IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA **v.** **JACKSON COSKO,** ***Defendant.***	**Case No. 18-CR-303** **Honorable Thomas F. Hogan**

GOVERNMENT'S SENTENCING MEMORANDUM

The United States, by and through its attorney, the United States Attorney for the District of Columbia, respectfully submits the following Sentencing Memorandum. The United States submits that the defendant deliberately and maliciously committed serious crimes directed at United States Senators and the Senate; that the defendant's crimes imposed significant harm on individual Senators, their families, staff, and the Senate; and that his crimes call out for a significant sentence. In that context, and in view of the totality of the circumstances, the government submits that the defendant should be sentenced to the high end of the range recommended by the U.S. Sentencing Guidelines ("U.S.S.G."), that is to say, 57 months in prison.

INTRODUCTION

The defendant has pleaded guilty to carrying out a months-long series of burglaries and sophisticated data theft offenses directed at the office of United States Senator Maggie Hassan; to a separate set of "doxxing" offenses[1] through which he maliciously released personal information of Senators Lindsay Graham, Orrin Hatch, Mike Lee, Rand Paul, and Mitch McConnell; and to obstruction of justice, because he attempted to silence a witness by threatening to release the

[1] "Doxxing" is the act of publishing private or identifying information about an individual on the Internet, typically with malicious intent. As used in in this Memorandum, it refers to violations of 18 U.S.C. § 119 (Making Public Restricted Personal Information).

private health information of a Senator's children, because he corrupted another person and persuaded her to attempt to "wipe down" the scene of his burglaries, and because he attempted to destroy evidence in his own apartment. The defendant ultimately pleaded guilty to five felony counts.

The defendant's crimes spanned several months and reflected a deliberate malice and self-righteous entitlement that distinguishes his offense conduct from purely impulsive, one-time mistakes, and from offenses driven solely by intoxication or addition. For months, the defendant engaged in the data-theft campaign targeting Senator Hassan's office. Moreover, after a weekend of mulling over the response (and the harm) caused by his doxxing Senators Lindsay Graham, Orrin Hatch, Mike Lee, the defendant essentially decided that his targets deserved it, that he should target Senators Paul and McConnell, and that he should commit additional doxxing offenses, even writing an (undated) note to himself, suggesting a "contest of who to dox next[.]"

The defendant's burglary and computer hacking campaign imposed significant harm on the office of Senator Hassan and on the United States Senate as an institution – it represented the single largest known theft of electronic data from the Senate; upon discovery of the defendant's last burglary, one Senate computer was immediately removed from service; and after it was discovered that the defendant had placed secret keylogger devices on several other computers, another twelve Senate computers had to be quarantined, examined, and replaced. The defendant's doxxing offenses imposed similarly significant harms, not only by causing substantial fear and distress among the family members of the targeted Senators, but also by requiring the U.S. Capitol Police, as well as local police agencies, to conduct directed uniformed patrols of the residences of affected Senators.

The defendant's doxxing conduct also prompted unidentified third parties to direct retaliatory abuse and racial harassment at another staffer in the House of Representatives – someone who was entirely innocent, but because the defendant used a shared IP address to conduct his doxxing, and because he hid his true identity (leading to speculation about the identity of the perpetrator), third parties wrongly blamed the other staffer for the defendant's conduct. They then subjected her to voluminous online harassment, causing her to temporarily leave her house for safety reasons – the very same type of harm that the defendant inflicted on his own targets.

As set forth below, the government respectfully submits that, in light of the determined, prolonged, and considered nature of the defendant's conduct, the harm imposed by his crimes, and the fact that, under his plea agreement, he has received substantial benefit (that is, the government not pursuing three additional doxxing counts under 18 U.S.C. § 119 and at least one count of aggravated identity theft under 18 U.S.C. § 1028A), the defendant should be sentenced to the high end of the already-reduced range under the applicable Guidelines, that is to say, that he should be sentenced to 57 months in prison.

