UNITED STATES ARMY COURT OF CRIMINAL APPEALS

Before
CAMPANELLA, CELTNIEKS, and HAGLER
Appellate Military Judges

UNITED STATES, Appellee
v.
Private First Class BRADLEY E. MANNING (nka CHELSEA E. MANNING)
United States Army, Appellant

ARMY 20130739

U.S. Army Military District of Washington
Denise R. Lind, Military Judge
Colonel Corey J. Bradley, Staff Judge Advocate (pretrial)
Colonel James R. Agar, II, Staff Judge Advocate (post-trial)

For Appellant: Vincent J. Ward, Esquire (argued); Captain J. David Hammond, JA; Lieutenant Colonel Jonathan F. Potter, JA; Vincent J. Ward, Esquire; Nancy Hollander, Esquire (on brief); Lieutenant Colonel Christopher D. Carrier, JA.

Amicus Curiae:

For Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, and the Center for Democracy and Technology: Jamie Williams, Esquire; Andrew Crocker, Esquire (on brief).

For Amnesty International Limited: John K. Keker, Esquire; Dan Jackson, Esquire; Nicholas S. Goldberg, Esquire (on brief).

For American Civil Liberties Union Foundation: Esha Bhandari, Esquire; Dror Ladin, Esquire; Ben Wizner, Esquire (on brief).

For Open Society Justice Initiative: James Goldston, Esquire; Sandra Coliver, Esquire (on brief).

For Appellee: Captain Catherine M. Parnell, JA (argued); Colonel Mark H. Sydenham, JA; Lieutenant Colonel A.G. Courie III, JA; Major Steve T. Nam, JA; Captain Timothy C. Donahue, JA; Captain Jennifer A. Donahue, JA; Captain Samuel E. Landes, JA (on brief); Captain Allison L. Rowley, JA.

31 May 2018

OPINION OF THE COURT

CAMPANELLA, Senior Judge:

A military judge sitting as a general court-martial convicted appellant, in accordance with her pleas, of one specification of violating a lawful general regulation and two specifications of general disorders in violation of Articles 92 and 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. §§ 892, 934 (2006). The military judge also convicted appellant, contrary to her pleas, of four specifications of violating a lawful general regulation, one specification of wantonly causing intelligence to be published, six specifications of violating 18 U.S.C. § 793(e), one specification of violating 18 U.S.C. § 1030(a)(1), and five specifications of violating 18 U.S.C. § 641, in violation of Articles 92 and 134, UCMJ.[1]

The convening authority approved the adjudged sentence of a dishonorable discharge, confinement for thirty-five years, forfeiture of all pay and allowances, and reduction to the grade of E-1. The military judge credited, and the convening authority approved, 1,293 days of confinement credit, 112 days of which was Article 13, UCMJ, credit.

On 17 January 2017, President Barack Obama commuted appellant's sentence of thirty-five years imprisonment to time served plus 120 days, leaving intact all other conditions and components of the sentence. Thereafter, appellant conceded two of the initial assigned errors as moot based on the President's commutation.[2]

This case is before us for review pursuant to Article 66, UCMJ. Appellant asserts eight assigned errors, five of which merit discussion, one of which merits relief. We have also considered the matters appellant personally asserted pursuant to *United States v. Grostefon*, 12 M.J. 431 (C.M.A. 1982), and conclude appellant's *Grostefon* matters do not warrant relief.

BACKGROUND

In 2007, appellant joined the Army as an all-source intelligence analyst. Appellant attended and passed the Army intelligence analyst advanced skill training, which included lessons on terrorist use of information on the internet and lessons on information security. Appellant's information security training was extensive and

[1] The court acquitted appellant of one specification of aiding the enemy in violation of Article 104, UCMJ, and one specification of transmitting defense information under 18 U.S.C. §793(e), in violation of Article 134, UCMJ.

[2] Specifically, appellant conceded the assigned errors of whether the military judge abused her discretion by admitting certain sentencing testimony and whether this court should re-adjudge the sentence based on cumulative errors alleged to have occurred throughout the case.

included instruction regarding why information is classified, restriction on access to classified information, and storage and safekeeping of classified information to ensure unauthorized persons do not gain access.

Appellant was taught how to use numerous information sources to conduct intelligence analysis and create intelligence reports. Intelligence reports produced by analysts are intended to provide situational awareness to forces during military operations. Appellant's training warned that operational information should not be discussed on the internet or in email, and to assume the enemy is always able to view and read information on the internet. Appellant obtained a security clearance that allowed her access to classified information in order to conduct her job.

During her pre-deployment train-up, appellant obtained a higher security clearance, which allowed her access to even more sensitive classified compartmentalized information. On 7 April 2008 and 17 September 2008, appellant signed two separate nondisclosure agreements, acknowledging she understood the security indoctrination concerning the nature and protection of classified information and that unauthorized disclosure could cause irreparable damage to the United States. Appellant avowed not to divulge classified information to those not authorized access and acknowledged doing so would be a criminal act.

In addition to learning about the need to protect classified information, appellant, on at least one occasion, also taught others. On 13 June 2008, appellant created a slide show entitled "Operations Security," which defined critical sensitive information and listed common security breaches. The conclusion of the presentation advised avoiding public disclosure of classified sensitive information—to include posting it on the internet.

On 11 October 2009, appellant deployed to Forward Operating Base (FOB) Hammer, Iraq, with the 10th Mountain Division. Appellant was assigned to work in the Intelligence Section of the 2nd Brigade Combat Team as an all-source intelligence analyst. As such, appellant had access to and reviewed voluminous amounts of classified and sensitive information across the intelligence spectrum. This included classified significant activity reports (SIGACTs) in both Afghanistan and Iraq, U.S. Southern Command (SOUTHCOM) detainee intelligence reports, and U.S. State Department diplomatic cables. The data to which appellant had access contained a vast amount of information related to past and present military operations, revealing such restricted information as tactics, techniques, and procedures used by allied forces both offensively and defensively, the names of suspected enemies, the names of covert cooperatives, code words, unit locations, specific military missions, and other controlled records.

Appellant's job included downloading, indexing, and plotting SIGACTs on maps based on locations and enemy threats. Appellant knew the enemy engaged in a

similar pattern of analysis regarding United States operations. By all accounts, for her rank and experience, appellant was an excellent intelligence analyst, able to skillfully synthesize large volumes of information and provide particularly helpful reports as requested by her superiors.

