LINCOLN MEMORIAL UNIVERSITY
LAW REVIEW

VOLUME 5 FALL 2017 ISSUE 1

ACCOUNTABILITY FOR ACCESS TO CLASSIFIED INFORMATION: THE UNITED STATES CANNOT AFFORD TO IGNORE BREACHES OF CONFIDENCE

Larry W. Perkins [a1]

I. INTRODUCTION

Donald Trump and Hillary Clinton engaged in a war of words over a potential compromise of classified information via email servers during the 2016 presidential election. Hillary Clinton told CNN, "[i]t was a mistake for me to use personal

[a1] *This note was prepared by Dr. Larry W. Perkins in his personal capacity. The opinions expressed are the author's own and do not reflect the view of the United States Department of Energy or the United States Government.*

email. And I regret that."[1] Ms. Clinton then commented during the October 9, 2016, presidential debate that "it's just awfully good that someone with the temperament of Donald Trump is not in charge of the law of our country."[2] Donald Trump responded, "[b]ecause you'd be in jail."[3]

The 2016 presidential election in the United States brought the public release of classified information to the forefront of discussion worldwide. However, this is not the first time discussion as to the consequences for releasing classified information into the public realm has occurred. From members of Congress to journalists to military generals, there has been an ongoing discussion in the United States about how to ensure

---

[1] Elise Labott & M.J. Lee, *Clinton reiterates email use was a 'mistake' as State Dept. reopens probe,* CNN Politics, July 8, 2016, http://www.cnn.com/2016/07/07/politics/state-department-reopens-probe-into-clinton-emails/, (last visited March 25, 2017); Richard Pollock, *State Dept Can't Find Evidence Hillary Was Trained To Handle Classified Documents*, The Daily Caller, July 10, 2016, http://dailycaller.com/2016/07/10/exclusive-state-dept-cant-find-evidence-hillary-was-trained-to-handle-classified-documents/, (last visited March 25, 2017). (Secretary Clinton did not know '(C)' meant the information was classified)

[2] Aaron Blake, *Everything that was said at the second Donald Trump vs. Hillary Clinton debate, highlighted*, Wash. Post., October 9, 2016, https://www.washingtonpost.com/news/the-fix/wp/2016/10/09/everything-that-was-said-at-the-second-donald-trump-vs-hillary-clinton-debate-highlighted/?utm_term=.76c72fa0af9f, (last visited March 25, 2017).

[3] *Id*.

the protection of classified information and deter those with access from releasing that information intentionally or unintentionally. The distinction is frequently drawn between the intentional release and negligent release, but that distinction is not always sufficient to determine whether there should be consequences for the individual releasing the information. The following sections will discuss the numerous examples of how the law on the release of classified information has been applied previously and how that implementation was not always consistent. Ultimately, the United States needs a single clear law on classified information that is implemented consistently across the board. The level of punishment should be determined by the intent of the crime. However, those who negligently disclose classified information should also receive punishment; the fact that the classified information took a non-physical form should not equate to a get out of jail free card.

This paper will investigate the current law as it relates to the unlawful public release of classified information. Noting that the federal government has used multiple statutes to prosecute individuals that release classified information inappropriately, the vast majority of the prosecutions utilize the

Espionage Act, 18 U.S.C. Chapter 37 Sections 791-799[4]. The primary sections of this act that have been utilized are 18 U.S.C. §§ 793 and 794.[5] As such, Part II of this paper will focus on the required paperwork and training necessary to obtain a government security clearance, as well as the use of the Espionage Act, specifically 18 U.S.C. §§ 793 and 794,[6] and the common challenges to those provisions. This information will provide an understanding of the current law, what federal employees and contractors are told with respect to the access and release of classified information, and how that law is applied. This section includes a sampling of recent cases and instances where the current law has been applied to individuals and demonstrates the confusion and lack of consistency in the application and prosecution of disclosure violations. In Part III of this paper, the public's perception of classified information and what protection is given such information will be explored. Finally, in Part IV, I argue that the laws pertaining to the

[4] 18 U.S.C.A. §§ 791-799 (West, Westlaw current through P.L. 114-248).
[5] 18 U.S.C.A. § 793 (West, Westlaw current through P.L. 114-248); 18 U.S.C.A. § 794 (West, Westlaw current through P.L. 114-248).
[6] *Id.*

disclosure of classified information must be clarified and consistently implemented to effectively protect classified information. Specifically, (1) §§ 793 and 794[7] should be modified and simplified; (2) prosecutions should be emphasized for both high profile government officials and low-level staff; (3) training of employees and contractors with security clearances should be improved; and (4) the public should be better informed as to the reasons information is made classified and as to why government officials and contractors cannot comment on the information.

II. CURRENT LAW AND TRAINING

There are three types of classified information when it comes to national security interests: (1) Confidential, (2) Secret, and (3) Top Secret.[8] Confidential information is the lowest level of classified information and is defined as information that

---

[7] *Id.*

[8] Northrop Grumman, *Annual DoD Security Refresher Training*, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiWuKLWzovSAhUDQiYKHbxbB6IQFggaMAA&url=http%3A%2F%2Fwww.northropgrumman.com%2FAboutUs%2FDocuments%2FClearance%2Fannual_dod_refresher_ext.pdf&usg=AFQjCNEBGi0CXrycDXt5EQ8dpcsUZB1hlA&bvm=bv.146786187,d.eWE, (last visited March 25, 2017).

could cause damage to national security if released.[9] The next level of classified information, Secret, is defined as information that could cause grave damage to national security if released.[10] Finally, the highest level of classification, Top Secret, is defined as information that could cause exceptionally grave damage to national security if released.[11] A security clearance is required to access any of these three types of classified information.[12] An individual will know if a particular document is classified for a number of reasons including that the document must be labeled, the document must contain a specific coversheet, electronic transmittal of the document requires an approved secure communication system, and the document may only be viewed in approved areas (e.g., may not be taken home) unless approved by senior management.[13] There is other information that may not be released to the public but is not classified and does not require a security clearance to access (e.g., Official Use

[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *DoD Information Security Program: Protection of Classified Information,* DOD Manual Department of Defense Manual 5200.01, Volume 3, Change 2, March 19, 2013.

Only Information, Law Enforcement Sensitive Information).[14] This paper is focused on the classified information that requires a security clearance for access.

