IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
AUGUSTA DIVISION

UNITED STATES OF AMERICA	*	
	*	**CR 1:17-34**
v.	*	
	*	
REALITY LEIGH WINNER,	*	
	*	
Defendant.	*	
	*	
	*	
	*******	

GOVERNMENT'S SENTENCING MEMORANDUM

In February 2017, only a couple of months after the completion of her six years in the United States Air Force, defendant Reality Leigh Winner returned to the government as a contractor with a private corporation assigned to the National Security Agency ("NSA"). During various times in the Air Force, as well as during her work as a contractor, the defendant held a TOP SECRET//SENSITIVE COMPARTMENTED INFORMATION ("SCI") security clearance and had access to classified information. From the defendant's many years with a security clearance—and as she acknowledged on numerous occasions during security briefings—she understood the harm that the unauthorized disclosure of classified information can cause to our national security. Despite this knowledge, on or about May 9, 2017, the defendant searched for, identified, and printed a classified intelligence report, which was classified at the TOP SECRET//SCI level and contained national defense information ("NDI"). The defendant then removed it from its authorized location and put it in a mailbox in an envelope addressed to a news agency. As the defendant admitted when she pled guilty, she did not engage in this conduct by accident, mistake, or any other innocent reason. Rather, the defendant acted with

knowledge that her disclosure was both unauthorized and unlawful. In so doing, she knowingly and intentionally betrayed the trust of her country and jeopardized our national security. In fact, subject matter experts have assessed that the defendant's unauthorized disclosure caused exceptionally grave harm to our national security.

The defendant has now accepted responsibility for her very serious crime. The government and the defendant agree that the appropriate sentence is a term of imprisonment for 63 months followed by three years of supervised release. The government respectfully requests that the Court accept the parties' agreement pursuant to Federal Rule of Criminal Procedure 11(c)(1)(C), and sentence the defendant accordingly.

I. PROCEDURAL BACKGROUND

The defendant was arrested after the Federal Bureau of Investigation ("FBI") executed a search warrant at her residence on June 3, 2017, for evidence of, *inter alia*, violations of Title 18, United States Code, Section 793(e) (hereinafter, "Section 793(e)"). She was subsequently charged by criminal complaint on June 5, 2017, with one count of violating Section 793(e), and on June 7, 2017, the defendant was indicted on the same violation.[1] On June 21, 2018, the parties executed a plea agreement pursuant to Rule 11(c)(1)(C) (the "Plea Agreement"), in which the parties agreed the appropriate sentence for the defendant's crime is a sentence of imprisonment for 63 months followed by a three-year term of supervised release. The Court held a change of plea hearing on June 26, 2018, *see* Dkt. 315, during which the defendant entered a

[1] The Defendant was subsequently charged with one count of violating Section 793(e) in a superseding indictment that did not differ substantively from the original indictment.

guilty plea, *see* Dkt. 316, but the Court deferred its decision of whether to accept the plea until after the issuance of the presentence investigation report ("PSR").

On August 7, 2018, the final PSR was provided to the parties and the Court. The U.S. Probation Office calculated a total offense level of 29[2] and a criminal history category of I, resulting in an advisory guidelines range of 87 to 108 months. PSR ¶ 69. As set forth in the Plea Agreement, the parties agree with this guidelines calculation. Plea Agreement ¶ 11. The sentencing in this case is set for August 23, 2018. *See* Dkt. 319.

II. FACTUAL BACKGROUND

A. Professional Background

To place the defendant's conduct in context, it is important to appreciate her lengthy government employment, during which she became well-acquainted with the proper handling of classified information and the consequences of unauthorized disclosures. In May 2017, when the defendant committed the charged unauthorized disclosure, she was employed as a contractor with a private corporation, Pluribus International ("Pluribus"), and was assigned to an NSA facility in the Southern District of Georgia. *See* PSR ¶ 5. As a result of her official responsibilities, the defendant held a TOP SECRET//SCI security clearance and had access to classified information and NDI. *Id.*[3] Although the defendant had only been employed at

[2] Pursuant to U.S.S.G. § 2M3.3(a)(1), the base offense level is 29. The defendant's base offense level is increased by two levels for abuse of a position of trust. *See* U.S.S.G. § 3B1.3. The defendant plainly abused her position of trust as an intelligence agency contractor who had a TOP SECRET//SCI security clearance and had signed multiple nondisclosure agreements. The defendant's base offense level is decreased by two levels because she accepted responsibility for the offense. *See* U.S.S.G. §3E1.1(a).

