained therein cannot be separated from the information because the information requires protection. *See, e.g.,* Testimony of Mr. Lewis; *May, supra*. The Defense attacks Mr. Lewis's credibility, but the Defense Motions are not the appropriate forum for argument regarding witness credibility. *See* RCM 917(d). Thus, evidence of value of the records, to include their information, poses no prejudice to the accused.

B. Defense Has Had Ample Notice of Valuation Based on Information

The appellate record demonstrates that the Defense has been on notice that the United States intended to elicit testimony from Mr. Lewis on the value of government information since well before the start of this trial, and specifically that the United States intended to offer him as an expert in this field. Below are excerpts from both the United States and Defense filings that outline this notice:

On 26 October 2012, the United States stated in its witness list #2 with explanations, "[Mr. Lewis] will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CCCLXVII at 8.

On 12 December 2012, the United States stated in its witness list #3 with explanations, "[Mr. Lewis] will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDXXXVI; AE CDXXXVII at 8.

On 31 January 2013, the United States stated in its witness list #4 with explanations, "[Mr. Lewis] will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDLXXV; AE CDLXXVI at 7.

On 31 January 2013, the United States stated in its Grunden response that Mr. Lewis "will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDLXXIX; AE DLXXX at 18.

On 1 February 2013, the United States stated in its Grunden response corrected copy that Mr. Lewis "will testify about counterintelligence and the value of information, including classified information concerning the value of government information." AE CDLXXIX; AE DLXXX at 18.

On 22 February 2013, the Defense stated in its MRE 505(h) notice that Mr. Lewis "is a counterintelligence specialist with DIA and has worked in the field generally for many years." AE CDXC at 14. The Defense explains that the United States provided the following as an explanation of his testimony- "He will testify about counterintelligence and the value of information, including classified information concerning the value of government information." *Id.* The defense further states:

The matters covered by the defense in cross examination will fall within the general outlines provided by the Government above. The defense reasonably expects to discuss the experience of Mr. Lewis on other cases. That experience gives Mr. Lewis the expertise to opine as to the value of government information.

Id.

On 24 April 2013, the Defense stated in its Grunden filing that Mr. Lewis will testify about the "value of CIDNE [d]atabases, charged SOUTHCOM information, and the USF-I GAL." AE CXXV at 16. In the same filing, they also stated Mr. Lewis will "testify about how the value of those items and how their value is determined." *Id.* Additionally, the Defense stated that he will testify about money offered for the information in the databases and "generally about how the information, even if dated, will be of some value" to foreign entities. *Id.*

On 10 May 2013, the United States filed its notice of accounting of discovery and expert witnesses, which stated next to Mr. Lewis's name that "[t]he United States may qualify this witness as an expert in counterintelligence and the value of national security information[.]" AE CXLIII at 4.

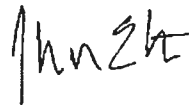
On 13 May 2013, the Defense stated in its corrected copy of its Grunden filing that Mr. Lewis will testify about the "value of CIDNE [d]atabases, charged SOUTHCOM information, and the USF-I GAL." AE CXV at 16. In the same filing, they also stated Mr. Lewis will "testify about how the value of those items and how their value is determined." *Id.* Additionally, the Defense stated that he will testify about money offered for the information in the databases and "generally about how the information, even if dated, will be of some value" to foreign entities. *Id.*

On 15 May 2013, the United States filed a corrected copy of its notice of accounting of discovery and expert witnesses, which stated next to Mr. Lewis's name, "The United States may qualify this witness as an expert in counterintelligence and the value of national security information[.]" AE CLXIII at 4.

Thus, the Defense has had ample notice about the United States' intention to rely on the information contained in the compromised records to establish valuation. Therefore, the Defense has not suffered any prejudice.

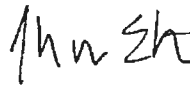
CONCLUSION

The United States submitted evidence relevant to the § 641 specifications that was admitted. The Defense argues that the United States has failed to satisfy the standard set forth in RCM 917(d). The admitted evidence establishes a reasonable inference that the accused stole and converted the databases and records listed in the § 641 specifications. The Defense arguments that the § 641 specifications constitute fatal variances lack merit because the evidence proves the contents of the databases and the records were stolen or converted. The evidence does not constitute a material variance. Additionally, the Defense had adequate notice and ability to prepare the accused's defense for trial.



ALEXANDER S. VON ELTEN
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 11 July 2013.



ALEXANDER S. VON ELTEN
CPT, JA
Assistant Trial Counsel