In order to use the secret classified computer network (SIPRNET), appellant agreed to an "acceptable use policy" (AUP) wherein she promised to: 1) use the network for only authorized purposes; 2) protect classified information; and 3) not to put unauthorized software on the computer network.

In 2009, appellant began visiting the Wikileaks website. Wikileaks was a clearinghouse for making sensitive government information public on its internet site. Wikileaks solicited its website users to obtain and reveal sensitive government information to it—and, in turn, Wikileaks would post the information on its public website, without identifying the source of the information. Wikileaks also ran online chatrooms where participants discussed political current events and computer-related topics.

Appellant conducted computer searches in government databases looking for specific information solicited by Wikileaks on its website. Appellant also conducted research about Wikileaks. She accessed a website run by the U.S. Army Counterintelligence Center (USACIC) that contained a report concerning the Wikileaks organization. The report stated Wikileaks was a threat to U.S. operational security, information security, and counterintelligence security, because of its public posting of classified and sensitive information. Additionally, the report concluded that Wikileaks' public posting of classified and sensitive information could be valuable to insurgents, terrorists, and foreign military forces collecting information against the United States and in planning attacks. In other words, the report opined Wikileaks' operations were a threat to national security.

One day while working in the secure classified information facility (SCIF), appellant downloaded thousands of classified SIGACTs from both the Combined Information Data Network Exchange for Iraq (CIDNE-I) and for Afghanistan (CINDE-A) onto a compact disc (CD). She then removed the CD from the SCIF and took it to her quarters where she copied the contents onto her personal laptop computer and copied the information onto a memory card.

In January 2010, while in Maryland on mid-tour leave from her deployment, appellant uploaded the classified information contained on the memory card to the Wikileaks website. Within this unauthorized transmission of the classified information to Wikileaks, appellant also uploaded a smiling self-photo and the following remarks:

> Items of Historical Significance for Two Wars:

> Iraq and Afghanistan Significant Activities (SIGACTs) Between 0000 on 1 JAN 2004 and 2359 on 31 DEC 2009 (Iraq local time, and Afghanistan local time)
>
> CSV [comma separated value, data format] extracts are from the Department of Defense (DoD) Combined Information and Data Exchange (CIDNE) Database.
>
> It's already been sanitized of any source identifying information.
>
> You might need to sit on this information, perhaps 90-180 days, to figure out how to best release such a large amount of data, and to protect source [sic].
>
> This is possibly one of the more significant documents of our time, removing the fog of war, and revealing the true nature of the 21st century asymmetric warfare.
>
> Have a good day.

Upon returning to Iraq from mid-tour leave, appellant, using SIPRNET, conducted a computer search of the Department of State's (DoS) Net-Centric Diplomacy (NCD) database, a site where classified State Department materials concerning sensitive diplomatic relations and activities were stored. Through appellant's online Wikileaks chats, appellant learned of Wikileaks' interest in a diplomatic controversy involving the United Kingdom, the Netherlands, and Iceland. In January 2010, appellant searched for documents related to the controversy and found a sensitive DoS cable entitled "10 Reykjavik 13" concerning the dispute. Appellant downloaded the classified cable to a CD, again took the CD to her quarters, uploaded the cable to her personal laptop, and sent it to Wikileaks. Shortly thereafter, Wikileaks posted the cable to their public website.

Appellant also downloaded an aerial video of a helicopter weapons team engaging targets during a combat engagement. The aerial video illustrated a great deal of sensitive technical and tactical facts to include the helicopter's use of lasers, the angle of engagement, and its speed and altitude. Appellant uploaded the aerial video to Wikileaks and informed the organization through the chatroom to "expect an important submission."

In early March 2010, appellant began chatting directly with Wikileaks' leader, Julian Assange. Appellant asked Assange for help in bypassing the SIPRNET security systems to allow appellant to anonymously navigate the SIPRNET system

therein. On 7 March 2010, appellant asked Assange about the value of the U.S. Southern Command detainee assessment memoranda regarding Guantanamo detainees. The memoranda contained information related to detainee identity, capture information, background, intelligence summaries, and detainee cooperation, among other things. Assange indicated the reports would be valuable. Appellant then downloaded 700 detainee assessments from the SIPRNET to a CD along with the USACIC assessment report regarding Wikileaks and sent them to Wikileaks.

On 15 March 2010, Wikileaks posted the USACIC report regarding Wikileaks on its website. On 5 April 2010, Wikileaks released the aerial video. On 25 April 2011, Wikileaks released the 700 detainee assessment reports.

Additionally, appellant transferred an unauthorized computer program called Wget to the SIPRNET computer at her workstation in late March 2010. Wget is a computer program that facilitates downloading and copying enormous amounts of information quickly, so as to avoid manually downloading each piece of data. Wget operates in the background of the computer, while the user is working separately on other tasks. Wget bypassed the ordinary method of accessing cables via the DoS portal. Appellant used Wget to download and copy batches of sensitive cables from the DoS's NCD portal to CDs. She then took the CDs to her living quarters. The forensic evidence indicated appellant downloaded approximately 250,000 cables from the portal. The larger file was corrupted and appellant was not able to upload all the information to Wikileaks. Ultimately, appellant pleaded guilty to transmitting more than seventy-five classified cables to Wikileaks. The cables included information concerning foreign government information that was protected for national security purposes.

Also, in March 2010, appellant downloaded and copied a classified report from the U.S. Central Command database regarding an administrative investigation into an airstrike. The report contained information related to: troop movements; close air support procedures; and other sensitive tactics, techniques, and procedures. Appellant once again took the CD to her quarters and uploaded the investigation to the Wikileaks website.

On 7 May 2010, Wikileaks solicited military email addresses from its users. Shortly thereafter, appellant created a tasker on her computer reminding herself to acquire the Global Address List from the Unites States Forces-Iraq Microsoft/Outlook server (USF-GAL). On or about 13 May 2010, appellant downloaded approximately 74,000 military email addresses from the unclassified computer network and transferred them to her personal computer. The forensic investigation into appellant's activities eventually uncovered the email addresses located in the unallocated space of appellant's personal computer—indicating they were deleted but not written over. No evidence was introduced at trial indicating appellant disclosed the email addresses to Wikileaks.

