U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

January 25, 2024

BY HAND (WITH CLASSIFIED ATTACHMENT)
BY ECF

Hon. Jesse M. Furman
United States District Judge
Southern District of New York
Thurgood Marshall U.S. Courthouse
40 Foley Square
New York, New York 10007

Re: *United States v. Joshua Adam Schulte*, S2/3 17 Cr. 548 (JMF)

Dear Judge Furman:

Joshua Adam Schulte stands convicted of some of the most heinous, brazen violations of the Espionage Act in American history. Schulte's theft of an arsenal of extremely sensitive intelligence-gathering cyber-tools from the Central Intelligence Agency ("CIA") and subsequent dissemination of that information to WikiLeaks—which in turn publicized it to America's adversaries—is "one of the largest unauthorized disclosures of classified information in the history of the United States." (Letter from David S. Cohen, Deputy Director, CIA, attached as Exhibit A[1]). His crimes "placed directly at risk CIA personnel, programs, and assets; and jeopardized U.S. national security." *Id.* After being caught for those crimes, Schulte declared what he called "my information war," announced his intention to "#FuckYourTopSecret" (2022 GX809 at 3, 11),[2] and further disclosed and attempted to disclose even more classified information from jail in flagrant defiance of numerous warnings and a Court order. And all the while, both before and after his arrest, Schulte fed an abhorrent personal fixation through his collection and viewing of an enormous trove of child sexual abuse materials ("CSAM") depicting the rape and sexual abuse of children as young as two years old, including images of bondage and sadomasochism and

[1] In addition to Deputy Director Cohen's letter, the Government also respectfully submits a classified letter from Peter T. Ranks, Director of CIA's Center for Cyber Intelligence ("CCI"), that discusses in more detail the impact of Schulte's crimes on the CIA as the victim of the espionage-related crimes charged in this case (the "CCI Letter").

[2] As used in this submission, "2022 Tr." refers to the transcript of the defendant's 2022 trial, and "2023 Tr." refers to the transcript of the defendant's 2023 trial. "2022 GX" refers to Government exhibits at the 2022 trial, and "2023 GX" refers to Government exhibits at the 2023 trial. "Schulte Ltr." refers to the defendant's January 18, 2024 sentencing submission. "PSR" refers to the Probation Department's Final Presentence Investigation Report, filed December 4, 2023.

involving sex acts performed on children by adult men and by animals. After considering all of the relevant sentencing factors under 18 U.S.C. § 3553(a), a sentence of life imprisonment, as prescribed by the United States Sentencing Guidelines ("U.S.S.G." or the "Guidelines"), is the only appropriate punishment for these crimes and this criminal.

I. Schulte's Offense Conduct.

The Court is well-familiar with the specifics of Schulte's offenses, which were proven in great detail at his trials in 2022 and 2023. The Government agrees with the detailed factual recitation set forth in the PSR, and summarizes salient facts briefly below.

A. Schulte's Employment at the CIA and Initial Abuse of Administrator Privileges.

In brief, Schulte began working for the CIA in approximately 2012 as a software developer in the CCI, which conducts offensive cyber operations, that is, cyber espionage relating to foreign governments or terrorist organizations. (PSR ¶ 45.) Schulte worked in the Applied Engineering Division ("AED"), which developed cyber tools for that mission. (*Id.*) Until approximately March 2016, Schulte was assigned to the Operations Support Branch ("OSB"), which was particularly focused on counterterrorism, developing cyber tools designed to gain access to computer networks and gather intelligence information. OSB's tools were used in, among other thing, human-enabled operations or asset-enabled operations—that is, cyber operations that involved a person with access to the computer network being targeted by the cyber tool. (PSR ¶ 46.)