[3] Information classified at any level can only be lawfully accessed by persons determined by an appropriate United States government official to be eligible for access to classified information,

Pluribus since February 2017, the defendant had been affiliated with the United States Air Force between in or about December 2010 through in or about December 2016, and she had also held a TOP SECRET//SCI security clearance during various times in that period. *Id.* at ¶ 6.

Of importance, the defendant was well trained in the proper handling of classified intelligence and knew the damage that unauthorized disclosures could cause to our national security. Prior to May 2017, the defendant received training regarding classified information, including the definitions of classified information, the levels of classification, and SCI, as well as the proper handling, marking, transportation, and storage of classified materials. *Id.* at ¶ 10. The defendant knew that the unauthorized removal of classified materials and transportation and storage of these materials in unauthorized locations risked disclosure and transmission of those materials and therefore could endanger the national security of the United States and the safety of its citizens. *Id.* In particular, the defendant knew that the unauthorized disclosure of TOP SECRET information reasonably could be expected to cause exceptionally grave damage to the national security of the United States,[4] and that violation of rules governing the handling of classified information could result in criminal prosecution. *Id.*

---

who have a security clearance, who have signed an approved non-disclosure agreement, and who have a "need to know" the classified information.

[4] Information may be classified as "TOP SECRET" if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security. Exec. Order 13526 § 1.2. Access to SCI is further restricted. SCI is a type of classified information concerning or derived from sensitive intelligence sources, methods, or analytical processes. SCI must be handled within formal access control systems established by the Director of National Intelligence. One must receive explicit permission to access an SCI control system or compartment. Once it is determined a person should have access to an SCI compartment, that person signs a nondisclosure agreement specific to that compartment.

B. Defendant's Unauthorized Disclosure of National Defense Information

The defendant has admitted that her unauthorized disclosure of TOP SECRET national defense information was not an accident or a mistake. Plea Agreement at ¶ 2o. Rather, the defendant's unauthorized disclosure was the calculated culmination of a series of acts. On November 9, 2016, just prior to her separation from the Air Force and the termination of her access to classified information, the defendant researched whether it was possible to insert a thumb drive into a Top Secret computer without being detected, and then inserted a thumb drive (which the government never recovered) into a Top Secret computer. Dkt. 163 at 10; Dkt. 115 at 5-6; Dkt. 120 (Transcript of Detention Hearing (Sept. 29, 2017)) at 48-49. Soon after her discharge from the Air Force, the defendant researched job opportunities that would provide her renewed access to classified information. She contemporaneously searched for information about anti-secrecy organizations such as Anonymous and Wikileaks. Dkt. 163 at 10.

On or about February 9, 2017, the defendant became a linguist with Pluribus, assigned to the NSA. She signed a non-disclosure agreement in which she both promised to keep secret classified information and attested she was accepting this responsibility "without any mental reservation or purpose of evasion." Dkt. 107 at 4. Notwithstanding this oath, the Defendant had, approximately eight days before starting work with Pluribus, installed the Tor[5] browser on her

[5] The Onion Router is a tool that renders any user's Internet activity anonymous. It is commonly referred to as "Tor." The U.S Naval Research Laboratory designed Tor as a project to be implemented and deployed for the primary purpose of protecting government communications. It is now available to the public at large. The Tor software protects users' privacy online by relaying their Internet communications through multiple computers around the world and adding a layer of encryption at each relay. As a result, no single relay point records both the original source address and destination address for Internet traffic. This prevents attribution of Internet communications to a particular machine or location, and permits a user to access sites that could

computer. Then, two days before starting work with Pluribus, the defendant had used her phone to capture an image of a webpage listing eight "securedrop" addresses for media outlets seeking leaked information. Dkt. 163 at 10; Dkt. 109 at 2. Also, on February 9, 2017, the defendant sent a message to her sister mocking Pluribus's security training. Dkt. 163 at 11; Dkt. 110 at 28 ("[I]t was hard not to laugh when [the security officer] was like, "yeah so uh we have guys like Edward Snowden . . . so uh we uh have to keep an eye out for that insider threat, especially with contractors . . . .").