On 20 May 2010, using an encrypted messaging system, appellant began chatting with Adrian Lamo, a computer hacker, wherein appellant admitted she gave information to Wikileaks. Appellant used the code name "bradass87" in her exchanges with Mr. Adrian Lamo. The following messages were exchanged between the two:

> bradass87: the air gap [the separation between standalone networks and the wider internet] has been penetrated[.]
>
> 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[.]
>
> . . .
>
> 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[.]
>
> . . .
>
> bradass87: funny thing is . . .we transffered so much data on unmarked CDs . . . everyone did . . . videos . . . movies . . .music all out in the open . . . bringing CDs too and from the networks was/is a common phenomenon
>
> adrianlamo: is that how you got the cables out?
>
> bradass87: perhaps. i would come in with music on a CD-RW labelled with something like "Lady Gaga". . . erase the music . . . then write a compressed split file . . . no-one ever suspected a thing. =L kind of sad
>
> adrianlamo: and odds are, they never will
> bradass87: i didnt even have to hide anything . . . everyone just sat at their workstations . . . watching music

> videos / car chases / buildings exploding . . . and writing more stuff to CD/DVD . . . the culture fed opportunities
>
> adrianlamo: what do you consider the highlights?
>
> bradass87: The Gharani airstrike videos and full report Iraq war event log the "Gitmo papers" and the State Department cable database.
>
> . . .
>
> bradass87: waiting to redeploy to the US, be discharged . . . and figure out how on earth im going to transition … all while witnessing the world freak out as its most intimate secrets are revealed.
>
> . . .
>
> bradass87: I just . . . couldn't let these things stay inside of the system . . . and inside of my head . . .
>
> . . .
>
> bradass87: i could've sold to russia or china, and made bank?
>
> adrianlamo: why didn't you?
>
> bradass87: because it's public data
>
> adrianlamo: i mean, the cables
>
> bradass87: it belongs in the public domain . . . . information should be free . . . it belongs in the public domain
>
> . . .
>
> adrianlamo: embassy cables?
>
> bradass87: yes. 260,000 in all

(errors in original).

On 25 May 2010, Mr. Lamo reported to law enforcement that appellant admitted to him through online chats that appellant had disclosed thousands of classified documents. On or about 30 May 2010, appellant was placed in pretrial confinement at FOB Hammer, Iraq, for compromising classified information.

LAW AND DISCUSSION

A. Computer Fraud and Abuse Act

THE DEFINITION OF "EXCEEDS AUTHORIZED ACCESS" IN THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030(a)(1) (SPECIFICATION 13 OF CHARGE II)[3]

The Computer Fraud and Abuse Act (CFAA)

Appellant was convicted of one specification of Article 134, UCMJ, for violating 18 U.S.C. § 1030(a)(1) of the CFAA by using the Wget software program to access, search and download diplomatic cables maintained in a classified DoS database.[4]

Pursuant to 18 U.S.C. § 1030(a)(1), the government must prove appellant intentionally accessed a computer without authorization or *exceeded* her authorized access, and in doing so obtained information determined by the United States government to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data from a protected computer and then willfully communicated, delivered, or transmitted that information to any person not entitled to receive it, or willfully retained the same.

While appellant pleaded guilty to obtaining and transmitting the classified cables to Wikileaks pursuant to Article 134, UCMJ, she challenges the assimilated crime of violating 18 U.S.C. § 1030(a)(1), asserting the military judge's

[3] Two related assignments of error were raised by Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, and Center for Democracy and Technology, and adopted by appellant: 1) whether the Computer Fraud and Abuse Act prohibits violations of computer use restrictions; and 2) whether the military judge's reading of the act renders the statute unconstitutionally vague.

[4] Appellant pleaded guilty to an Article 134, UCMJ, offense of knowingly accessing more than seventy-five classified United States DoS cables, and willfully communicating, delivering, transmitting, or causing to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, and that such conduct was prejudicial to good order and discipline and of a nature to bring discredit upon the armed forces.

interpretation of that statute was erroneous. Appellant asserts she had the right of *access* to the DoS information she downloaded and transferred to Wikileaks and that the use of the Wget program cannot by itself establish appellant exceeded authorized access within the meaning of the CFAA. Appellant argues the term "exceeds authorized access" is ambiguous and the statute does not encompass use violations but only access violations. Appellant asks this court to apply the rule of lenity and dismiss the specification.

The statute thus provides two ways of committing the crime of improperly accessing a protected computer: 1) accessing without authorization; or 2) exceeding authorized access. 18 U.S.C. § 1030(a)(2)(C). Section 1030(e)(6) defines "exceeds authorized access" as meaning "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [sic] is not entitled so to obtain or alter."[5]

Since appellant pleaded guilty to accessing the SIPRNET system, obtaining DoS cables, and willfully transmitting them to Wikileaks, the question presented is whether appellant's use of the system exceeded her authorized access. In the military justice system, this is a case of first impression. As there is no relevant case law on this issue from military appellate courts, we look to federal courts for guidance. Within federal jurisprudence, a split of opinion amongst the circuits exists. The United States Courts of Appeals for the First, Fifth, Seventh, and Eleventh Circuits read "exceeds authorized access" broadly; the Second, Fourth, and Ninth Circuits have reached a narrower interpretation of this language, or have resolved the issue in favor of appellants based on the rule of lenity.

Under the broad view, "exceeding authorized access" may be shown by how one uses information obtained from a computer system.[6] For example, using the

---

[5] "Viewing material on a computer screen constitutes 'obtaining' information under the CFAA." *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 648 (E.D. Pa. 2007) (citing legislative history for CFAA).

[6] In the case of *United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010), an employee of the Social Security Administration was subject to a policy that forbade "accessing information on its databases for nonbusiness reasons." Rodriguez was charged with violating the CFAA by using his access to copy the personal records of seventeen people for nonbusiness reasons. *Id*. At trial, Rodriguez argued he was authorized to access these databases. *Id*. at 1263-64. The Eleventh Circuit upheld Rodriguez' conviction because he "exceeded his authorized access . . . when he

(continued . . .)

information for an improper purpose (e.g. contrary to a company computer use policy) could show a user "exceeded authorized access." Under the narrower interpretation, users cannot exceed authorized access within the meaning of section 1030(e)(6) when they access information they are authorized to access, even if their access is motivated by an improper purpose or if they use the information for an unauthorized purpose.[7] In other words, a user must gain access to the information through some unauthorized means, for example bypassing controls or misusing a password.