A. TRAINING

Training individuals with access to classified information is required but may be slightly different among federal agencies (e.g., the Department of Defense has specific security manuals and annual training documents[15]). Generally, an individual that is applying for a security clearance must complete a 127-page form that addresses past personal and professional life and experiences.[16] These individuals are also required to sign a nondisclosure agreement which states:

> I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency)

[14] DOD, *supra* note 8; Dept. of Homeland Security, *Safeguarding Sensitive But Unclassified (For Official use Only) Information*, MD Number 11042.1, Jan. 6, 2005.
[15] DOD, *supra* note 8; DOD, *supra* note 13.
[16] SF86-10, *Questionnaire For National Security Positions.*

> responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.[17]

In addition to the nondisclosure agreement, additional training regarding the handling of classified information is also required annually. The training reminds security clearance holders of their responsibilities and requirements for protecting classified information.[18] Unfortunately, the required annual training is frequently not completed.[19] For example, in 2009 only 20% of the cleared individuals at the State Department had completed the required training.[20] It was also reported that only

---

[17] SF312-13, *Classified Information Nondisclosure Agreement.*
[18] DOD, *supra* note 8.
[19] Catherine Herridge, *Fewer than one in five State Dept employees with security clearance completed classified info training*, FoxNews, Sept. 27, 2016, http://www.foxnews.com/politics/2016/09/27/fewer-than-one-in-five-state-dept-employees-with-security-clearance-completed-classified-info-training.html; *Compliance Follow-up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information*, AUD-SI-16-43, September 2016, (last visited March 25, 2017).
[20] *Id*.

twenty-percent of the cleared State Department employees had completed the training at least once since obtaining a clearance.[21] The Office of Inspector General was unable to identify the number of State Department contractors that had completed the training because the Bureau of Diplomatic Security could not provide a complete list of all current Department security-cleared contractors.[22]

B. CURRENT STATUTORY VIOLATIONS

The current statutes used to prosecute those who unlawfully disclose classified information include everything from theft of government information to espionage. However, the vast majority of the prosecutions fall under the Espionage Act as codified in 18 U.S.C. §§ 791-99.[23] The key sections of this law that address the release of classified information are 18 U.S.C. §§ 793 and 794, which restrict the gathering, transmitting or losing defense information.[24] The remaining sections of the Espionage Act are more focused and less useful

---

[21] *Id*.
[22] *Compliance Follow-up Review of the Department of State's Implementation of Executive Order 13526, Classified National Security Information*, AUD-SI-16-43, September 2016.
[23] 18 U.S.C.A. §§ 791-799.
[24] 18 U.S.C.A. § 793; 18 U.S.C.A. § 794.

for prosecutors. Specifically, § 791 has been repealed;[25] § 792 involves harboring persons;[26] § 795 involves photographing or sketching defense facilities;[27] § 796 involves using aircraft to photograph defense facilities;[28] § 797 involves publication and sale of photographs of defense facilities;[29] and § 798 involves communication and cyphers.[30] While each of these sections could be used in specific situations, the more widely used sections of §§ 793 and 794 focus on gathering and transmitting information that could harm the defense of the United States.[31] As such, the remainder of this paper will focus on challenges that have been made to §§ 793 and 794.[32] The following discussion provides a summary of the elements in each subsection of §§ 793 and 794.[33]

Section 793(a) applies to those individuals who obtain information with respect to the "national defense" with an

---

[25] 18 U.S.C.A. § 791 (West, Westlaw current through P.L. 114-327).
[26] 18 U.S.C.A. § 792 (West, Westlaw current through P.L. 114-327).
[27] 18 U.S.C.A. § 795 (West, Westlaw current through P.L. 114-248).
[28] 18 U.S.C.A. § 796 (West, Westlaw current through P.L. 114-248).
[29] 18 U.S.C.A. § 797 (West, Westlaw current through P.L. 114-248).
[30] 18 U.S.C.A. § 798 (West, Westlaw current through P.L. 114-248).
[31] 18 U.S.C.A. § 793; 18 U.S.C.A. § 794.
[32] *Id.*
[33] *Id.* (The full text of the §§ 793 and 794 are provided in Attachment 1 for reference.)

intent or reason to believe that the information is to be used to the injury of the U.S. or to the advantage of a foreign nation.[34] These individuals might not have a security clearance but trespass on a military base and take pictures of classified military weapons projects or steal classified military plans.[35]

Section 793(b) contains the same requirements and reason as § 793(a), but the individual might not have been successful in obtaining the classified material but merely attempts to copy it.[36]

Section 793(c) contains the same requirements as § 793(a) but applies to those individuals who are interested in receiving such classified information.[37] In addition, this subsection specifically requires that the defendant know or have reason to believe that the information was or will be obtained in violation of this statute.[38]

Section 793(d) applies to individuals with security clearance who are legally in possession or have access to the

---

[34] 18 U.S.C.A. § 793.
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*

information and willfully provide such information to individuals who do not have the requisite security clearance to view the material.[39] The classified information must be "relating to the national defense" and can include writings and code books.[40] The defendant must also have reason to believe that the information could be used to injure the United States or aid a foreign nation.[41] It is also a violation when a defendant has possession of the information and refuses to produce it when asked by U.S. officials.[42] This section was used for one of the charges against Edward Snowden.

Section 793(e) contains the same requirements as § 793(d); however, this subsection applies to those who find themselves unlawfully coming into contact with such material and then distributing it to other such individuals not authorized to receive the information.[43] For example, the media outlet with unlawful access passing the information on to the public.