In addition to being a developer, Schulte was also, for a time, one of the administrators of the suite of development programs produced by Atlassian Corporation that OSB and other development branches used to develop cyber tools. (PSR ¶ 47.) Schulte was also one of the OSB developers who administered a server used by OSB to design and test cyber tools. (*Id.*)

In March 2016, Schulte was moved from OSB to the Remote Development Branch ("RDB") as a result of personnel issues. (2022 GX1046; 2022 Tr. 486-90, 1392.) Following that transfer, in April 2016, Schulte abused his Atlassian administrator powers to grant himself administrator privileges to an OSB project for which he had been made an ordinary user as a result of his move from OSB to RDB. (PSR ¶¶ 49-50.) When Schulte first discovered that his project administrator status had been removed, he confronted a colleague who had implemented the permissions change, falsely claimed to have gotten approval from a supervisor to have his permissions restored, and threatened that he would "eventually get access back to the [project] and that access should just be enabled now." (PSR ¶ 50.) After Schulte unsuccessfully sought to be restored as a project administrator through a series of emails with additional supervisors, he simply used his Atlassian administrator privileges to make himself an administrator for the OSB project. (PSR ¶ 51.)

Schulte's abuse of administrator privileges was detected, and CCI leadership directed that Atlassian administrator privileges would immediately be transferred from developers to another division, the Infrastructure Support Branch ("ISB"). (PSR ¶¶ 52, 56.) The Monday after the developers' Atlassian administrator privileges were revoked and transferred to ISB administrators, Schulte was given a warning about self-granting administrator privileges that had previously been revoked. (PSR ¶ 60; 2022 GX1066, 1095.) Schulte lied about his threat that he would "eventually

get access back" to the project and claimed he said that he was going to add his own access back unless someone with authority advised him not to; and claimed that he thought the removal of his permissions was unauthorized. (PSR ¶ 60.) In a later meeting with one of the heads of CCI, during which Schulte was warned that he could be fired for abusing administrator privileges, Schulte boasted, threatened, or both, that "I could restore my privileges if I wanted to, you know I could do that." (2022 Tr. 1677.)

B. Schulte Uses a Secret Administrator Session To Steal the CIA's Cyber Tool Library.

Before Schulte's Atlassian administrator privileges were revoked, he opened a secret administrator session on OSB's server (PSR ¶ 54), which was also used to host an Atlassian tool called "Confluence" as a virtual server. The Confluence virtual server running on OSB's server had access to the network location where backups of AED's development suites were stored, which contained extensive documentation about the CIA's cyber tools. (2022 GX1207-36; 2022 Tr. 766, 814-16, 1382-84.)

After Schulte's and the other developers' Atlassian administrator privileges were transferred to ISB, Schulte lied to his supervisor and claimed that "I verified that all private keys with access have been destroyed/revoked." (2022 GX1063.) Shortly before making this representation, Schulte tested his administrator access to the OSB server using a private key and found that it was still active, and Schulte was still running an administrator session on OSB's server when he made the representation. (2022 GX1703-1 at 32, 1209-17; 2022 Tr. 841-42.)

Already angry about the personnel issues that led to his reassignment from OSB to RDB and the reassignment itself, Schulte was livid about the revocation of his Atlassian administrator privileges, and immediately began testing his ability to access restricted parts of the CIA cyber tool development network in order to steal AED's cyber tool library. (2022 GX1203-18, 1202-7, 1209-09, 1209-13, 1703-1 at 11-12 & 15-20, 1704-1 at 32-34, 3501-1; 2022 Tr. 778, 811-14, 816-20, 1148-49.) Although Schulte could not access the network location where Atlassian backups were stored after the removal of his Atlassian privileges (PSR ¶ 55), he was able to use his administrator session on the OSB server to view the Confluence virtual server and review, edit, and delete log files. (2022 GX1209-8, 1703-1 at 36-37 & 39, 1203-43; 2022 Tr. 845-49.)

On April 20, 2016—only six days after abusing his administrator privileges and only two days after being admonished for doing so—after other developers had left the office, Schulte used his secret OSB server administrator session to execute a complicated series of maneuvers on the CIA network to restore his Atlassian administrator privileges, break in to the backups, steal copies (the "Stolen CIA Files"), revert the network back to its prior state, and delete hundreds of log files in an attempt to cover his tracks. (PSR ¶¶ 66-68; 2022 GX1201-16, 1202-18, 1202-19, 1202-20, 1202-21, 1203-1, 1203-2, 1207-27, 1207-30, 1703-1 at 47-51, 53-55, 61, 63-64, 66, 68-90; 2022 Tr. 762-63, 854-93, 1083-84, 1089, 1379-81, 1624.)