The statute's definition of "exceeds authorized access" provides that the statute is violated when a computer user uses her initial authorized access to then obtain or alter information that she "is not entitled *so* to alter or obtain." 18 U.S.C. § 1030(e)(6) (emphasis added). The "surplusage" canon provides that, "if possible, every word and every provision is to be given effect and that no word should be ignored or needlessly be given an interpretation that causes it to duplicate another provision or to have no consequence." *United States v. Sager*, 76 M.J. 158, 161 (C.A.A.F. 2017). The definition of the word "so" is "in a manner or way indicated or suggested." *Webster's Collegiate Dictionary* 1113 (10th ed. 1999). Given the normal use and meaning of the word "so," we conclude Congress contemplated the statute to reach

---

(continued . . .)
obtained personal information for a nonbusiness reason." *Id*. at 1263. The Eleventh Circuit interpreted "exceeds authorization" to mean outside the scope of the intended authorization. *Id*.; *see also United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010) (one can exceed authorized access when he exceeds the "purposes for which access is 'authorized.'"); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2005) (under an agency-theory, when appellant's adverse interests breached his duty of loyalty, he terminated his authorization to access the company laptop.); *Ef Cultural Travel Bv v. Explorica*, 274 F.3d 577, 581-82 (1st Cir. 2001) (affirming summary judgment because appellant's breach of his broad confidentiality agreement "exceeded authorized access" under the CFAA).

[7] *See e.g. United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 n.7 (9th Cir. 2009) (stating in dicta that defendant does not "exceed 'authorized access' under the CFAA when he breaches a duty of loyalty to authorizing party"); *Bell Aero. Servs. v. U.S. Aero. Servs.*, 690 F. Supp. 2d 1267 (M.D. Ala. 2010); *Orbit One Communs. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D.N.Y. 2010); *Nat'l City Bank, N.A. v. Republic Mortg. Home Loans, LLC*, 2010 U.S. Dist. LEXIS 36946 (W.D. Wash. 2010); *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605 (M.D. Tenn. 2010); *US Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189, 1192 (D. Kan. 2009) (collecting cases); *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.*, 2009 U.S. Dist. LEXIS 72579, at *5-6 (E.D.N.Y. 2009); *Brett Senior & Assocs., P.C. v. Fitzgerald*, 2007 U.S. Dist. LEXIS 50833, at *4 (E.D. Pa. 2007).

users whose initial access to information is authorized, but who later use their access to obtain that information in an unauthorized manner.

Here, appellant's SIPRNET access was limited by a number of memorialized restrictions concerning official use, unauthorized software, and unauthorized introduction of executable files. First, in order to obtain access to her SIPRNET account, appellant agreed to an AUP. The AUP proclaimed that "[a]ccess to [these] network[s] is for official use and authorized purposes as set forth in DOD 5500.7-R 'Joint Ethics Regulation' or as further limited by this policy." The AUP also prohibited the use of unauthorized hardware or software on a SIPRNET system, and the introduction of executable code without authorization.[8] Appellant's computer use was also governed by Army Regulation 25-2, Information Management: Information Assurance (23 March 2009). Army Regulation 25-2 prohibits the use of shareware or freeware, absent authorization. Finally, appellant signed numerous non-disclosure agreements. While some of these sources create restrictions on use of information, others are plainly restrictions on access.

The military judge found 18 U.S.C. § 1030(a)(1) to be ambiguous. She applied lenity and rejected the broad approach. The military judge did not consider appellant's purpose or appellant's transmission of the information to Wikileaks as proof of "exceeding authorized access." She found *how* appellant accessed the information violated the authorized use policy and thus exceeded access. We need not decide which interpretation, narrow or broad, applies to military courts. Here the military judge followed the narrow approach and found appellant's conduct to be an access violation. We agree this was an access violation as discussed below.

Appellant's argument conflates "use" violation with "access" violation. Appellant argues that any access restriction must be code-based or technical. We do not read that requirement into the statute. This case does not hinge on a violation in the use of information—nor did the military judge find a use violation. Rather, the *method and manner* in which appellant accessed the classified State Department system exceeded her authorization. Had appellant gone through all the individual clicks necessary to access the DoS's portal, find and download the files, and repeat those steps seventy-five times—this would present a different issue. We find appellant's use of Wget allowed her to access the cables by circumventing the DoS portal and contacting the server directly, which allowed her to directly download the cables onto her hard drive, and ultimately transmit seventy-five classified cables to Wikileaks.

Based on the foregoing, we conclude computer access *beyond the manner* authorized, meets the element of "exceeds authorized access." Therefore, we find,

[8] Executable code includes .exe, .com, .vbs, and .bat files.

as the military judge did, appellant's use of the Wget program exceeded her authorized access, and thus violated the CFAA.

Clauses 1 and 2 of Article 134, UCMJ.

The military judge found appellant guilty of all three clauses under Article 134, UCMJ. In addition to assimilating 18 U.S.C. § 1030 via clause three of Article 134, UCMJ, in Specification 13 of Charge II, the government also charged and appellant pleaded guilty to violations of clause one and clause two. The military judge found appellant's conduct prejudicial to good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces, pursuant to Article 134, UCMJ. Even assuming appellant's actions fell outside the scope of 18 U.S.C. § 1030(a)(1), appellant's conviction for this Article 134 offense would still stand. Based on the evidence presented, we find appellant's plea provident and conviction legally and factually sufficient under both clauses one and two.

B. The Espionage Act (18 U.S.C. § 793(e))

THE DUE PROCESS CLAUSE AND FIRST AMENDMENT AS APPLIED TO 18 U.S.C. § 793(e)

Appellant asserts 18 U.S.C. § 793(e) is unconstitutionally vague in that the term "relating to national defense" as applied to classified records is not sufficiently clear as to provide fair notice and invites arbitrary law enforcement. Appellant also asserts the statute is unconstitutionally overbroad in that it prohibits a substantial amount of protected speech. We disagree on both counts.

This court reviews de novo the constitutionality of an act of Congress. *United States v. Disney*, 62 M.J. 46, 48 (C.A.A.F. 2005).

Void for Vagueness

The phrase "information relating to the national defense" is not defined in 18 U.S.C. § 793(d). Nonetheless, courts have held that "'national defense' had acquired a well-known meaning 'as a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.'" *United States v. Rosen*, 445 F. Supp. 2d 602, 619 (E.D. Va. 2006) (citing *Gorin v. United States*, 312 U.S. 19, 28 (1941)); *see also United States v. Truong Dinh Hung*, 629 F.2d 908, 918 (4th Cir. 1980); *United States v. Drummond*, 354 F.2d 132, 151 (2d Cir. 1965); *United States v. Heine*, 151 F.2d 813, 817 (2d Cir. 1945).