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*

Section 793(f) also requires that the defendant have lawful possession of the information (e.g., document, code book, etc.) and that the information is "relating to the national defense."[44] However, this section applies to those individuals with a security clearance who are grossly negligent and allow such material to fall into the hands of those not cleared.[45] The gross negligent mens rea requirement in 18 U.S.C. § 793(f) includes the loss of classified information due to negligence (e.g., forgetting it).[46] Examples of a negligent disclosure are Secretary Clinton's email server or a secret service agent leaving a laptop with classified information in a car which is stolen. In addition, the defendant is also in violation of this subsection if he or she has knowledge of the event and fails to report it to his superior officer.[47]

Section 793 prescribes a punishment of a fine and imprisonment not more than ten years.[48] Under the U.S. federal sentencing guidelines, with no prior criminal history, the

---

[44] *Id.*
[45] *Id.*
[46] United States v. Gonzalez, 16 M.J. 428, 429-430 (1983).
[47] *Id.* (Section 793 (g) is the conspiracy provision while § 793 (h) addresses forfeiture of property under this statute).
[48] 18 U.S.C.A. § 793.

imprisonment for violation of this section varies depending on the details and the subsection violated as shown in the following table.[49]

Section	**Top Secret Information**	**Other Classified Information**
793 (a)	168-210 months	97-121 months
793 (b)	168-210 months	97-121 months
793 (c)	168-210 months	97-121 months
793 (d)	168-210 months or 87-108 months Depending on the details of the violation	97-121 months or 51-63 months Depending on the details of the violation
793 (e)	168-210 months or 87-108 months Depending on the details of the violation	97-121 months or 51-63 months Depending on the details of the violation
793 (f)	27-33 months	12-18 months
793 (g)	168-210 months or 87-108 months Depending on the details of the violation	97-121 months or 51-63 months Depending on the details of the violation
794	360 months – life	210-262 months

[49] United States Sentencing Commission, *Guidelines Manual*, §§2M3.2-2M3.4 (Nov. 2016).

Similar to § 793(a), § 794(a) applies to any individual (with or without a security clearance) that obtains material with respect to the "national defense" and passes on such material with the intent or a reason to believe that it is to be used to the injury of the U.S. or advantage of a foreign nation.[50] In addition to § 793(a) requirements, this subsection requires that that information be provided to, or an attempt was made to provide the information to a foreign country.[51] For example, it would be difficult to prosecute Secretary Clinton or General Petraeus under this section unless there was some proof that they intended or had reason to know the actions would result in delivery of classified information to a foreign nation and it would injure the U.S. or be an advantage to the foreign nation. The section sets out the penalties and when they may be applied.[52] Specifically, § 794 prescribes a punishment of death or imprisonment for any term of years up to life.[53] Under the

---

[50] 18 U.S.C.A. § 794.
[51] *Id.*
[52] *Id.* (§ 794 (b) addresses the release of information during a time of war. In addition, § 794 (c) addresses a conspiracy with respect to this statute while § 794 (d) addresses forfeiture of property under this statute).
[53] *Id.*

U.S. federal sentencing guidelines, with no prior criminal history, the imprisonment for violation of this section is 360 months to life for Top Secret classified information and between 210-262 months for other classified information.[54]

The Espionage Act has many nuances and specifics that are required to obtain a conviction under the statute. The result is a confusing set of laws that require significant interpretation by the courts. This confusion is what defendants have frequently challenged to avoid conviction under the Espionage Act. Some of the primary examples of these challenges are the focus of the following section.

C. CHALLENGE TO THE ESPIONAGE ACT

There is a fair amount of case history associated with 18 U.S.C. §§ 793-94 challenging various sections and arguing that phrases are void for vagueness, that various mens rea requirements are not clear or met, that the statute violates the free speech and self-incrimination rights of the U.S. Constitution and that the statute violates the Congressional

[54] United States Sentencing Commission, *Guidelines Manual*, §2M3.1 (Nov. 2016).

requirements associated with treason. [55] We address each of these challenges in the following discussion.

One of the primary challenges that has been made to §§ 793 and 794 has been with respect to the phrase "national defense." [56] Each subsection of § 793 and subsection (a) of § 794 use the phrase "national defense" when addressing the type of information that is covered by that specific subsection.[57]

The Supreme Court has defined the phrase "national defense."[58] Specifically, the Court held in *United States v. Abu-Jihaad* that "national defense" is not defined in the code but has been consistently interpreted by the courts to be a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[59] The Court then discussed limitations on the use of this phrase in a prosecution.[60] The Court indicated that the information must be "closely held."[61] This limitation was

---

[55] 18 U.S.C.A. § 793; 18 U.S.C.A. § 794.
[56] *Id.*
[57] *Id.*
[58] United States v. Abu-Jihaad, 600 F.Supp.2d 362, 385-88 (D. Conn. 2009).
[59] *Id*. at 385.
[60] *Id*. at 386-88.
[61] *Id*. at 386.

explained by the Court by noting that a conviction could not be maintained if the defendant collected the information from publicly available sources and pieced it together on his own.[62] The Court explained that if the Government did not keep the information secret, then use of the information was not a violation of the espionage laws.[63] This is distinguishable from the issues surrounding Edward Snowden because the government did protect that information but it was stolen by someone with a security clearance. Further, individuals with a security clearance are trained that they must have a need-to-know to view classified information; therefore, they are not allowed to view WikiLeaks information that may be classified and must not confirm or deny any information associated with those leaks.[64] The Court went further to explain that the statute does not strictly require the information be classified for a prosecution, but classification of the information is an important consideration in determining if the information falls under the statute.[65] The Court has also clarified that "national

[62] *Id*.
[63] *Id*.
[64] DOD, *supra* note 8.
[65] Abu-Jihaad, 600 F.Supp.2d at 387.

defense" is not restricted to military activities and facilities (e.g., a study of a worldwide communication satellite system by the Central Intelligence Agency).[66] In 2011, the Supreme Court rejected claims that "national defense" was too vague to allow implementation via the statute.[67]

Some defendants have also attempted to use the doctrine of *noscitur a sociis* ("words are generally known by the company they keep") to argue that "information relating to the national defense" is not clear as to whether it applies to tangible information, intangible information, or both. [68] However, the Supreme Court in *United States v. Kim* concluded that the statute provides an appropriate standard of conduct and is not vague.[69] In *United States v. Kiriakou*, the Court clarified that "information regarding the national defense" consists of tangible and intangible information in § 793(d).[70] Tangible information would include things such as books and documents while intangible information would be knowledge.[71] The difference

---

[66] United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir. 1979).
[67] United States v. Drake, 818 F.Supp.2d 909, 916-19 (D. Md.2011).
[68] United States v. Kim, 808 F.Supp.2d 44 (D.D.C.2011).
[69] *Id*. at 51-53.
[70] United States v. Kiriakou, 898 F.Supp.2d 921, 923 (E.D. Va. 2012).
[71] *Id*.

between the two in the statute depends on the mens rea in the subsection with intangible property requiring a "reason to believe could cause injury" or a bad faith requirement.[72]