In the ensuing months, Winner repeatedly expressed contempt for the United States. On February 25, 2017, Winner wrote that she was "gonnafail" her polygraph examination, which would ask if she had "ever plotted against" the government; claimed that she said she "hate[s] America like 3 times a day"; and when asked "But you don't actually hate America, right?", responded, "I mean yeah I do it's literally the worst thing to happen on the planet." Dkt. 163 at 11; Dkt. 110 at 32. On March 7, 2017, Winner expressed delight at an alleged compromise of classified information, and indicated that she was on the "side" of Wikileaks founder Julian Assange and alleged NSA leaker Edward Snowden. Dkt. 163 at 11; Dkt. 110 at 34.

On May 5, 2017, a U.S. Intelligence Community Agency (the "Agency") produced an intelligence report and attachment (collectively, the "Intelligence Report") that contained NDI. Plea Agreement ¶ 2h. The Intelligence Report was classified at the TOP SECRET//SCI level, and marked as such. PSR ¶ 13. On or about May 9, 2017, the defendant willfully disclosed the Intelligence Report to a news outlet (the "News Outlet"). She did so by searching for,

---

otherwise be blocked. In addition, sites on the "dark web," including "hidden services," are only accessible through Tor.

identifying, and printing the Intelligence Report and sending it to the News Outlet. *Id.* at ¶¶ 15, 17.

The Intelligence Report described intelligence activities by a foreign government directed at targets within the United States and revealed the sources and methods used to acquire the information contained in the Intelligence Report. Plea Agreement ¶ 2j.[6] Such information was NDI: it related to the military and national preparedness of the United States; its disclosure would be potentially damaging to the United States or useful to an enemy of the United States; and it was closely held by the United States, as it had not been made public by the United States and was not found in sources lawfully available to the general public. *Id.* at ¶ 2k. Instead, the Intelligence Report was disseminated on a classified database, access to which was restricted to authorized users who possessed a TOP SECRET//SCI security clearance, authorized access to the classified SCI compartment at issue, and authorized access to the classified database itself. The Agency confirmed that although the defendant had the required access to search for and view the Intelligence Report, the information contained in the Intelligence Report was unrelated to her job duties, and the defendant therefore did not possess a "need to know." PSR at ¶ 16. As the defendant knew, the News Outlet did not have lawful access to the contents of the Intelligence Report. Nor was the defendant ever authorized, directly or indirectly, by the United States to deliver, communicate, or transmit any national defense information to the News Outlet or any other member of the media. *See* Plea Agreement at ¶¶ 2m, n.

[6] The Intelligence Report remains classified. On July 13, 2017, the parties submitted to the Court to supplement the PSR a "Classified Addendum to Joint Statement of Offense Conduct" (hereinafter, "Classified PSR Addendum"). The Classified PSR Addendum describes the Intelligence Report in greater detail.

U.S. Government subject matter experts have determined that the defendant's unauthorized disclosure caused exceptionally grave harm to U.S. national security, which included, but was not limited to, impairing the ability of the United States to acquire foreign intelligence information similar to the information the defendant disclosed.[7]

C. Defendant's Statements to the FBI

The FBI interviewed the defendant on June 3, 2017. In her interview, the defendant admitted (after initial denials and false statements) intentionally identifying and printing the Intelligence Report, despite not having a "need to know" and with knowledge that the Intelligence Report was classified. PSR ¶ 17. She further admitted to removing the Intelligence Report from her office space, retaining it, and mailing it to the News Outlet, which she knew was not authorized to receive it. *Id.* She acknowledged that the content of the Intelligence Report, including information about "sources and methods," could be damaging to the United States if revealed. *Id.* The defendant admitted that despite this knowledge, she intended for the News Outlet to publish the content of the Intelligence Report. *Id.*

III. APPLICABLE LAW

Section 3553, Title 18, provides that, in determining a particular sentence, the Court should consider the nature and circumstances of the offense and characteristics of the defendant. 18 U.S.C. § 3553(a)(1). In addition, it states that the Court must consider other factors, including the need for the sentence "to reflect the seriousness of the offense, to promote respect for the

[7] For this reason, although the government is not seeking an upward departure, one could be appropriate because the defendant "significantly endangered" national security. *See* U.S.S.G. § 5K2.14. The harm caused by the defendant's unauthorized disclosure is further explained in the Classified PSR Addendum. *See* Classified PSR Addendum at 7-8.

law, . . . to provide just punishment for the offense; [and] to afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(A) & (B). Further, the sentence should protect the public from further crimes of the defendant and provide the defendant with needed correctional treatment. 18 U.S.C. § 3553(a)(2)(C) & (D). Finally, the sentence should "avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6).