As observed by the Supreme Court:

> The root of the vagueness doctrine is a rough idea of fairness. It is not a principle designed to convert into a constitutional dilemma the practical difficulties in drawing criminal statutes both general enough to take into account a variety of human conduct and sufficiently specific to provide fair warning that certain kinds of conduct are prohibited.

Colten v. Kentucky, 407 U.S. 104, 110 (1972).

The question in this case is whether the words "information relating to national defense" provide sufficient notice that disclosing information relating to national defense is "unauthorized" and whether appellant's conduct "is plainly within" the terms of the statute.

We reject appellant's claim that the statute is too vague to provide fair notice of the criminal nature of disclosing classified documents. The facts of this case leave no question as to what constituted national defense information. Appellant's training and experience indicate, without any doubt, she was on notice and understood the nature of the information she was disclosing and how its disclosure could negatively affect national defense.

The military judge construed 18 U.S.C. § 793 in a manner consistent with existing precedent. Appellant's conduct falls within that definition. Accordingly, we find no error.

Overbreadth and the First Amendment

Appellant asserts her actions in disclosing classified information related to national security are protected by the First Amendment and that she did not have reason to know the records she disclosed could be used "to the injury of the United States or to the advantage of any foreign nation." We disagree. Appellant had no First Amendment right to make the disclosures—doing so not only violated the non-disclosure agreements she signed, but also jeopardized national security.

United States courts have repeatedly held that the First Amendment does not protect unauthorized disclosures of classified information. A statute is facially overbroad when no set of circumstances exists when it could be valid. *United States v. Salerno*, 481 U.S. 739, 745 (1987). In the context of the First Amendment, a statute is "overbroad" when a substantial number of its applications are unconstitutional when compared with the statute's plainly legitimate sweep. *United States v. Stevens*, 599 U.S. 460, 490-91 (2010). First Amendment overbreadth challenges are an exception to the general rule. *United States v. Morison*, 844 F.2d 1057, 1075 (4th Cir. 1988).

In the face of a similar First Amendment challenge, the United States Court of Appeals for the Fourth Circuit, in *Morison*, upheld the Espionage Act convictions of an employee of the Naval Intelligence Support Center who had a Top Secret security clearance and had also signed a non-disclosure agreement. *Id*. at 1060. The accused unsuccessfully argued his conviction under the Espionage Act could not stand because he leaked the classified information to the press, rather than to a foreign power. *Id*. at 1063.

The Fourth Circuit stated:

> [T]hough he cannot point to anything in the legislative record which intimates that Congress intended to exempt "leaks to the press," as the defendant describes it, he argues that, unless such an exemption is read into these sections they will run afoul of the First Amendment. Actually we do not perceive any First Amendment rights to be implicated here . . . . It is a prosecution under a statute, of which the defendant, who, as an employee in the intelligence service of the military establishment, had been expressly noticed of his obligations . . . is being prosecuted for purloining from the intelligence files of the Navy national defense materials clearly marked as "Intelligence Information" and "Secret" and for transmitting that material to "one not entitled to receive it" . . . . We do not think that the First Amendment offers asylum under those circumstances . . . merely because the transmittal was to a representative of the press.

Id. at 1068 (citing *Branzburg v. Hayes*, 408 U.S. 665, 691 (1972) ("It would be frivolous to assert—and no one does in these cases—that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws.")).

We squarely reject appellant's First Amendment challenge and firmly hold that a soldier who willfully communicates information relating to the national defense "is not entitled to invoke the First Amendment as a shield to immunize his act of thievery." *Morison*, 844 F.2d at 1069-70 ("To permit the thief thus to misuse the Amendment would be to prostitute the salutary purposes of the First Amendment.").

C. Stealing, Purloining, or Converting (18 U.S.C. §641)

NOTICE, MAJOR CHANGE, AND LEGAL AND FACTUAL SUFFICIENCY TO SUSTAIN CONVICTIONS FOR VIOLATING 18 U.S.C. § 641, TO WIT, STEALING, PURLOINING, OR CONVERTING "DATABASES" (SPECIFICATIONS 4, 6, 8, 12, AND 16 OF CHARGE II)

Appellant was found guilty of five specifications of violating 18 U.S.C. § 641 for stealing, purloining, or knowingly converting various "databases," in Specifications 4, 6, 8, and 12 of Charge II and for stealing, purloining, or knowingly converting the "USF-GAL" in Specification 16 of Charge II. The military judge granted the government's motion to amend Specifications 4, 6, and 16 of Charge II to include the words "a portion of" in front of the words "database" and the "USF-GAL" and then found appellant guilty in accordance with the amended specifications. In other words, appellant was found to have stolen, purloined or converted "information" from those databases—only a portion of the contents of the database—not the database itself. In the remaining two specifications, appellant was found guilty of stealing the entire SOUTHCOM and DoS NCD database.

Appellant asserts she was not on notice to defend against stealing, converting, or purloining various documents and records contained *within* each database she was alleged to have stolen or converted. She asserts the amendments of Specifications 4, 6, and 16 of Charge II created major changes, leaving her unprepared to defend against said specifications.

For the following reasons, we find appellant was properly on notice to defend against the records contained within the databases and thus, the military judge created no major change.

Notice

It is well understood that the military is a notice-pleading jurisdiction. As our superior court has held:

> The true test of the sufficiency of an indictment is not whether it could have been made more definite and certain, but whether it contains the elements of the offense intended to be charged, and sufficiently apprises the defendant of what he must be prepared to meet; and, in case any other proceedings are taken against him for a similar offense, whether the record shows with accuracy to what extent he may plead a former acquittal or conviction.

United States v. Sell, 3 U.S.C.M.A. 202, 206, 11 C.M.R. 202, 206 (1953). Rule for Courts-Martial (R.C.M.) 307(c)(3) also provides for notice pleading.

Appellant argues the government should have specifically included the particular documents alleged to have been stolen by appellant within each specification so as to provide notice. Under the facts of this case, we do not see this as necessary. Each specifications apprised appellant of the essential elements of the crime under 18 U.S.C. § 641 to include the conduct (steal, purloin, or convert), what (records), when, and the value of the items. We find the specifications were sufficient to apprise appellant of what she needed to defend herself against, and to protect her from subsequent prosecution for the same conduct.

Major Change

We turn next to the military judge's decision to grant the government's motion to amend the charge sheet with respect to Specifications 4, 6, and 16 of Charge II. Appellant argues that the military judge fundamentally changed the nature of the charged property from 'databases' to 'information and records' contained within the databases and thus created a major change.