C. Schulte Transmits the Stolen CIA Files to WikiLeaks and Securely Deletes Data from His Home Computer.

Between April 18 and May 5, 2016, Schulte took a number of steps to transmit the Stolen CIA Files to WikiLeaks: Schulte updated his versions of Tails (an operating system that boots from an external media device and is designed to leave no forensic trace of the user's activities) and the Tor browser (an encrypted, anonymizing network that makes it difficult to intercept or trace internet communications that can access the "dark web ") on his home computer—both tools recommended by WikiLeaks to potential leakers. (PSR ¶ 69.) Schulte researched, downloaded, and tested different tools for secure data deletion—the kind of data deletion that frustrates forensic recovery efforts—another tactic recommended by WikiLeaks. (PSR ¶ 70.) On May 5, 2016, having transmitted the Stolen CIA Files to WikiLeaks, Schulte wiped and reformatted his home computer's internal hard drives. (PSR ¶ 70.) Schulte also had several other external hard drives that had been securely wiped by the time the FBI seized them from his apartment in 2017.

Schulte resigned from the CIA in late 2016 and relocated to Manhattan. In the time-period between leaking the Stolen CIA Files and resigning, Schulte repeatedly embellished and escalated his false claims about his April 2016 abuse of administrator privileges, falsely claimed he was retaliated against for reporting personnel issues, falsely accused colleagues of misconduct, and again misused project administrator privileges to exclude OSB developers from another OSB cyber tool development project. (2022 GX1080, 1093, 1096; 2022 Tr. 548-58, 1667-72.) One of Schulte's supervisors, increasingly exasperated by Schulte's obstreperous conduct, explained that "I was frustrated by the fact that you kept trying to obtain your admin privileges over the [OSB development] project after being told not to do so, not to be [ ] reinstating your admin privileges and it kept coming up. And as a supervisor, when we asked you not to do that and you continued to do it, it became a problem. It was very frustrating." (2022 Tr. 681.)

D. WikiLeaks Releases Data from the Stolen CIA Files, Causing Instant Devastation to the CIA's Cyber Operations.

On March 7, 2017, WikiLeaks began publishing classified data from the Stolen CIA Files. (2022 GX1.) Between March and November 2017, there were a total of 26 disclosures of classified data from the Stolen CIA Files, which WikiLeaks denominated as Vault 7 and Vault 8 (the "WikiLeaks Disclosures"). (PSR ¶ 78.)

The impact on the CIA was immediately catastrophic. The network used to develop cyber tools was disconnected and the network and every external device connected to it were turned over to the FBI in support of its investigation. (*Id.*) Personnel involved in cyber operations had no computer equipment for cyber development. A number of personnel diverted their resources from developing tools for cyber operations to assessing the extent of the intrusion and the risk and impact of additional disclosures. Further cyber operations were halted and previous and ongoing operations were at risk of exposure. Cyber tools had to be rebuilt and redesigned. The effect of the WikiLeaks Disclosure was a "digital Pearl Harbor. We were dead in the water." (2022 Tr. 1681; *see also* 2022 Tr. 112-13.)

E. Schulte Lies to the FBI.

On March 15, 2017, two FBI agents approached Schulte as he was leaving work at Bloomberg and asked to speak with him. During a voluntary interview at a nearby restaurant, Schulte made numerous false statements, including denying being responsible for the theft of the Stolen CIA Files or for the WikiLeaks Disclosures. (PSR ¶ 79.) Schulte participated in two further voluntary interviews, accompanied by counsel, with FBI agents and Assistant United States Attorneys on March 20 and 21, 2017, at the U.S. Attorney's Office in the Southern District of New York. (PSR ¶ 82.). Schulte made additional false statements during these interviews, spinning fake narratives about ways the Stolen CIA Files could have been obtained from CIA computers that were intended to deflect suspicion away from Schulte and to divert law enforcement resources to unproductive investigative efforts. (*Id.*) Schulte further denied his involvement in the theft, including specifically denying taking the types of actions that he did, in fact, take on April 20, 2016 that enabled him to commit his crimes. (PSR ¶ 83.).