FACTUAL BACKGROUND

On April 5, 2019, the defendant accepted responsibility and pled guilty to two counts of Making Public Restricted Personal Information, in violation of 18 U.S.C. § 119, one count of Computer Fraud, in violation of 18 U.S.C. § 1030(a)(2), one count of Witness Tampering, in violation of 18 U.S. C. § 1512(b)(3), and one count of Obstruction of Justice, in violation of 18 U.S.C. § 1512(b)(2)(B). In exchange for the defendant's guilty plea, the government agreed to dismiss the existing indictment and agreed not to charge the defendant with any further crimes, including additional counts under 18 U.S.C. § 119 and 18 U.S.C. § 1028A.

The Defendant's Senate Employment and Termination

Beginning in 2017, the defendant served as a staffer and computer systems administrator in the Office of Senator Hassan. As a system administrator, the defendant had an intimate knowledge of, and broad access to, computer systems, administrative accounts, and related security practices and measures (including passwords and usernames). The defendant was, in essence, entrusted with access to all of the computer systems and data in the Senator's office.

The defendant was terminated for performance-related reasons in May 2018. The defendant believed that his termination was unjust; he was indignant about having been forced to leave the job; and he continued to be angry about his termination for months. Driven by that anger, as well as concern about his prospects for future employment, the defendant took advantage of his in-depth knowledge of the office's computer security measures and practices, engaged in an extensive computer fraud and data theft scheme that he carried out by repeatedly burglarizing Senator Hassan's Office. The defendant ultimately copied entire network drives, sorted and organized sensitive data, and explored ways to use that data to his benefit.

Burglary & Data Theft

The defendant broke into Senator Hassan's Office on at least four occasions, including on or about July 26, 2018, August 6, 2018, and October 2, 2018. The defendant gained access to Senator Hassan's Office by unlawfully obtaining keys from SUBJECT A, a staffer who was (at the time) employed in the Office. The defendant had a prior close relationship with SUBJECT A, and the defendant continued that relationship after the termination of his employment. Initially, the defendant took advantage of that relationship and obtained SUBJECT A's keys without the knowledge or permission of SUBJECT A. Once he obtained the keys, the defendant used them to enter the Senator's Office alone at night, with the specific intent of unlawfully accessing Senate-

owned computers, for the express purpose of stealing electronic information – including login credentials and other means of identification belonging to Senate employees.

During his repeated burglaries of Senator Hassan's Office, and assisted by the insider knowledge that he gained as a system administrator in that Office, the defendant obtained and took dozens of means of identification (including network login credentials) belonging to at least six employees of the Office of Senator Hassan – that is, his conduct constituted numerous instances of identity theft. The defendant also surreptitiously installed "keylogger" devices on at least six computers in Senator Hassan's Office. The keylogger devices were designed to be unobtrusive, legitimate looking devices that would go unnoticed by the individuals that were using the affected computers. They were also designed to record the keystrokes that Senate staffers typed on their Senate-owned computers – including the keystrokes that comprised usernames and passwords for Senate computers and computer networks, as well as personal e-mail accounts.[2]

During the burglaries after the installation of the keyloggers, the defendant accessed the keylogger devices and obtained the information they had recorded. The defendant was thus able to identify the login credentials that provided access to Senate computers and computer networks. The defendant then fraudulently used those stolen login credentials, unlawfully accessed Senate computers and computer networks, and then stole data (including dozens of additional login credentials for other electronic accounts for multiple victims), personal information, and electronic mail belonging to Senator Hassan's Office and its employees.

[2] According to information provided by the defendant, he used keylogger devices which emitted their own wireless networking ("Wi-Fi") signal. In order to avoid detection, the defendant configured the keyloggers so that their Wi-Fi signals would remain invisible to anyone who did not know the network name. As a result of this configuration the U.S. Capitol Police have been unable to find and access the keylogger signal, even after recovering the keylogger devices.

During the burglaries, the defendant copied dozens of gigabytes of data from computers in Senator Hassan's Office, including dozens of usernames and passwords belonging to Senate employees, credit card information belonging to Senate employees, social security numbers belonging to Senate employees, personally identifying information ("PII") belonging to hundreds of other persons, and tens of thousands of e-mails and internal documents belonging to Senator Hassan's Office. The defendant also obtained contact information for numerous sitting U.S. Senators, which included their home addresses and private phone numbers.