Still, other phrases in the various statutes have also been challenged for vagueness. The military courts addressed the "unauthorized possession" language in § 793(e) and concluded that authorized possession turns into unauthorized possession when the individual exceeds the scope of the authorization that was provided to him.[73] The defense argued in *United States v. McGuinness* that because the defendant was authorized to access the information, he did not have "unauthorized possession."[74] 18 U.S.C § 793(f) has been challenged by indicating that the phrase in the statute that says the violator "permits" the information to be removed prohibits its application if the defendant removed the classified materials himself.[75] Thus, the defendant did not "permit" someone to access the information because he took it himself.[76] The military

[72] *Id.* at 923-24.
[73] United States v. McGuinness, 33 M.J. 781, 786 (1991); United States v. McGuinness, 35 M.J. 149, 152-53 (1992).
[74] McGuinness, 33 M.J. at 784; McGuinness, 35 M.J. at 152.
[75] United States v. Roller, 37 M.J. 1093 (1993).
[76] *Id.*

courts rejected this challenge and indicated that the defendant removing the information himself was still "permitting" the classified information to be removed as defined in the statute.[77] In 2011, the Supreme Court also rejected claims that "willfulness" was too vague to allow implementation via § 793(e).[78]

Another frequent challenge to convictions under §§ 793-794 centers around the mens rea and the mindset of the individual that was charged with violation of the statute.[79] This challenge has also been addressed by the courts. For example, the Supreme Court ruled that a conviction under § 793(d) requires proof that the defendant was legally in possession of the material, the material must be "associated with the national defense", and the defendant must have tried to provide that information to someone that was not authorized to have the material.[80] In 2009, the Supreme Court clarified that in addition to the defendant having lawful possession of the material, the material being related to "the national defense", and the

---

[77] *Id.*
[78] Drake, 818 F.Supp.2d at 916-19.
[79] 18 U.S.C.A. § 793; 18 U.S.C.A. § 794.
[80] Schmuck v. United States, 489 U.S. 705, 721-22 (1989).

material being provided to someone not authorized to receive it, § 793(d) also requires that the information be communicated willfully and the defendant must have a reason to believe the information could harm the United States or help a foreign government.[81] In 1971, the United States Court of Military Appeals indicated that § 793(d) required willfulness, but did not require bad faith was for a conviction under the statute.[82]

The military courts have also provided explanation and clarification on the mens rea required for the espionage laws. The courts explained the various levels of mens rea by explaining that 18 U.S.C. § 793(a) requires bad faith, whereas § 793(e) requires only willfulness and § 793(f) requires gross negligence.[83]

The Supreme Court also addressed the distinction between § 793(d) and § 794(a).[84] The Court held that § 793(d) only addresses those individuals who are trusted with the classified information and subsequently violated that trust.[85]

---

[81] United States v. Abu-Jihaad, 600 F.Supp.2d 362, 384, 388 (D. Conn. 2009).
[82] United States v. Attardi, 20 USCMA 548, 554 (1971).
[83] United States v. Diaz, 69 M.J. 127, 132-33 (2010).
[84] Hoffman, 995 F.Supp.2d at 565.
[85] *Id*.

The Court held that § 793(d) may be used to prosecute the individual for attempting to provide the information to anyone not entitled to receive it.[86] Conversely, according to § 794(a) it is irrelevant how the individual received the classified information; the fact that the person has the information and attempted to provide it to a foreign government is adequate for this element of the crime.[87] As such, § 794(a) is broader than § 793(d) as it relates to the details of the case (e.g., how the information was obtained) and therefore easier to prosecute.[88]

Prosecutors have also charged individuals when the recipient of the information was not a foreign government news. In 1985, defense attorneys argued that § 793(e) was not applicable when classified information is released to the press.[89] The Court concluded that the United States would be just as harmed by a release of information to the press as release to a single individual.[90]

---

[86] *Id*.
[87] *Id*.
[88] *Id*.
[89] United States v. Morison, 604 F.Supp. 655, 657-58 (D. Md.1985).
[90] *Id*. at 660, 662; United States v. Morison, 844 F.2d 1057, 1063-68 (4th Cir.1988).

Defense attorneys have also argued that the requirement to produce information when requested under § 793(e) was a violation of a defendant's Fifth Amendment rights because such production required the defendant to incriminate himself by admitting he had possession of the information.[91] However, the Court concluded that this claim was not material as there is no provision in the statute to punish an individual that has possession of classified information but returns that information when requested by the government (i.e., one element of the crime is to willfully retain or fail to return the classified information).[92] As such, the military courts and the Supreme Court both concluded that requiring the return of classified information does not violate a defendant's Fifth Amendment rights.[93]

Defendants have also challenged the Espionage Act by claiming that it violates the Treason Clause of the U.S. Constitution because the activities in the Espionage Act are not

[91] Morison, 604 F.Supp. at 657-58.
[92] *Id*. at 660-62; Morison, 844 F.2d at 1063-68.
[93] Morison, 604 F.Supp. at 657-58; United States v. Oxfort, 44 M.J. 337, 338-43 (1996).

specifically defined in the Constitution.[94] However, the Supreme Court concluded that Congress has the authority to specify other conduct that is not equivalent to treason but still punishable under the espionage laws.[95] Similarly, the Court rejected a claim that the government was not consistent in what they prosecute under the statute and therefore it was impossible for the defendant to know what was illegal.[96] The Court explained that this argument does not hold any water for a number of reasons including the government's difficulty of meeting the elements of the conviction and the complications of having a trial with classified information.[97] In the same case, the Court rejected a claim that oral communication of classified information was protected as free speech under the First Amendment to the Constitution.[98]

In *United States v. Rosen*, one of the most well-known cases on espionage, the defendants argued § 793 violated the First and Fifth Amendments to the United States Constitution,

---

[94] Kim, 808 F.Supp.2d. 44.
[95] *Id.* at 50.
[96] *Id.* at 55.
[97] *Id*.
[98] *Id*.

however, these challenges were rejected by the Court.[99] The Court noted that this was not a blanket exemption from a First Amendment challenge but must be considered on a case by case basis.[100] Specifically, the Court held that individuals that work for or with the government frequently have a contractual arrangement of some type and could be prosecuted without violating the First Amendment, but individuals not associated with the government could only be prosecuted if the release of information was directly related to national security.[101] The Court also clarified that release of classified information implies the government has indicated it is accurate and could still result in a conviction under § 793, even if the information was already available to the public.[102] The Court in *Rosen* rejected a claim that the information was received orally and therefore could not be confirmed to be classified when released.[103] The Court also rejected a claim that the defendants did not receive fair warning of how the statute would be applied.[104]

D. EXAMPLES OF APPLICATION OF CURRENT LAW

[99] United States v. Rosen, 445 F.Supp.2d 602, 607 (E.D. Va. 2006).
[100] *Id*. at 632.
[101] *Id*. at 635-39.
[102] *Id*. at 620.
[103] *Id*. at 623.
[104] *Id*. at 627-28.