IV. THIS COURT SHOULD ACCEPT THE PARTIES' AGREEMENT AND SENTENCE THE DEFENDANT ACCORDINGLY

As the Court is aware, the parties have reached an agreement as to the appropriate sentence in this case pursuant to Federal Rule of Criminal Procedure 11(c)(1)(C). Specifically, the parties have agreed that the defendant should be sentenced to 63 months of imprisonment and three years of supervised release. The agreement reflects a fair resolution of the defendant's criminal culpability especially when balanced against the further harm to the national security that would likely result from a trial.

As an initial matter, a significant term of incarceration for the defendant is plainly appropriate. Given the defendant's long history of government employment, the defendant understood the trust the United States places in individuals who receive a security clearance. The defendant blatantly violated this trust. Around the same time the defendant took a job with Pluribus requiring a security clearance in February 2017, she was expressing contempt for the United States, mocking compromises of our national security, and making preparations to leak intelligence information. Then, in May 2017, she compromised national security by providing the News Outlet with the TOP SECRET//SCI Intelligence Report. By definition, the unauthorized disclosure of TOP SECRET information can reasonably be expected to cause

exceptionally grave damage to the national security. Exec. Order 13526 § 1.2. In this instance, subject matter experts confirmed that it did. PSR ¶ 22.

Further, the defendant has specifically disavowed that she acted by accident or mistake, and agreed instead that she acted willfully—that is, she knew that her conduct was a violation of U.S. criminal laws. Plea Agreement ¶ 2o. Moreover, she has admitted that she knew the Intelligence Report was classified as TOP SECRET//SCI and contained national defense information.[8]

The parties' sentencing agreement provides a just resolution to this case. Although the recommended sentence is below guidelines and provides the defendant with a lesser term of imprisonment than likely would be imposed after trial and conviction, under the agreement the defendant will be held accountable for her crime not only by admitting her guilt to the indictment but by her standing convicted of a serious federal felony that will preclude her from ever accessing our country's secrets again. The defendant will also be required to serve a term of incarceration that will deter others who are entrusted with our country's sensitive national security information and would consider compromising it. Accordingly, the sentence will promote respect for the law and afford adequate deterrence to similar criminal conduct in the future.

The negotiated sentencing agreement also confers significant benefits on the government. First, it avoids the expense, time, and risk associated with a jury trial and appeal, as well as additional lengthy pre-trial proceedings under the Classified Information Procedures Act. The

[8] Similarly, on June 3, 2017, the defendant admitted to the FBI that the Intelligence Report could be used to the injury of the United States and to the advantage of a foreign nation. PSR ¶ 17.

issues presented by trying a case that has classified information at its core are complex; and their final resolution, whether by this Court or on appeal, is uniquely difficult to predict. *See United States v. Kim*, 808 F. Supp. 2d 44, 55 (D.D.C. 2011) (observing that there has been a "dearth of prosecutions" under Section 793(d)[9] "most likely" because of the "difficulty in establishing such a violation, combined with the sensitive nature of classified information and the procedures that must be followed in using such information in trial"). An adverse determination concerning the handling of classified information at trial—whether by the trial court or on appeal—can severely hamper, if not end, a Section 793(e) prosecution, as has occurred in other cases involving unauthorized disclosures to the media.