The defendant copied the stolen data onto multiple computers and electronic storage devices. The defendant sorted and organized at least some of the data, including by compiling one electronic folder that he designated as "high value." This "high value" folder included, among other items, the personal home addresses of multiple Senators.

There is evidence that the defendant considered various ways of using the stolen data to extort Senator Hassan's office, in exchange for a positive employment reference. Specifically, during the course of the Summer of 2018, as he was repeatedly burglarizing the Senator's office, the defendant repeatedly asked a friend (referred to here as "Witness 4") hypothetical questions about whether or not certain extortionate uses of stolen data would be unlawful. Witness 4 said that he repeatedly told the defendant not to do anything foolish.

The Defendant's Doxxing Offenses

On September 27, 2018, while watching the televised broadcast of a United States Senate hearing concerning the nomination of a United States Supreme Court Justice, the defendant became angry at some of participants in the hearing, in particular Senators that were supportive of the nomination. The defendant acted on that anger by maliciously publishing the personal home addresses and telephone numbers of Senators Lindsay Graham, Orrin Hatch, and Mike Lee. The

defendant published that information maliciously, with the intent to intimidate the Senators, and with the knowledge and intent that others who learned of the information would then use the information to intimidate the three aforementioned Senators, as well as members of their immediate families, by using the information that the defendant had now made public.

Specifically, between about 5:15 p.m. and 5:55 p.m., the defendant used a computer that was connected to the internet through a facility maintained by the House of Representatives and visited the "Wikipedia" articles for each of those Senators. The defendant then edited those Wikipedia articles – which were publicly available over the internet – so that the articles would include the Senators' home addresses and telephone numbers. The defendant also helped publicize those edits, by posting or "re-tweeting" posts about his edits over Twitter.

During the next few days, news organizations reported on the publication of the above-listed Senators' personal information (and described the impact that the publication had upon the Senators and their family members). Senator Rand Paul called for an investigation of the defendant's initial doxxing offenses. The defendant responded by maliciously publishing the personal home addresses and telephone numbers of Senator Paul as well as Senate Majority Leader Mitch McConnell, with the intent to intimidate them, and with the knowledge and intent that others would use that information to intimidate them. Specifically, on October 1, 2018, at about 5:50 p.m., using a computer that was connected to the internet through a facility maintained by the Senate, the defendant edited a "Wikipedia" article so that it would include Senator Paul's home address and phone number, as well the text, "He dares call for an investigation of ME?!?!?!? . . . I am the Golden God! . . . Also It's my legal right as an American to post his info . . . We are malicious and hostile . . . Send us bitcoins . . . Wednesday night will be the doxxed next[.]"

Finally, a few minutes later, using the same computer and internet connection, the defendant published the home address and telephone number of Senator Mitch McConnell.

The evidence shows that the defendant knew that his conduct caused harm to others, and that he derived satisfaction from media and other reports that his doxxing offense had caused emotional distress. For example, it was publicly reported that the doxxing led to telephone calls and harassment that caused emotional distress by the spouse of one of the defendant's targets. The defendant saw these reports and, on October 2, 2018, happily reported them to a friend (Witness 5), writing "Haha it ruined [a Senator's] wifes [sic] birthday[.]" Similarly, in other conversations with Witness 4, the defendant made clear that, in his opinion, the fact that his doxxing offenses caused distress among the victims was "really funny."

The Defendant's Use of SUBJECT A's Office Keys

During the Summer of 2018, the defendant was a friend of SUBJECT A, who was employed by Senator Hassan at the time. The defendant spent time socially with SUBEJCT A. According to the defendant, on at least one occasion in July 2018, he took SUBJECT A's office keys, without SUBJECT A's permission or knowledge. At some point after, SUBJECT A realized that the defendant had taken her keys and then asked the defendant about the issue. According to SUBJECT A, when the defendant responded with a cryptic non-answer to her question, SUBJECT A did not confront him, and did not explicitly know what the defendant had done.