As noted by the Supreme Court, prosecutions under § 793 are not frequent, presumably due to the tight restrictions placed on successful prosecution within the language of the statute itself.[105] However, there have been some recent examples of prosecutions using § 793. For example, in *United States v. Hitselberger*, the defendant was charged under § 793(e) for removing and retaining documents associated with national defense, among other charges beyond the Espionage Act such as removing public documents from a secure location.[106] The defendant made a conscious effort to hide the classified material and sneak it out undetected.[107] In another case, a retired Navy radioman was court-martialed and sentenced to eight years in prison for conducting espionage for the government of the Philippines when he collected and stole classified communication information in violation of § 793(d).[108] Theresa Marie Squillacote was convicted of espionage,

---

[105] *Id.* at 613.
[106] United States v. Hitselberger, 991 F.Supp.2d 130, 133 (D.D.C. 2014); United States v. Hitselberger, 991 F.Supp.2d 101, 102 (D.D.C. 2013).
[107] Hitselberger, 991 F.Supp.2d at 134.
[108] Allen v. United States, 46 Fed.Cl. 677, 678 (2000); United States v. Allen, 31 M.J. 572 (1990).

including § 793(b) and § 794(a), on behalf of Germany and sentenced to just under 22 years imprisonment when she copied and attempted to transmit classified documents to various foreign governments.[109] Abu-Jihaad was convicted of espionage under statutes including § 793(d) and sentenced to ten years imprisonment for transferring classified information to Azzam Publications in support of jihad.[110] There were also some other cases prior to 2000 where defendants were convicted under § 793 subsections (a)-(g) and § 794 subsections (a)-(b).[111] The one common theme in these cases is that each defendant was making an intentional, conscious effort to collect and steal the classified information.

III. PUBLIC PERCEPTION

[109] *In re* Squillacote, 790 A.2d 514, 514, 516 (D.C. Cir. 2002).
[110] Abu-Jihaad, 630 F.3d 362.
[111] McLucas v. DeChamplain, 421 U.S. 21 (1975); Truong Dinh Hung v. United States, 439 U.S. 1326 (1978); Morison v. United States, 486 U.S. 1306 (1988); United States v. Rosenberg, 195 F.2d 583 (2d Cir.1952); United States v. Abel, 258 F.2d 485 (2d Cir.1958); Boeckenhaupt v. United States, 392 F.2d 24 (4th Cir.1968); Boeckenhaupt v. United States, 537 F.2d 1182 (4th Cir.1976); United States v. Pelton, 835 F.2d 1067 (4th Cir.1987); United States v. Pollard, 959 F.2d 1011 (D.C. Cir.1992); United States v. Kampiles, 609 F.2d 1233 (7th Cir.1979); United States v. Boyce, 594 F.2d 1246 (9th Cir.1979); United States v. Lee, 589 F.2d 980 (9th Cir.1979); United States v. Miller, 984 F.2d 1028 (9th Cir.1993); United States v. Forbrich, 758 F.2d 555 (11th Cir.1985); Coplon v. United States, 191 F.2d 749 (D.C. Cir.1951); Scarbeck v. United States, 317 F.2d 546 (D.C. Cir.1962);United States v. Kostadinov, 572 F.Supp. 1547 (S.D.N.Y.1983); United States v. Lee, 79 F.Supp.2d 1280 (D.N.M.1999).

The public is not trained or knowledgeable of the requirements associated with classified information and how it must be protected. As a result, the public gets most, if not all, of their information and knowledge from the media and news articles. Unfortunately, the news media is also uninformed and lacks the knowledge to inform the public as to the requirements associated with classified information. For example, the media reported extensively on some high-profile cases such as Edward Snowden. A vast majority of the discussion and articles that have been published by the media about Snowden have focused on whether Snowden is a hero or a villain.[112] The same type of discussion of Secretary Clinton's emails has been raging in the media as demonstrated during the 2016 Presidential election. So, how does the information provided in the media

---

[112] Nate Fick, *Was Snowden hero or traitor? Perhaps a little of both*, Wash. Post, January 19, 2017, https://www.washingtonpost.com/opinions/was-snowden-hero-or-traitor-perhaps-a-little-of-both/2017/01/19/a2b8592e-c6f0-11e6-bf4b-2c064d32a4bf_story.html?utm_term=.1d3c2b2b0235, (last visited March 25, 2017); Amnesty International, *Edward Snowden is a hero not a traitor*, https://www.amnesty.org/en/get-involved/take-action/edward-snowden-hero-not-traitor/, (last visited March 25, 2017); John Cassidy, *Why Edward Snowden is a Hero*, The New Yorker, June 10, 2013, http://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero, (last visited March 25, 2017).

relate to the information available from the actual government agencies responsible for protecting classified information?

The Brennan Center for Justice at New York University School of Law published an article about the lack of protection for whistleblowers as it relates to national security.[113] This article stated, "existing legal protections for whistleblowers are limited and generally do not extend to leaks of classified information."[114] The article also stated that recent orders that are intended to address this issue are not adequate and that no disclosure is protected from criminal prosecution.[115] In reality, this article is incredibly misleading. While it is true that simply releasing classified information is not allowed, it is not true that whistleblowers are unprotected if classified information is involved. The Intelligence Community Whistleblower Protection Act (ICWPA) of 1998 discussed how to use secure methods to report issues associated with classified information

---

[113] *National Security Whistleblowing: A Gap in the Law*, Brennan Center for Justice, Aug. 21, 2013, https://www.brennancenter.org/analysis/national-security-whistleblowing-gap-law, (last visited March 25, 2017).
[114] *Id*.
[115] *Id*.

to Congress.[116] When appropriate concerns are reported through this manner, the whistleblower is protected.[117] This was emphasized in a 2007 report for Congress on the Whistleblower Protection Act (WPA) which stated:

> The WPA protects 'any' disclosure evidencing a reasonable belief of specified misconduct, a cornerstone to which the MSPB [Merit Systems Protection Board] remains blind. The only restrictions are for classified information or material the release of which is specifically prohibited by statute. Employees must disclose that type of information through confidential channels to maintain protection; otherwise there are no exceptions.[118]

As noted by reports for Congress and the Inspector General, protection is provided for whistleblowers using classified information, but they must follow a specified procedure to ensure proper protection of that classified information.[119] The Brennan Center report that is available to the public is inaccurate with respect to whistleblowers and

---

[116] *Intelligence Community Whistleblower Protection Act (ICWPA)*, http://www.dodig.mil/programs/whistleblower/icwpa.html, (last visited March 25, 2017).
[117] *Id.*
[118] L. Paige Whitaker, *The Whistleblower Protection Act: An Overview* (Cong. Research Serv., CRS Report for Congress Order Code RL 33918, March 12, 2007).
[119] *Id.;* ICWPA, *supra* note 118.

classified information and misleads the public on the topic.[120] This inaccuracy is also proven false by reviewing the federal training on whistleblowers.[121] The training specifically states that classified information may be released in a whistleblower action, but it must be in a proper manner and location.[122] For example, if Edward Snowden had developed concerns with how the National Security Agency was using metadata, he could have sent the information via specified secure means to the Inspector General or called a Defense hotline for further instructions on how to communicate the concern.

The Washington Post also ran an opinion article about the myths associated with classified information.[123] In this

---

[120] Brennan, *supra* note 115.
[121] Office of the Dir. of Nat'l Intelligence, *Unauthorized Disclosures of Classified Information Text Alternative*, The Nat'l Counterintelligence and Sec. Ctr., Sept. 2011, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiV-d2s0ovSAhVQ3yYKHVhvBZYQFggcMAE&url=https%3A%2F%2Fwww.ncsc.gov%2Ftraining%2FWBT%2Fdocs%2FUDB_091211.pdf&usg=AFQjCNGb0e2d1m1Q-i36NWFPCxe6w-5rgg&bvm=bv.146786187,d.eWE, (last visited March 25, 2017).
[122] *Id*.
[123] Elizabeth Goitein, *Myths on Classified Information*, Wash. Post., Sept. 18, 2015, https://www.washingtonpost.com/opinions/five-myths-about-classified-information/2015/09/18/a164c1a4-5d72-11e5-b38e-06883aacba64_story.html?utm_term=.bc4c41e9cd65, (last visited March 25, 2017).

article, the Washington Post claims that even if an official decides that disclosure would be harmful if released, he or she is not required to make the information classified.[124] To the contrary, it is impossible for an uncleared news reporter to determine what information is improperly classified. Nor does the article offer any evidence or reference to support this false claim. Rather the Department of Defense manual discusses required training for those who make classification decisions.[125] The training emphasizes avoiding over-classification.[126] In other words, the individuals must classify information based on content and not on whether the information would be harmful.

The Washington Post then states that derivative classification can be performed by any individual that can access the information.[127] This demonstrates a lack of understanding of classification. In reality, there are two types of classification, original classification and derivative classification.[128] Original classification is the determination as to

---

[124] *Id*.
[125] DOD, *supra* note 13.
[126] *Id*.
[127] Goitein, *supra* note 125.
[128] DOD, *supra* note 8.

whether information should be classified or not.[129] The original classification authority is only available to persons who have a "unique mission with responsibility in one of the subject areas prescribed."[130] These individuals are specifically designated and do not include all employees.[131] Derivative classification occurs when information is derived from other classified information.[132] This results in the new document being classified, but that derivative classifier (i.e., the person generating the document with the derivative information) is not determining whether the original information should or should not be classified.[133] Similarly, the Department of Defense indicates that derivative classifiers must be properly trained and an individual not trained may not serve as a derivative classifier.[134]

The Washington Post article goes on to indicate that there is no protection for whistleblowers.[135] As discussed

[129] *Id.*
[130] DOD, *supra* note 13.
[131] DOD, *supra* note 8.
[132] *Id.*; DOD, *supra* note 13.
[133] *Id.*
[134] *Id.*
[135] Goitein, *supra* note 125.

previously, there are many ways that whistleblowers are protected when it comes to classified information, but there is a requirement to follow a specific process.[136]

The Washington Post article also indicates that our classification system does not protect individuals from harm and proposes an easy fix is that declassification should be automatic after a set period of time.[137] These claims are made based on assumptions that are not substantiated in any way. President Eisenhower once stated "[I]t is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosures of classified information relating to the national defense . . . ."[138] Current world events more than destroy the claim for automatic declassification. The United States built a nuclear weapon during World War II. Countries today, such as North Korea or Iran, would be happy to get any information used during that effort, even if the technology is old and inefficient. Automatic

---

[136] L. Paige Whitaker, *The Whistleblower Protection Act: An Overview* (Cong. Research Serv., CRS Report for Congress Order Code RL 33918, March 12, 2007); ICWPA, *supra* note 118.
[137] Goitein, *supra* note 126.
[138] Hutson v. Analytic Sciences Corp., 860 F.Supp. 6, 12 (D. Mass.1994).

declassification would essentially put military technology and nuclear weapons in the hands of every country around the globe. These claims by the Washington Post associated with classified information serve to further mislead and confuse the public at large.

One cannot describe the public's understanding of classified information without discussing Secretary of State Hillary Clinton's emails. Numerous news articles implied that these activities were prevalent throughout the government. For example, reports indicated that Secretary Clinton was not trained on proper handling of classified materials.[139] The implication, whether intentional or not, is that if the Secretary of State does not get training, then it is likely most individuals with access to classified information are not trained. While reports indicate that a large percentage of employees were not trained in the State Department,[140] there is no information that this is prevalent among other federal agencies that handle

[139] Richard Pollock, *State Dept Can't Find Evidence Hillary Was Trained To Handle Classified Documents*, The Daily Caller, July 10, 2016, http://dailycaller.com/2016/07/10/exclusive-state-dept-cant-find-evidence-hillary-was-trained-to-handle-classified-documents/, (last visited March 25, 2017).
[140] Herridge, *supra* note 19.

classified information. Other high-profile cases in the recent past have led the public to believe that classified information is not protected adequately and perhaps does not need to be. Specifically, General David Petraeus admitted to allowing unauthorized individual access to classified information.[141] General Petraeus plead guilty to a misdemeanor charge of mishandling classified information resulting in a fine and two years of probation but no jail time.[142]