F. Schulte's Receipt and Possession of CSAM.

In March 2017, the FBI searched Schulte's residence in New York pursuant to a search warrant and recovered, among other things, multiple computers, servers, and other electronic storage devices, including Schulte's personal desktop computer (the "Desktop Computer"). On the Desktop Computer, FBI agents found encrypted containers containing tens of thousands of videos and images of child sexual abuse materials, including approximately 3,400 images and videos that meet the legal definition of child pornography, otherwise known as CSAM. (PSR ¶ 84.) Schulte had collected those materials over the course of years, both before and after his employment at the CIA. These files included extraordinarily disturbing and horrific images of child pornography depicting the rape and sexual abuse of children as young as two years old, images of bondage and sadomasochism, and images involving sex acts performed on children by adult men and by animals. (*Id.*) For example, one video file showed a young girl less than 12 years old bound by ropes and cables who was masturbated by an adult male, who was forced to perform oral sex on an adult male, who was forced to have her genitals licked by a dog, and who was forced to perform oral sex on a dog. (2023 Tr. 140-41, 158-60; 2023 GX1001-4.) Many of the child pornography files that Schulte downloaded had descriptive titles that identified the ages of the children involved and described the sexual abuse shown in the files, sometimes in graphic terms. (PSR ¶ 84.)

The child pornography that Schulte saved on his Desktop Computer was stored beneath several layers of encryption. The computer itself was encrypted, and the Linux Mint virtual machine where a large portion of the child sexual abuse materials were stored was also password-encrypted. After decrypting the Linux Mint VM, an additional password was required to log in. A third password was required to access the "josh" home directory where the child pornography was stored. The child pornography was further stored inside an encrypted container called "data.bkp" which required a fourth level of password access. Most of the child pornography on the virtual machine was stored in the "data.bkp" container. Additional child pornography was also saved within a second encrypted container, also called "data.bkp," that was saved inside the outer "data.bkp" container. The inner "data.bkp" container required a fifth level of password access. (*Id.*)

Forensic evidence shows that Schulte opened and viewed those child sexual abuse materials on his Desktop Computer (PSR ¶ 89), and reveals a disturbing pathology in which Schulte frequently viewed those materials on dates in which events relevant to his crimes of espionage occurred. For example, on the night of April 18, 2016 (the day Schulte was admonished by the CIA for self-granting previously revoked privileges), he opened files called "OPVA PTHC[3] 2015 11yo and uncle best anal fuck creampie ever!!!!!.avi." (2023 GX 2301 at 37.) Similarly, on April 20, 2016 (the same day Schulte committed the theft of the Stolen CIA Files), Schulte opened a 16-minute video showing the bondage, rape, and bestiality of a nine-year old girl described above. (2023 GX 2301 at 41.)

G. Schulte Continues His Efforts to Leak Classified Information and Protected Discovery Materials From Prison As Part of an "Information War" Against His Prosecution.

Schulte was charged by complaint with offenses related to the possession, receipt, and transportation of child pornography, and arrested on August 24, 2017. He was briefly remanded, but ultimately released on bail on September 15, 2017, subject to strict conditions, including, among others, home incarceration and no use of computers or the Internet in the absence of express authorization from Pretrial Services. (D.E. 8.)

On September 18, 2017, the United States District Judge Paul A Crotty entered a protective order prohibiting Schulte from disseminating discovery materials produced by the Government and marked as Confidential (the "Protective Order"). (PSR ¶ 92.) On December 14, 2017, the Court revoked Schulte's bail based on, among other things, Schulte's violations of his bail conditions by having someone else access the internet on his behalf, including through the use of Tor. (*Id.*). Schulte was remanded to the Metropolitan Correctional Center ("MCC"), where he was initially housed in the general inmate population. (*See* PSR ¶ 93.)