In August 2018, SUBJECT A needed money to make a rent payment, and asked the defendant for a loan. When he lent her the money, the defendant told SUBJECT A that he expected her to return the favor. According to SUBJECT A, at the time she believed that the defendant meant that, at some unspecified point, he would ask to borrow her office keys again.

Later, in September 2018, the defendant showed SUBJECT A that he possessed internal e-mails from Senator Hassan's Office. The e-mails, which were dated after the end of the defendant's employment, related to an internal matter at the Senator's Office. Based on the content of the e-mails as well as various statements by the defendant, SUBJECT A knew that the defendant had stolen the e-mails, and that he had done so by unlawfully accessing Senate computers.

The Final Burglary & Obstruction

On October 2, 2018, the defendant directly asked SUBJECT A to lend him her office keys. At that time, based on all of their previous interactions, SUBJECT A correctly believed that the defendant wanted her keys so that he could unlawfully enter the Senator's Office and unlawfully access computers in the Senator's Office. SUBJECT A believed that she "owed" the defendant a favor, and, despite knowing the defendant's intended use, she handed her keys over to the defendant.

Shortly afterwards, the defendant used SUBJECT A's key to open the locked office door of Senator Hassan's Office. Once inside, the defendant planned on unlawfully accessing a Senate-owned computer that was used by Witness 3, an employee of Senator Hassan. When the defendant entered the office, he went to Witness 3's computer, used Witness 3's login credentials (which the defendant had previously stolen), and logged in to Witness 3's computer. The defendant opened a web-based e-mail application, which Witness 3 had never used, and attempted to review Witness 3's e-mails. The defendant wanted to review those e-mails to determine whether or not Senator Hassan's Office had provided unfavorably employment references about him.

Shortly thereafter, while the defendant was typing at Witness 3's keyboard and unlawfully accessing Witness 3's computer, Witness 2 entered Senator Hassan's Office, and immediately recognized the defendant as a person who did not have authority to be inside the Senator's Office.

The defendant used Witness 3's keyboard, locked Witness 3's computer, and fled. A few minutes later, at 10:25 p.m., the defendant sent a threatening e-mail to Witness 2. The defendant sent the e-mail from the address livefreeorpwn@gmail.com, an e-mail address that the defendant had created to conceal his true identity, including in connection with other activities involving data that the defendant had stolen from Senator Hassan's Office. The e-mail to Witness 2 was directed to Witness 2's email account at Senator Hassan's Office, and was titled, "I own EVERYTHING." The body of the e-mail stated, "If you tell anyone I will leak it all. Emails signal conversations gmails. Senators children's health information and socials." The defendant's reference to "signal conversations" was a reference to the use of Signal, an encrypted messaging application. The defendant's reference to "socials" was a reference to social security numbers.

According to Witness 2, Witness 2 was deeply disturbed by the defendant's threat, and over having to report the incident to law enforcement.

Later that evening, after the defendant had returned home, the defendant began to plan to destroy and conceal evidence of his crimes. The defendant wrote a note/checklist, reminding himself to "Backup all files . . . Mail backup . . . Burn aliases . . . Wipe down comps[.]" The defendant then attempted to actually delete electronic evidence, including electronic evidence of his data theft from Senator Hassan's Office, as well as evidence of his doxxing offenses. The items that the defendant deleted data from included a laptop computer that the defendant had used to "dox" the other Senators, and which he used to obtain and download stolen data from the Senator's Office.

The following morning, on October 3, 2018, the defendant met with SUBJECT A, to return SUBJECT A's key. During their meeting, and consistent with his handwritten note, the defendant told SUBJECT A to wipe down all of the computers, keyboards, and computer mice, and to unplug

the computers in Senator Hassan's Office. SUBJECT A understood, and the defendant hoped, that these actions would destroy latent fingerprints as well as electronic evidence of his unlawful conduct, and prevent them from being available for any criminal and grand jury investigation. SUBJECT A, who knew that the defendant had unlawfully entered Senator Hassan's Office the night before, did in fact attempt to "wipe down" computer keyboards and computer mouse devices, but was unable to complete the task of unplugging the computers, because Witness 3 entered the Office. SUBJECT A then texted the defendant, at about 8:28 a.m. on October 3, 2018, stating, "Hey[.] So I was able to wipe down the keys and mouse but [Witness 3] was coming so I could [not] do the other thing[.]" The defendant replied, "Thanks," and SUBJECT A finished the conversation by responding, "Np, sorry I couldn't do everything."