"Whether a change made to a specification is minor is a matter of statutory interpretation and is reviewed de novo." *United States v. Reese*, 76 M.J. 297, 300 (C.A.A.F. 2017) (citing *United States v. Atchak*, 75 M.J. 193, 195 (C.A.A.F. 2016)). Rule for Courts-Martial 603(a) provides "[m]inor changes in charges and specifications are any except those which add a party, offenses, or substantial matter not fairly included in those previously preferred, or which are likely to mislead the accused as to the offenses charged." The government can make minor changes to a charge and specification before arraignment. R.C.M. 603(b). Major changes, or "[c]hanges or amendments to charges or specifications other than minor changes may not be made over the objection of the accused unless the charge or specification affected is preferred anew." R.C.M. 603(d).

Generally, "changes in the alleged time or date of an offense are permissible since they normally do not affect the substance of the offense, preclude invocation of the statute of limitations, or mislead the accused as to that which he must defend against." *United States v. Longmire*, 39 M.J. 536, 538 (A.C.M.R. 1994) (internal citations omitted)). Applying the plain language of R.C.M. 603, we do not find the military judge erred in finding the changes were minor.

First, the change did not alter the substance of the offenses and the overt acts remained the same. The alleged conduct remained essentially the same. Second, the change did not affect a substantial matter not fairly included in the previously preferred charges and specifications.

The plain meaning of the word "database" necessarily includes the records that make up the database.[9] In the charged specification, each specific database identified is followed by the phrase "containing more than [a number] records." By numbering the records within the database, the government explicitly noted that the databases are made up of many records. It would seem that finding appellant guilty of stealing only a portion of the records within the database is the equivalent of finding her guilty of a lesser-included offense.

Given this modification, we see no palpable way in which defense counsel would have altered their trial defense strategy, which was: to justify appellant's takings as excusable; attacking whether a purloining, stealing, or converting had actually occurred; and attacking whether appellant's actions seriously and substantially interfered with the government's rights in the information. We do not find appellant was misled in any meaningful way by this change thereby prejudicing her defense trial strategy.

Further, the change did not expose appellant to greater punishment. It actually reduced the amount of information alleged to have been stolen. The nature of the offense did not change nor is appellant at some risk for another prosecution for the same conduct in that a new charge would contain the same information. Accordingly, this court finds, as the military judge did, appellant was on notice the specifications alleged the theft of documents contained within the databases and that the substituted language was a minor change. To that end, we conclude changing the specifications from alleging specific databases containing records to alleging "a portion of" those databases neither materially altered the specifications nor was the change likely to mislead appellant.

Factual and Legal Sufficiency Regarding "Stealing, Purloining, and Converting" Records and Information

Appellant asserts the evidence was factually and legally insufficient to support appellant's convictions for stealing, purloining, and converting records and information. Specifically, appellant argues the government failed to prove the records themselves, or the information contained within those records, were stolen or converted because they never left the government's possession and appellant's actions did not deprive the government of use of benefit of the information either temporarily or permanently. We disagree.

We review factual and legal sufficiency de novo. UCMJ art. 66(c). The test for factual sufficiency is "whether, after weighing the evidence in the record of trial and making allowances for not having personally observed the witnesses, the

[9] Database is defined as "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*, 422 (8th ed. 1999).

members of [this court] are [ourselves] convinced of appellant's guilt beyond a reasonable doubt." *United States v. Rosario*, 76 M.J. 114, 117 (C.A.A.F. 2017) (quoting *United States v. Oliver*, 70 M.J. 64, 68 (C.A.A.F. 2011)). In conducting this fresh look, we apply "neither a presumption of innocence nor a presumption of guilt" but rather make an "independent determination as to whether the evidence constitutes proof of each required element beyond a reasonable doubt." *United States v. Washington*, 57 M.J. 394, 399 (C.A.A.F. 2002). "The test for legal sufficiency is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Gutierrez*, 73 M.J. 172, 175 (C.A.A.F. 2014) (quoting *United States v. Bennitt*, 72 M.J. 266, 268 (C.A.A.F. 2013)).

Appellant argues a digital copy is distinct from the original digital record contained within the database and that appellant's actions did not seriously interfere with the government's property rights in the database because the information never left the government's possession.

In *United States v. DiGilio,* the United States Court of Appeals for the Third Circuit considered a similar issue. 538 F.2d 972 (3rd Cir. 1976). DiGilio and his associates were indicted for conspiracy to defraud the United States, and for converting to their own use photocopies of official files of the Federal Bureau of Investigation. *Id*. at 975. DiGilio argued that the government was not deprived of the use of the information within these records, and thus his conduct did not fall within § 641. *Id*. at 977. DiGilio further argued that the copies are not themselves "'records' within the meaning of the statute." *Id*. In support of this argument, he urged the court "that at most, the government lost exclusive possession of the information contained in its confidential records, and that Congress never intended [18 U.S.C.] § 641. . . to protect the governmental interest in exclusive possession of information." *Id*. The court found appellant used government time, resources, and supplies to make the copies. The court held "[a] duplicate copy is a record for purposes of the statute, and duplicate copies belonging to the government were stolen." *Id*. *see also United States v. Fowler*, 932 F.2d 306, 309-10 (4th Cir. 1991) (appellant attempted to argue that documents and the information contained within those documents were different; the court rejected this argument, held "information is a species of property and a thing of value.").

In this case, the evidence supports, and we find beyond a reasonable doubt, that appellant created duplicates of the records contained within the databases, took the duplicate records, and at the time she took the duplicate records, she intended to send them to Wikileaks, depriving the government of their exclusive use and benefit. We find the government had a property interest in the information, including the right to protect classified information by storing it in a secure location and further restricting access. Consistent with the military judge's findings, we conclude ample

evidence exists to satisfy the evidentiary requirements of "stealing, purloining, or knowingly converting" for the purposes of 18 U.S.C. § 641.

D. Expert Testimony

THE GOVERNMENT'S COUNTERINTELLIGENCE EXPERT ON THE VALUE OF THE INFORMATION AT ISSUE IN SPECIFICATIONS 4, 6, 8, 12, AND 16 OF CHARGE III

Appellant challenges the military judge's decision to permit expert testimony on the value of records in Specifications 4, 6, 8, and 12 of Charge II.