While incarcerated, in approximately April 2018, Schulte sent a copy of the affidavit in support of the warrant to search his apartment, which was subject to the Protective Order, to reporters with the *Washington Post* and *The New York Times*. In recorded prison telephone calls on April 17, 2018, Schulte discussed the information he had provided to the reporters with family members, and Schulte's family members' discussions with reporters on his behalf. Schulte's family members also arranged three-way conference calls with a reporter and on one of those calls, Schulte noted that the search warrant affidavit was subject to the Protective Order. (PSR ¶ 95.) After articles containing information from that affidavit were published, at a court conference on May 18, 2018, Judge Crotty admonished Schulte of the terms of the Protective Order, and Schulte acknowledged, "I understand." Despite the Court's admonition, Schulte continued his plans to disclose protected discovery materials and classified information. (PSR ¶ 96.)

---

[3] "PTHC" means "preteen hardcore," a term describing CSAM. (2023 Tr. 128.) "Yo" in the CSAM context indicates that age of the child depicted. (*Id.*) Finally, "OPVA" stands for "Onion Pedo Video Archive," which describes certain CSAM files found on the anonymous dark web browser program Tor. (*Id.* 140.)

In the summer and fall of 2018, Schulte made plans to wage an "information war" against the United States government to influence his criminal case through the media and to retaliate against his prosecution and perceived grievances against the CIA. In furtherance of this campaign, Schulte obtained access to contraband cellphones that he used to create anonymous, encrypted email and social media accounts. (PSR ¶ 98).

Schulte documented his planned campaign in handwritten journals. In an entry dated August 8, Schulte wrote: "If govt doesn't pay me $50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery that is the USG [United States government]. I will look to breakup diplomatic relationships, close embassies, end U.S. occupation across the world . . ." (2022 GX809 at 2.) On August 14, Schulte wrote: "Got to use last night," referring to a contraband cellphone; "[t]he way is clear. I will set up a wordpress . . . From here, I will stage my information war." Schulte wrote about releasing posts and articles on social media as he wrote them. (*Id.* at 3.) In an "article" Schulte was writing about his various grievances against the government, he wrote: "The FBI, in all its brilliance, has just taken a senior engineer with intimate knowledge of the NSA, CIA, and all projects and operations he's worked on . . . Does that sound like the most intelligent move, really? Obviously this isn't intended as a threat . . . Essentially, it's the same as taking a soldier in the military, handing him a rifle, and then begin beating him senseless to test his loyalty and see if you end up getting shot in the foot or not. It just isn't smart." (2022 GX820-430 & -431.)

Schulte continued to document his plans in an entry dated August 21st, a checklist of actions for furthering his information war, avoiding detection, and deleting evidence. (2022 GX809 at 5.) Schulte's list included deleting emails and documents from one of his anonymous accounts; creating new logins and passwords for accounts; creating a new encrypted email account; setting up new WhatsApp, Signal, and Telegram accounts with different phone numbers; resetting his contraband cellphone and cleaning off the apps; and changing the IMEI associated with his Samsung contraband cellphone. (*Id*.) Schulte learned that the FBI had learned the IMEI of one of his other cellphones by subpoena, and worried that the IMEI could be used to identify his accounts. (*Id*.) That following day, Schulte used a random password generator to create new passwords for his email and social media accounts. (*Id.* at 6; 2022 Tr. 1833-34.)

On August 23, 2018, Schulte wrote about transitioning to his new encrypted email accounts and cleaning the contraband cellphone. Schulte also noted that he had started emailing a reporter from the Washington Post. Using a messaging app and an anonymous email account, Schulte communicated with the reporter about his prosecution, pretending to be one of his own family members and a friend of the family. In an email dated September 24, 2018, Schulte emailed the reporter a search warrant affidavit that had been produced in discovery subject to a protective order, along with Schulte's comments on the affidavit. Schulte's criticisms of the affidavit's allegations included classified information about the DevLAN network and the number of employees in CIA cyber intelligence groups. In addition to emailing the reporter, Schulte attempted to use the contraband cellphones to transmit his discovery materials to WikiLeaks, but was unable to do so. His journal entry for September 12, 2018 includes the note, "DL disc UL WL," meaning "download discovery, upload to WikiLeaks." (PSR ¶ 101.)