THE PLEA AGREEMENT

In the early stages of the case, the defendant accepted responsibility for his conduct and agreed to be interviewed by law enforcement. In order to give credit for the defendant's cooperation and acceptance of responsibility, the government extended a plea offer that significantly reduced the defendant's potential sentencing exposure. Specifically, the government extended a plea offer that permitted the defendant to plead guilty to two counts under 18 U.S.C. § 119, rather than five, and that permitted the defendant to avoid charges under 18 U.S.C. § 1028A.

If the defendant had been convicted of three additional doxxing counts, he would have faced a higher recommended sentence under the Guidelines, because each violation of 18 U.S.C. § 119 would have constituted a separate "unit" under the grouping analysis required under U.S.S.G. § 3D1.4. In addition to that increased sentencing range under the U.S.S.G. for the doxxing, computer fraud, and obstruction counts, a conviction under 18 U.S.C. § 1028A would

have required and additional two-year mandatory minimum sentence, which the Court would be required to impose consecutive with the sentences for all other charges.

ARGUMENT

I. Introduction

The government respectfully submits that a significant sentence is warranted under all of the circumstances of the case. The defendant's crimes were deliberate, malicious, and sustained over a long period of time; his crimes caused serious harm to the United States Senate, to individual Senators, and to their families and staff; and the defendant's acceptance of responsibility is amply reflected by the charge bargaining incorporated into the Plea Agreement.

II. Application Of The Sentencing Guidelines

A. Legal Analysis

The Guidelines provide advisory recommendations which the courts "must consult . . . and take . . . into account when sentencing," United States v. Booker, 543 U.S. 220, 264 (2005), defendants for violations of the United States Code. As the Supreme Court has explained, "[a]s a matter of administration and to secure nationwide consistency, the Sentencing Guidelines should be the starting point and the initial benchmark" in for determining the appropriate sentence. Gall v. United States, 552 U.S. 38, 49 (2007).

B. The Presentence Investigation Report

a. Offense Level For Counts One and Two

As set forth in the Presentence Investigation Report ("PSR"), the Probation Office determined that, after accounting for the applicable specific offense characteristics and a three-

point deduction for the defendant's acceptance of responsibility, the offense level for Counts One and Two (the doxxing counts) is "23."[3] The government submits that this calculation is correct.

i. The PSR Correctly Applies U.S.S.G. § 3B1.3

The government anticipates that the defense will assert that the PSR erroneously applies a two-level enhancement for "abuse of a position of trust" or use of a "special skill" under U.S.S.G. § 3B1.3. The government believes that the PSR correctly applies this enhancement. In an objection submitted to the Probation Office, the defense argued that U.S.S.G. § 3B1.3 should not apply, because the defendant "did not abuse any position of public or private trust," because "at the time of the offenses . . . Mr. Cosko was not employed with Senator Hassan's office." However, the government believes that the defendant did abuse his position of trust, and that his offense conduct required the application of special skills within the meaning of U.S.S.G. § 3B1.3.

First, the defendant's offense conduct involved the abuse of a position of trust. Prior to his termination, the defendant served as a computer systems administrator in the Office of Senator Hassan. In connection with that position, the defendant was entrusted with an intimate knowledge of, and broad access to, the computer systems, administrative accounts, and related security measures (including passwords and usernames) in Senator Hassan's Office. That is, precisely because of his trusted position as the systems administrator, he had access to certain information – network configurations, security measures, and login credentials – used in connection with his offenses. The fact that the defendant was fired did not relieve him of his obligation to keep confidential information confidential, nor did it authorize him to use that information for the purpose of committing crimes.