We review a military judge's decision to permit expert testimony pursuant to Military Rule of Evidence (Mil. R. Evid.) 702 for an abuse of discretion. *United States v. Billings*, 61 M.J. 163, 166 (C.A.A.F. 2005). "The military judge has broad discretion as the 'gatekeeper' to determine whether the party offering expert testimony has established an adequate foundation with respect to reliability and relevance." *United States v. Green*, 55 M.J. 76, 80 (C.A.A.F. 2001). "The abuse of discretion standard is a strict one, calling for more than a mere difference of opinion. The challenged action must be 'arbitrary, fanciful, clearly unreasonable,' or 'clearly erroneous.'" *United States v. McElhaney*, 54 M.J. 120, 130 (C.A.A.F. 2000); *see also United States v. Sanchez*, 65 M.J. 145, 148-49 (C.A.A.F. 2007). Whether the military judge properly followed *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 592-97 (1993) is reviewed de novo. *McElhaney*, 54 M.J. at 130.

Determining Value

The military judge defined value, with respect to 18 U.S.C. § 641, as:

> "Value" means the greater of 1) the face, par, or market value, or 2) the cost price, whether wholesale or retail. A "thing of value" can be tangible or intangible property, government information, although intangible, is a species of property and a thing of value. The market value of stolen goods may be determined by reference to a price that is commanded in the market place whether that market place is legal or illegal. In other words, market value is measured by the price a willing buyer will pay a willing seller. (The illegal market place is also known as a "thieves market.") "Cost price" means the cost of producing or creating the specific property allegedly stolen, purloined, or knowingly converted.

Value is an essential element of the crime in a prosecution under 18 U.S.C. § 641. Therefore the government must prove beyond a reasonable doubt that the property stolen had value. *United States v. Lignon*, 440 F.3d 1182, 1184 (9th Cir. 2006) (citing *United States v. Seaman*, 18 F.3d 649, 650 (9th Cir. 1994)). If the value of the property exceeds $1,000, the maximum punishment is confinement for ten years. 18 U.S.C. § 641. If the value of the property is $1,000 or less, the maximum punishment is confinement for one year. *Id*. As the statute reads, there are two major measures of value: the measure of value in exchange (face, par, or market) and the measure of value as calculated by the cost to the government for creation or acquisition (wholesale or retail). *United States v. Kroesser*, 731 F.2d 1509, 1516-17 (11th Cir. 1984).

This is not a case where intellectual property is stolen and a company can assess the value of that stolen information based on profit loss or some other quantitative measurement. Thus there is no "readily ascertainable" market value. In such a situation, courts agree that "any reasonable method may be employed to ascribe an equivalent monetary value to the items." *Ligon*, 440 F.3d at 1184 (internal citations omitted); *see also United States v. Batti*, 631 F.3d. 371, 374 (6th Cir. 2011). This includes the value in what is referred to as the "thieves market." *United States v. Drebin*, 557 F.2d 1316, 1328 (9th Cir. 1977); *see also United States v. Langston*, 903 F.2d 1510, 1514 (11th Cir. 1990) and *United States v. Wright*, 661 F.2d 60, 61 (5th Cir. 1981).

The government offered evidence of this measure of value using different types of information for various specifications. This is not inappropriate. With respect to the information at issue in Specifications 4, 6, and 12 of Charge II (CIDNE-I, CIDNE-A, DoS NCD respectively), the government offered both cost price and market value. The military judge ultimately only accepted the market value information. For Specification 8 of Charge II (SOUTHCOM), the government offered both cost price and thieves' market value and the military judge accepted both measures. Finally, for Specification 16 of Charge II (USF-GAL), the government offered cost price (maintenance and creation) and thieves' market value. The military judge accepted the creation cost and thieves' market value.[10]

The measure of value offered by the government was appropriate. We turn now to the issue of whether the basis for that measure of value, the opinion testimony of Mr. Lewis, was appropriate.

[10] The military judge declined to consider database management, hardware, software, or maintenance costs. Instead, she considered only evidence of costs associated with the creation of the individual records or email accounts as part of the "cost price" for Specifications 8 and 16.

Mr. Lewis' Qualifications and Ability to Opine on Value

In the instant case, the defense did not object to Mr. Lewis' qualifications as an expert in counterintelligence (CI).[11] They did, however, object to his expertise in the "valuing of government information by foreign intelligence services" (valuation). After a substantial hearing on the matter, with both open and closed sessions, the military judge found Mr. Lewis to be an expert in CI, but not an expert in the valuation of all government information by foreign intelligence services.

Instead, the military judge ruled that Mr. Lewis could offer his opinion on the value of certain documents if a proper foundation was laid. This is what occurred. The military judge found a foundation was properly laid showing how Mr. Lewis was familiar with the value of specific information to specific potential buyers based on his experience with similar exchanges.

The military judge found that Mr. Lewis was basing his testimony on information gathered through offensive CI operations that was systematically entered into a system employed by the Counter Espionage Division of the Defense Intelligence Agency (DIA). She further found those systems were used to prepare briefings at the highest levels, including before Congress, and are generally accepted as accurate. The military judge concluded the data collected by those systems was reliable. The military judge approached her rulings in a methodical manner, and placed her findings and analysis on the record. Finally, we find the opinion testimony regarding valuation did not exceed the scope of the witness's expertise. *United States v. Flesher*, 73 M.J. 303, 315 (C.A.A.F. 2014).

The Value of the USF-GAL

While we find the classified information that accounts for Specifications 4, 6, 8, and 12 of Charge II has value in a thieves' market clearly in excess of $1,000.00,

[11] Mr. Lewis was the Senior Expert and Counterintelligence Advisor to the Directorate of Science and Technology for the DIA. He regularly advised the most senior officials in the DIA, and provided briefings to the Secretary and Undersecretary of Defense for Intelligence and to Congress. He has spent nearly thirty years in the field of CI, holding many different roles and having varying levels of responsibility. We are confident that Mr. Lewis is more than qualified in the field of CI. We also find that without enlightenment "from those having a specialized understanding of the subject," the factfinder would not be qualified to determine intelligently and to the best possible degree the valuation of the property at issue. *United States v. Houser*, 36 M.J. 392, 399 (C.A.A.F. 1993) (quoting *State v. Chapple*, 135 Ariz. 281, 292-93, 660 P.2d 1208, 1219-20 (1983)) (internal citations omitted)).

we are not so convinced of the value of the USF-GAL, which accounts for Specification 16 of Charge II. *Rosario*, 76 M.J. at 117.