Most important, the United States must balance the need for prosecution with the damage that further disclosure of classified information at trial might cause. As it has advised the Court and the defense through classified filings, the government assessed that proving the government's case at trial would require the government to declassify TOP SECRET//SCI information, including the Intelligence Report that the defendant disclosed. Based on the statute with which the defendant is charged and the Court's rulings in the case, the government would also have had to elicit testimony from subject matter experts as to why the information in the Intelligence Report is national defense information, and the potential harm that could occur from its disclosure. The Intelligence Community assessed that this further disclosure of the

[9] 18 U.S.C. § 793(e) "has exactly the same structure as § 793(d), except that it applies to those who have unauthorized, rather than lawful, possession of NDI" and does not require a demand for the return of the NDI. *United States v. Kiriakou*, 898 F. Supp. 2d 921, 923 n.2 (E.D. Va. 2012); *see also Kim*, 808 F. Supp. 2d at 52 n.2.

Intelligence Report and explaining its contents would compound the exceptionally grave harm to national security already caused by the defendant. While the government would have taken the necessary steps at trial to prove the offense had the defendant not agreed to plead guilty, the plea agreement affords the government a substantial benefit in protecting from disclosure information that is still classified. The undersigned have consulted with the FBI and members of the Intelligence Community affected by the defendant's unauthorized disclosure, and they have concurred in this judgment.

Finally, the agreed-upon sentence avoids unwarranted sentencing disparities. Notably, it is difficult to make comparisons to other cases involving unauthorized disclosures of classified information to the media because there have been few such cases prosecuted in federal courts and because of the above-described challenges in prosecuting cases involving classified information. Each of these cases presents a different tension between the prosecutorial and intelligence interests at stake. Further, when such cases are resolved through guilty pleas, many of the facts underlying those pleas remain classified. Thus, making comparisons between those cases and this one based on publicly available information is of little utility.

Nevertheless, the government advises the Court that despite the agreed-upon sentence being below the applicable guidelines range, it would be the longest sentence served by a federal defendant for an unauthorized disclosure to the media. *Cf., e.g., United States v. Sachtleben* (S.D. Ind. 1:13-cr-00200-WTL) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, in November 2013 to 43 months for disclosure to a reporter of national defense information classified at the SECRET level relating to a disrupted suicide bomb attack and the recovery by the United States of the bomb); *United States v. Kiriakou* (E.D. Va. 1:12-cr-00127-LMB)

(defendant sentenced, pursuant to an 11(c)(1)(C) plea, in January 2013 to 30 months for disclosing information to journalists identifying Covert Officer A & Officer B, one of whose association with the CIA had been classified for over two decades); *United States v. Sterling* (E.D. Va. 1:10-cr-00485-LMB) (defendant sentenced, following trial, in January 2015 to 42 months for providing classified information about a certain classified CIA program and a human asset to a reporter who published the information in a book); *United States v. Kim* (D.D.C. 1:10-cr-00225-CKK) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, in April 2014 to 13 months for providing to a reporter the contents of a TOP SECRET//SCI intelligence report containing information about the military capabilities and preparedness of North Korea); *United States v. Leibowitz* (D. Md. 8:09-cr-00632-AW) (defendant sentenced, pursuant to an 11(c)(1)(C) plea, in May 2010 to 20 months for providing to the host of an Internet blog five documents that were classified at the SECRET level and which contained classified information relating to the communication intelligence activities of the United States).

Because it appropriately satisfies the need for both punishment and deterrence in light of the nature and seriousness of the offense, the Court should accept the parties' sentencing agreement and sentence the defendant accordingly.

V. CONCLUSION

For the reasons stated above, the government respectfully requests that the Court accept the parties' sentencing agreement pursuant to Federal Rule of Criminal Procedure 11(c)(1)(C) and sentence the defendant accordingly.

Respectfully submitted,

BOBBY L. CHRISTINE
UNITED STATES ATTORNEY

//s// Jennifer G. Solari

Jennifer G. Solari
Assistant United States Attorney

//s// Julie Edelstein

Julie A. Edelstein
Deputy Chief
U. S. Department of Justice
National Security Division

//s// David C. Aaron

David C. Aaron
Trial Attorney
U. S. Department of Justice
National Security Division

CERTIFICATE OF SERVICE

This is to certify that I have on this day served all the parties in this case in accordance with the notice of electronic filing ("NEF") which was generated as a result of electronic filing in this Court.

This 14th day of August 2018.

BOBBY L. CHRISTINE
UNITED STATES ATTORNEY

//s// Julie A. Edelstein

Julie A. Edelstein
Deputy Chief

950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
(202) 233-2260