[3] As noted in the PSR, the defendant has fully accepted responsibility for his conduct in a timely manner. The United States therefore moves for the additional one-level reduction in the defendant's offense level. The calculations in the PSR accounted for this motion.

Moreover, in addition to abusing the knowledge that he gained from his previous position as a systems administrator, the defendant carried out his crimes by applying unusual levels of skill and sophistication concerning computer and cybersecurity practices. The defendant knew where and how to obtain sophisticated "keylogger devices" that secretly recorded every keystroke on computers in the Senator's office; he knew how to configure them so that they would be difficult to detect; and he knew where to place them so that members of Senator Hassan's Office would not notice them. These sophisticated keylogger devices were "designed to be unobtrusive, legitimate looking devices that would go unnoticed" – and, in fact they did go unnoticed even after the defendant's arrest. To his credit, after his arrest the defendant ultimately told law enforcement about the keyloggers, but that does not change the degree of their sophistication. In fact, even after the defendant informed law enforcement about the keyloggers, and described their characteristics, law enforcement remained unable to detect the wireless networks they transmitted. The government believes that the defendant's use of these devices, in the manner and configuration that he did, involved the use of a "special skill" set within the meaning of U.S.S.G. § 3B1.3.

ii. The PSR Correctly Applies U.S.S.G. § 3B1.3

The government anticipates that the defense will assert that the PSR erroneously applies a two-level enhancement for obstruction of justice under U.S.S.G. § 3C1.1. The government believes that the PSR correctly applies this enhancement. In an objection submitted to the Probation Office, the defense argued, without explanation, that the obstruction of justice described in the Statement of Offense applied only to Count Three, and not to Counts One and Two.

However, as set forth in the Statement of Offense, which the defendant signed, the defendant plainly engaged in obstruction of justice relevant to Counts One and Two. Specifically, the Statement of Offense provides that, after he returned to his residence on the night of October

2, 2018, "the defendant began to plan to destroy and conceal evidence of his crimes. The defendant wrote a note/checklist, reminding himself to "Backup all files . . . Mail backup . . . Burn aliases . . . Wipe down comps[.]" The defendant then attempted to actually delete electronic evidence, including electronic evidence of his data theft from Senator Hassan's Office, as well as evidence of his doxxing offenses. The items that the defendant deleted data from included a laptop computer that the defendant had used to "dox" the other Senators, and which he used to obtain and download stolen data from the Senator's Office." Statement of Offense at 8-9. And he sent SUBJECT A back to Senator Hassan's Office specifically to destroy physical and digital evidence: to wipe down all of the computers, keyboards, and computer mice, and to unplug the computers.

b. Grouping Analysis For Counts One, Two and Three

i. Count Three Does Not Group With Counts One And Two

In the Plea Agreement, the parties agreed that "Count 1, Count 2, and Count 3 each constitutes a separate group" under the U.S.S.G. The parties further agreed "that Counts 1 and 2 each constitutes one Unit under U.S.S.G. § 3D1.4(a), and that Count 3 constitutes at least one-half Unit," and that "U.S.S.G. § 3D1.4 requires adding 3 levels to the offense level for Count 1 (based on the one Unit from Count 1, one Unit from Count 2, and . . . one-half Unit from Count 3)."

Notwithstanding the plea agreement, the PSR concluded that Count Three should be grouped with Counts One and Two, because, under U.S.S.G. § 3D1.2(c), "one of the counts embodies conduct that is treated as a specific offense characteristic in, or other adjustment to, the guideline applicable to another of the counts[.]" The Probation Office observed that U.S.S.G. § 2B1.1(18)(B) provides an enhancement for Count Three, because "the offense involved the unauthorized public dissemination of personal information."