The record reflects that appellant downloaded 74,000 .mil email accounts from the USF-GAL, and that she did so at the request of Wikileaks. We find the evidence of the value of the USF-GAL email addresses, both in terms of cost price and the thieves' market, to be more speculative, unlike evidence of classified information with which Mr. Lewis is more familiar. Accordingly, we are not convinced beyond a reasonable doubt that the value of the email addresses exceeded $1,000—but rather find the USF-GAL email addresses have *some* value. *Id*. We grant relief in our decretal paragraph.

E. Article 13 Credit

WHETHER THIS COURT SHOULD DISMISS ALL CHARGES, OR ALTERNATIVELY, AWARD MORE SENTENCING CREDIT, WHERE THE MILITARY JUDGE FOUND MULTIPLE VIOLATIONS OF ARTICLE 13, UCMJ, BUT FAILED TO CONSIDER THAT PFC MANNING WAS IN SOLITARY CONFINEMENT FOR APPROXIMATELY NINE MONTHS WHILE STRUGGLING WITH SEVERE MENTAL ILLNESS?[12]

Article 13, UCMJ, prohibits: 1) punishment of an accused prior to trial and, 2) conditions of arrest or pretrial confinement that are more rigorous than necessary to ensure an accused's presence for trial. Prong one involves the examination of both the purpose of the conditions of confinement and the intent behind the use of those conditions by government officials. Prong two involves examining whether the conditions of pre-trial confinement are so excessive as to constitute punishment. *See United States v. King*, 61 M.J. 225, 227-28 (C.A.A.F. 2005).

The question of intent to punish is "one significant factor in [the] judicial calculus" for determining whether there has been an Article 13 violation. *United States v. Huffman*, 40 M.J. 225, 227 (C.M.A. 1994) (citing *Bell v. Wolfish*, 441 U.S. 520 (1979)). An appellate court will defer to the findings of fact by the military judge where those findings of fact are not clearly erroneous. *United States v. Mosby*, 56 M.J. 309, 310 (C.A.A.F. 2002) (internal citation omitted). We will review de novo the ultimate question whether an appellant is entitled to credit for a violation of Article 13, UCMJ. *Id*. Further, the sufficiency of relief for violations

[12] The related assignment of error of whether appellant's confinement was unconstitutional and unlawful was raised by Amnesty International Ltd. and adopted by appellant.

of Article 13, UCMJ, is reviewed for an abuse of discretion. *United States v. Williams*, 68 M.J. 252, 257 (C.A.A.F. 2010).

The burden is on appellant to establish entitlement to additional sentence credit because of a violation of Article 13. *See* R.C.M. 905(c)(2). Whether appellant is entitled to credit for a violation of Article 13 is a mixed question of fact and law. *Mosby*, 56 M.J. at 310-11 (internal citations omitted).

After a lengthy review of witness testimony concerning the facts and circumstances related to the conditions of appellant's confinement, the military judge found the government did not intend to punish appellant, but rather intended to ensure she was safe, did not hurt herself, and was present for her court-martial.

Despite this finding, the military judge also found confinement conditions placed on appellant more onerous than necessary to ensure appellant's presence at trial. As such, the military judge gave appellant credit for four Article 13 violations. First, she gave appellant seventy-five days confinement credit for being held in "prevention of injury" (POI) status against the recommendation of mental health professionals from 1 November 2010 through 17 January 2011. Second, appellant received twenty-five days credit for being kept in POI status against the recommendations of mental health professionals after 1 April 2011. Third, she received ten days credit for being allowed only 20 minutes rather than one hour of outside recreation time a day from 29 July to 10 December 2010. Fourth, appellant received seven days credit for being held in suicide risk (SR) status against the recommendation of mental health professionals from 7-11 August 2010 and 19-20 January 2011. Cumulatively, the military judge granted appellant 112 days of pretrial confinement credit.

Based on appellant's conditions of confinement, the military judge found appellant was not held in solitary confinement. She found appellant was not alone and without human contact. She found appellant was held in a cell similar to that of other detainees at the facility and that appellant could see and hear what was going on in the hallway. Appellant also had weekly visits from her counsel and health care professionals and daily visits by brig staff. We do not find the military judge's findings to be clearly erroneous.

Appellant has not established the government's intent to punish appellant through her conditions of confinement. Both the direct and circumstantial evidence upon which the military judge made her decision support the military judge's determination. Based on the record before us, we hold the military judge's findings are not clearly erroneous. We further find the military judge did not abuse her discretion in determining the amount of credit to give appellant.

Even if this court were to find appellant was entitled to additional Article 13, UCMJ, credit, we take note that prior to the President's commutation, appellant requested this court either dismiss the charges or in the alternative provide appellant with 2640 days of confinement credit (roughly seven years credit). This would have reduced appellant's sentence from 35 years confinement to 28 years confinement. The President's commutation puts appellant in a better position than the confinement credit she requested.

CONCLUSION

The court AFFIRMS only so much of the finding of guilty of Specification 16 of Charge II as finds that the appellant

> Did, at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010, steal, purloin, or knowingly convert to his use or the use of another, a record or thing of value of the United States or of a department or agency thereof, to wit: a portion of the United States Forces – Iraq Microsoft Outlook / SharePoint Exchange Server global address list belonging to the United States government, of some value, in violation of 18 U.S. Code Section 641, such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

The remaining findings of guilty are AFFIRMED.

In accordance with the principles articulated by our superior court in *United States v. Winckelmann*, 73 M.J. 11, 15-16 (C.A.A.F. 2013) and *United States v. Sales*, 22 M.J. 305 (C.M.A. 1986), we are able to reassess the sentence on the basis of the error noted and do so after conducting a thorough analysis of the totality of circumstances presented by appellant's case and the President's commutation of appellant's sentence.

In evaluating the *Winckelmann* factors, the penalty landscape was reduced by nine years from ninety years to eighty-one years. Additionally, the remaining offenses capture the gravamen of appellant's misconduct. Finally, the sentence was adjudged by a military judge so we may reliably determine what sentence would have been imposed at trial. We are confident that based on the entire record and appellant's course of conduct, the military judge would have imposed a sentence of at least that which was adjudged.

Reassessing the sentence based on the noted error and the remaining findings of guilty, we AFFIRM the sentence as adjudged and approved. We find this

reassessed sentence is not only purged of any error but is also appropriate. All rights, privileges, and property, of which appellant has been deprived by virtue of that portion of the findings set aside by our decision, are ordered restored.

Judge CELTNIEKS and Judge HAGLER concur.

FOR THE COURT:

MALCOLM H. SQUIRES, JR.
Clerk of Court