What these articles do not report is that great lengths are taken to protect our nation's secrets. For example, the Court has protected classified information during hearings and trials indicating that the information may be protected from public release if it is a matter of national security, but methods should be used to ensure the protection does not affect the defendant's

---

[141] Jessica McBride, *David Petraeus: Why He Was Charged & Hillary Clinton Wasn't*, Heavy, July 6, 2016, http://heavy.com/news/2016/07/david-petraeus-hillary-clinton-james-comey-press-statement-classified-information-scandal-no-charges-charged-criminal-charges-emails-paula-broadwell-affair-donald-trump-reaction/; Adam Thorp, *Was there a double standard on the investigations of David Petraeus and Hillary Clinton?*, PolitiFact, July 7, 2016, http://www.politifact.com/truth-o-meter/article/2016/jul/07/trump-revives-accusation-double-standard-between-c/, (last visited March 25, 2017).

[142] *Id.*

right to a fair trial.[143] This disconnect is exacerbated by the fact that individuals with access to classified information are trained to neither confirm, deny, nor comment on any information that may be available to the public.[144]

IV. NEED FOR MODIFICATIONS TO THE CURRENT LAW

Given the current state of the law and the application of that law, there are many changes that are warranted to ensure the safety and security of our national secrets. This section proposes four changes to the law and how these changes can be applied to advance national security interests. These changes include: (1) revisions and clarification of the Espionage Act, (2) consistent prosecutions, (3) improved training, and (4) better explanations to the public at large.

A. CHANGES NEEDED TO THE ESPIONAGE ACT

First, it is evident from the case law that there has been much confusion about the application of §§ 793 and 794. As with any law, defendants and defense attorneys consistently try to find ways to avoid conviction under the law. A frequent

---

[143] United States v. Sterling, 724 F.3d 482, 515 (4th Cir.2013); 18 U.S.C.A. § APP. 3 §§ 4 and 6 (West, Westlaw current through P.L. 114-327. Also includes P.L. 114-329 and 115-1 to 115-18. Title 26 current through 115-18.).

[144] DOD, *supra* note 8.

challenge that has been applied in defense arguments has been that the statute is unconstitutionally vague, particularly as it relates to the phrase "national defense." While the courts have made an effort to broadly define national defense in this context, it is still very limiting with respect to classified information. If there is not a direct link between the acts of the defendant and national defense, then §§ 793-794 cannot be applied.[145] It would be easy to visualize material that the government could consider classified but that is not directly related to national defense or related activities as defined by the courts (e.g., commercial nuclear reactors, Foreign Intelligence Surveillance Act warrants).[146] There is a heavy responsibility that should go along with having a security clearance. This responsibility should not depend on whether the classified information accessed is related to national defense or is simply considered classified for other reasons. For example, commercial nuclear reactors would certainly have the potential to involve classified information. However, if the reactor is only

[145] 18 U.S.C.A. § 793; 18 U.S.C.A. § 794.
[146] 50 U.S.C.A § 1801 *et seq.* (West, Westlaw current through P.L. 114-327. Also includes P.L. 114-329 and 115-1 to 115-18. Title 26 current through 115-18.).

associated with generation of electricity for public consumption, it would likely be difficult to justify the national defense element of this statute. This type of information could certainly be a concern for the security of the American people if it were to fall into the hands of a rogue nation or terrorist organization. The restriction to tie the release of classified information to national defense is needlessly narrow. The term "national defense" should be stricken from the statue and in its place state that anything designated classified (e.g., Top Secret, Secret, or Confidential) is protected by the statute. Classified information has been classified for a reason, and this material must be protected for any number of reasons that may or may not be related to national defense. If there is a true need to protect national defense information that is not classified, then that should be addressed in a separate statute as it is best to clarify the statute and keep it simple and concise. Unfortunately, the existing statute has resulted in confusion by trying to provide detail in the "national defense" language.

Along those same lines, parts of the statute require a "reason to believe" that the information would injure the United States and willful or grossly negligent behavior to be

applicable. However, the responsibility that goes with having access to classified information should be much more simply defined. The statute should simply criminalize the willful release of classified information regardless of what the individual believed would happen with the information. The fact that the information is classified should be sufficient to put the individual on notice that it could injure the United States if released. The mens rea should be the intent to release that information.

Similarly, negligent treatment of classified material should continue to be treated as a crime. The mens rea would come from the knowledge that the information is classified so that reckless handling of the information results in the mens rea of not protecting classified information. The approach of the current statute that willful release incurs a more severe punishment than negligent release should be maintained. The recent issues surrounding Secretary Clinton and General Petraeus illustrate this point. There is no argument that Secretary Clinton intended to release classified information and harm the United States with her email server. However, the fact that other entities could have accessed that information does

not lessen the impact. If U.S. spies were identified through those emails and subsequently found by foreign governments, the argument that Secretary Clinton did not intend to harm the U.S. or those individuals does not change the fact that the harm occurred. As such, if Secretary Clinton knew the information was classified and did not protect it accordingly, then she would fall under the negligent release of classified information in this approach. Similarly, General Petraeus admitted to knowing the information he released was classified and intentionally released it anyway. He would fall under the intentional release of classified information in this approach.

Similarly, the current statute draws a distinction between physical information (e.g., books) and intangible knowledge. This adds confusion and should be removed. Regardless of whether the classified information is tangible or intangible, there is a serious potential to harm the security interests of the United States.

Finally, the sources and methods used for protection of classified information must also be protected. This type of protection should be clearer in the statute to emphasize the importance and lack of distinction between the methods and

the final information. One only need look at the damage done by Edward Snowden to understand that the methods of collecting classified information can be just as important as the information itself. The statute should specify that discussion of the methods and sources of classified information is also punishable under the statute. By making these changes in the statute, there will be a great deal of clarity and consolidation that will occur.

B. MORE CONSISTENT PROSECUTIONS

While the changes proposed will add clarity and allow easier prosecution for releasing unlawfully classified information, the key to the protection of the sensitive information is to punish violators of the statute. As noted in the referenced cases, the majority of §§ 793 and 794 prosecutions have been of government employees and contractors where the defendant made a conscious effort to steal information and provide that information to a foreign government or news outlet, knowing that the information is classified and protected by the government. However, when the defendant is a high profile or famous individual, suddenly the rules do not seem to

apply. The two prime examples are former Secretary of State Clinton and General Petraeus.