The government agrees that the defendant's offense conduct included the "unauthorized

public dissemination of personal information." However, the government respectfully submits that U.S.S.G. § 2B1.1(18)(B) does not account for the offense conduct of Counts One and Two. Counts One and Two are based on the defendant's making public restricted personal information with a particular criminal intent. That criminal intent – the heart of the violation of 18 U.S.C. § 119, the "intent to threaten, intimidate or incite the commission of a crime of violence" or the "intent and knowledge" that the information published "will be used" to do so – is not "embodied" in U.S.S.G. § 2B1.1(18)(B), which applies to any unauthorized dissemination of information of any kind, and for any purpose. In that context, it applies an enhancement of an additional two offense levels. If U.S.S.G. had been intended to cover the dissemination of information with the knowledge and intent that it would be used to threaten, intimidate, or incite violence against public officials or grand jurors, it would have been directed at that type of conduct (and likely would have required more than two levels of enhancement).

ii. Conclusion As To Grouping

For the reasons set forth above, the government submits that Counts One, Two and Three each constitute a separate group under U.S.S.G. § 3D1.2. As the parties agreed in the Plea Agreement, the government believes that, under U.S.S.G. § 3D1.4(a), Count Three constitutes either one-half or one whole unit. The government notes that, under U.S.S.G. § 3D1.4(a), whether Count Three is one-half unit, or whether it constitutes a whole unit, the end result is the same: the U.S.S.G. would require adding three offense levels to the defendant's overall score.

For these reasons, the government submits that, rather than the two offense levels added by the PSR, the grouping analysis under U.S.S.G. § 3D1.4 requires adding three offense levels.

c. The Defendant's Combined Offense Level

For the reasons set forth above, the government submits that the PSR correctly calculates

the offense level for Counts One and Two as **23**, and the government further submits that U.S.S.G. § 3D1.4 requires adding an additional three offense levels (rather than the two added by the PSR), resulting in a total combined offense level (prior to credit for acceptance of responsibility) of **26**. The government further submits that, after applying a three-level reduction for acceptance of responsibility, the defendant's final combined offense level is **23**.

d. The Recommended Sentencing Range Under The U.S.S.G.

The government agrees with the PSR's assessment that the defendant has a Criminal History Score of 0. The government submits that, based on the final combined offense level of 23, the recommended sentencing range under the U.S.S.G. is 46 to 57 months in prison.

III. The Statutory Sentencing Factors

As noted above, determining the recommended sentencing range under the U.S.S.G. is the first of two required steps for sentencing under the United States Code. The second step requires the court to consider that range, to consider other relevant factors set forth in the guidelines, and to consider the factors set forth in 18 U.S.C. § 3553(a). See, e.g., United States v. Hughes, 401 F.3d 540, 546 (4th Cir. 2005). These factors include (1) the nature and circumstances of the offense; (2) the history and characteristics of the defendant; (3) the need to impose a sentence that reflects the seriousness of the offense, promotes respect for the law, provides just punishment, affords adequate deterrence, protects the public, and provides the defendant with needed educational or vocational training and medical care; and (4) the need to avoid unwarranted sentence disparities among defendants with similar records convicted of similar conduct.

IV. The Government's Recommended Sentence

The government believes that the Court should sentence the defendant to the high end of the recommended sentencing range because the U.S.S.G. analysis would not otherwise capture the

severity of the defendant's conduct, would not reflect the nature of the harm imposed by the defendant's offenses, and does not account for the sustained and deliberate nature of his crimes.

V. Analysis of the Statutory Sentencing Factors

1. Nature and Circumstances of the Offenses

The government submits that this factor weighs heavily in favor of a significant sentence.

First, the defendant's burglary, doxxing, and computer fraud crimes were all committed deliberately, intentionally, and over an extended period of time. These were not crimes committed on an impulse, nor were they the product of a failure to think. The defendant plainly considered his actions, talked about them with others, and then continued down a determined path.

Second, the defendant's crimes were committed with a clear malicious intent toward other people. These were not crimes of a regulatory nature – with respect to the burglary and data theft, the defendant wanted revenge against his former employer, and he planned on extorting a positive reference. Similarly, with respect to the doxxing conduct, the defendant wanted to punish people who disagreed with his politics. Further, the defendant sought to extort a witness into silence, by threatening to release the private health information about a Senator's children.

Finally, although the defendant's crimes will be addressed in a single hearing – and were connected by the defendant's continuing belief that he was always right and those who opposed (or fired) him were always wrong, and by his belief that he could violate the sanctity of the United States Senate at will and threaten individual Senators as he pleased – the data theft, doxxing, and obstruction crimes were entirely distinct from one another, with distinct sets of victims, and causing distinct sets of harm. The defendant's burglary and data theft campaign targeted his former employer, who, in the defendant's view, should not have terminated his employment; his doxxing

campaign targeted United States Senators because he did not agree with their politics; and his witness tampering and obstruction of justice was a corrupt exercise in self-preservation.

2. History and Characteristics of the Offender

The defendant appears to be an intelligent and capable adult, having been raised by a good family in a stable environment, having graduated from college and pursued a graduate degree, and having enjoyed significant and loving support from both parents. While the defendant does have a criminal history, and a history with illegal drug use, a review of the PSR shows that there are no particularly mitigating circumstances in the defendant's character or background.

3. The Need to Promote Respect for the Law, to Provide Just Punishment, to Afford Adequate Deterrence, to Protect the Public

For the reasons set in Part 1 above, the government submits that the circumstances of this case demand a significant sentence, in order to promote respect for the law, provide adequate deterrence to the defendant and others, and to justly punish the defendant for his conduct, for the harm that he imposed on others, and for the impact of his actions on the victims in this case.

In addition, the government notes that the defendant operated under the belief that he was entitled to inflict emotional distress upon United States Senators and their families, simply because they disagreed with the defendant and had different political views. The government believes that there appears to have been an increase in similar criminal harassment, particularly through social media channels, by people across the political spectrum. In fact, in this particular case, after the defendant doxxed United States Senators based on their positions in a matter of public debate; people on the other end of the political spectrum responded by attempting to identify the defendant, and, after mis-identifying a different person (a staffer for a Member of the House of Representatives), responded by harassing and threatening her, causing that innocent staffer to fear for her safety. The government believes that a significant sentence would help to make clear that

difference of political opinion do not entitle people to engage in politically motivated, criminal attacks threatening elected officials with whom he disagrees, and would thereby encourage respect for the law, and deter future criminal conduct.

4. The Need to Provide the Defendant with Educational or Vocational Training or Medical Care

The defendant would no doubt benefit from additional education and counseling, but nothing in the PSR shows that he has any unusual or particular need for education, training, or medical care that would impact the appropriate sentence. The government would submit that the defendant should be evaluated for any counseling or therapy that would benefit him, but does not believe that the appropriate sentence is otherwise impacted by this statutory factor.

5. The Need to Avoid Unwarranted Sentence Disparities

The government believes its recommended sentence will avoid any unwarranted sentence disparities. First, government is not aware of any case involving conduct that is distinctly similar to the conduct in this unusual case – the defendant's data theft alone is *sui generis*, and when combined with the obstruction and doxxing offenses, there are few proper points of comparison. This is particularly so because the U.S.S.G. calculates the offense level for computer fraud based on economic harm, using the same Guideline that applies to commercial fraud, and while the defendant's offense conduct was malicious, it was not intended to cause economic harm. Second, the government submits that the Court can adequately avoid any potentially unwarranted sentencing disparities by imposing guidelines-compliant sentences.

CONCLUSION

For all of the foregoing reasons, the government respectfully requests that the Court sentence the defendant to a total of 57 months in prison. The government further requests that the Court sentence the defendant to three years of supervised release, and to pay the required special

assessments of $100 for each of Counts One, Two, Three, Four, and Five. Finally, the government requests that the terms of the defendant's supervise release include a requirement that he stay away, and refrain from contacting, the victim U.S. Senators and their families; a requirement that he stay away from the U.S. Senate; and a requirement that he shall not engage in any unlawful activity involving a computer.

Respectfully submitted,

ALESSIO D. EVANGELISTA
Attorney for the United States, Acting Under Authority Conferred by 28 U.S.C. § 515

BY: /s/
Demian S. Ahn
DC Bar No. 491109
Tejpal S. Chawla
DC Bar No. 464012
Assistant United States Attorneys
United States Attorney's Office
555 Fourth Street, N.W.
Washington, D.C. 20530