In the case of Secretary Clinton, there was no desire to go through the headaches of prosecuting her for failing to protect classified information in violation of § 793(f). At present, there has been no consequence at all for Secretary Clinton with respect to failing to follow the appropriate requirements for classified information. This failure may have resulted in the release of classified information. Similarly, General Petraeus was prosecuted but avoided any type of significant penalty by pleading guilty to a lesser offense. The lack of any true consequence for release of classified information by Clinton and Petraeus shows the staff-level employees and public that there really is no downside to trying to make money based upon access to classified information and/or bypass security protocols. This type of publicity serves to demoralize the government work force and make individuals with a security clearance ask themselves why they need to be diligent in protecting classified information. If senior military and political officials routinely skirt or intentionally violate the rules and there is no punishment, what is the point? In addition to the

need for a revised and clarified law on release of classified information, there needs to be a renewed and focused effort to prosecute violators of that law. These prosecutions must start at the top and work their way down to the staff level. A serious effort to enforce the rules will put everyone on notice, including political officials, that the security of our nation is paramount and will not be compromised at any level by anyone. The result will be an effort to emphasize proper handling of classified material and a much safer and secure country. Letting individuals off with no real penalty simply encourages and emboldens the next person to do the same thing, whether for monetary or political gain.

C. IMPROVED TRAINING TO ACCESS CLASSIFIED INFORMATION

Not only must there be changes made to the Espionage Act, but improvements must be made to the training of those who hold security clearances. As noted previously, there are multiple examples where training for handling of classified information is not consistently implemented. The real problem with the training falls into two areas. First, there is no real consequence for failing to complete classified material training.

The former Secretary of State did not complete the training and was allowed to run for President of the United States. In theory, failing to complete the training can result in revocation of the individual's security clearance, and thus restriction from access of classified material; however, in practice, this is not implemented. How many of the 80% of employees at the State Department who failed to complete the training lost their security clearance?[147] The articles and reports of this number do not reference anyone losing their clearance. Congress needs to mandate that the agencies and departments have a hard date each year for completion of classified material training. If this date is exceeded, the individual should immediately lose their security clearance. There are obvious needs for extenuating circumstances to reinstate the clearance, but these should be the exception and not the norm. If everyone fully understands what will happen if you fail to complete the training, then there will be very few who test the limits of that requirement. The second issue is that most classified material training is only available online. Most online training is more of a nuisance than an opportunity to learn or refresh knowledge. Individuals will

[147] Herridge, *supra* note 19.

frequently page through the online slides without reading any of them. In addition, exams that are provided online are also less than effective. Individuals are free to look up answers prior to answering. It is noted that references can frequently be used in real life, but a simple yes/no question that can be answered with a search function in the electronic file does not really test knowledge. There should be a requirement for periodic classroom training for access to classified information. This may not be feasible every year due to financial and resource restrictions, but periodic (e.g., every 2 or 3 years) classroom training is critical to ensure individuals maintain the level of knowledge necessary to protect the national secrets of the United States.

D. BETTER PUBLIC KNOWLEDGE AND UNDERSTANDING WITH RESPECT TO CLASSIFIED INFORMATION

Finally, the public is not informed as to how the government tries to protect national secrets and national security. For example, when asked about whether unlawfully disclosed information is true, an individual in an official position or with appropriate security clearance can neither

confirm nor deny.[148] This is completely appropriate to protect information. Denying something is classified in one instance will inadvertently admit something else is classified when denial is not provided. However, the public needs to be made aware that cleared individuals are not allowed to comment so that national secrets are protected. The government needs some type of media campaign to inform the public as to why these national secrets must be protected and that there cannot be any comment on the information. The biggest thing to explain to the public is that the information being protected cannot be disclosed due to national security. Some in the public believe classification is used to simply hide information from the public (i.e., the government is keeping something secret because it is doing something illegal or disliked). In reality, the information is protected to prevent damage to the safety and security of the United States. The government must undergo some type of media campaign to assure the public that the classification of material is for a good reason. Once the public is convinced, they

[148] DOD, *supra* note 8.

will not only support but will require that violators of the law be punished.

V. CONCLUSIONS

Consolidating the convoluted espionage laws into one statute will certainly make it easier for prosecutors to determine the applicable law when prosecuting a case. As currently written, the statute provides many potential ambiguities that are frequently challenged in court. While consolidation and clarification will assist in the prosecution for release of classified information, the key is to enforce the law consistently across the board. It should not matter who the individual is, they should be subject to the same consequences. Until the law is consistently enforced and applied to everyone, from politicians and military generals to lower level federal employees and contractors, there will never be a consistent understanding of what constitutes a violation of law when classified information is made available to the public. All individuals with access to classified information should be able to read and easily understand the law, be properly trained on the application of the law, and be subject to severe consequences for violating the law. This type of application will need to be applied from the

top down, including Congressmen, politicians, and high-ranking officials. Classified information is the key to the success and security of the United States. It must continue to be treated seriously with violations and unauthorized releases receiving consistent punishment at all levels. Individuals that have access to such information must be trained properly and effectively to ensure they know what they can or cannot do. A key to this implementation is convincing the public that the classified information protection is critical to the safety and security of our nation. These recommendations will serve to strengthen our security and enhance the safety of the citizens of the United States.

Appendix A

18 U.S.C.A. § 793 (West, Westlaw current through P.L. 114-248).

§ 793. Gathering, transmitting or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from

any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan,

map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined under this title or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

(h)(1) Any person convicted of a violation of this section shall forfeit to the United States, irrespective of any provision of State law, any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, from any foreign government, or any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, as the result of such violation. For the purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

(3) The provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)-(p)) shall apply to--

(A) property subject to forfeiture under this subsection;

(B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

Appendix A

18 U.S.C.A. § 794 (West, Westlaw current through P.L. 114-248).

§ 794. Gathering or delivering defense information to aid foreign government

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or, if there is no jury, the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against largescale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information

relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

(d)(1) Any person convicted of a violation of this section shall forfeit to the United States irrespective of any provision of State law.

(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation, and

(B) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

For the purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

(3) The provisions of subsections (b), (c) and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)-(p)) shall apply to--

(A) property subject to forfeiture under this subsection;

(B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.