Throughout August and September, Schulte drafted blog posts and tweets. In these, Schulte pretended to be one of his own former CIA colleagues and falsely claimed his innocence. (2022 GX809 at 8-13.) These draft tweets and blog posts contained classified information about CIA cyber tools and operations. S chulte sought to authenticate his assumed identity as a CIA developer by revealing information about a particular cyber tool called Bartender, including details of Bartender's operation and information that would have publicly associated Bartender with a piece of malware that had been found by security professionals, but had never been attributed to the CIA. (2022 GX809 at 8, 10, 11; 2022 Tr. 1421-28, 1604-05, 1653-55.)[4] The public release of this kind of information could enable targets of CIA cyber operations to identify, not only the cyber tool used in the operation, but individuals involved in deploying the tool—risking human assets being burned, retaliated against, and potentially executed. (Tr. 1366-67.) Schulte's writings also reflected his desire to leak and cause the leak of classified information, such as hashtags "#TopSecret" and "#FuckYourTopSecret" (2022 GX809 at 11) and exhortations to government employees to "send all your govt's secrets here: WikiLeaks." (*Id.* at 13.) The information Schulte planned to disclose in his information war was not included in his classified discovery or in the WikiLeaks Disclosures.

On September 12, 2018, Schulte wrote about finalizing copy, referring to his blog posts and articles; and scheduling tweets. Schulte in fact had created a Buffer account, an application for scheduling tweets or Facebook posts and had linked his Twitter account, "@freejasonbourne," to the Buffer account. One of Schulte's articles, called Article 10 or Malware of the Mind, included a description of CIA cyber tool techniques for concealing data. (PSR ¶ 104.) The FBI searched Schulte's MCC cell and seized the contraband phones on October 3, 2018, before Schulte publicly released his blog posts and tweets. (2022 Tr. 1813-14.)

On October 26, 2018, Special Administrative Measures ("SAMs") were imposed on Schulte based on his repeated disclosures and attempted disclosures of classified information and protected discovery materials. The SAMs, broadly speaking, limit his contact with other inmates and the public, allowing contact with his attorneys and monitored visits by family members. The SAMs were not imposed solely on the basis of Schulte's conduct at the CIA that led to his original charges for crimes of espionage—they were only imposed after he subsequently committed crimes (for which he has been convicted at trial) of disclosing and attempting to disclose *even more* sensitive national defense information while incarcerated in general population at the MCC.

II. Schulte's Convictions.

As a result of this conduct, in March 2020, Schulte was found guilty at trial of contempt of court and making material false statements, in violation of 18 U.S.C. §§ 401(3) and 1001.[5] On July 13, 2022, Schulte was found guilty at trial of eight counts: illegal gathering and transmission of national defense information in connection with his theft and dissemination of the Stolen CIA Files, in violation of 18 U.S.C. §§ 793(b) and (e); illegal transmission and attempted transmission of national defense information, both in violation of 18 U.S.C. § 793(e); unauthorized access to a

[4] In addition to Schulte's planned disclosures about Bartender, his planned internet posts contained classified information about other CIA operations, the particulars of which remain classified, and which were not derived from classified discovery or the WikiLeaks Disclosures.

[5] The jury failed to reach a verdict in the first trial on the remaining counts.

computer to obtain classified information and information from a department or agency of the United States in connection with his theft of the Stolen CIA Files, in violation of 18 U.S.C. §§ 1030(a)(1) and (a)(2)(B); and two counts of causing transmission of harmful computer commands, in connection with his theft of the Stolen CIA Files, in violation of 18 U.S.C. § 1030(a)(5). [6] Finally, on September 13, 2023, Schulte's third trial ended in a verdict of guilty on charges of receiving, possessing, and transporting child pornography, in violation of 18 U.S.C. §§ 2252A(a)(1), (a)(2)(B), and (a)(5)(B).

The maximum possible term of imprisonment on all counts of conviction is life imprisonment, and Schulte is subject to a mandatory minimum term of five years' imprisonment as a result of his convictions for receiving and transporting child pornography in violation of 18 U.S.C. §§ 2252A(a)(1) and (a)(2)(B).

III. The PSR and Guidelines Calculation.

The Government agrees with the calculation of the Guidelines set forth in the PSR, including the grouping analysis and applicable enhancements. That results in a combined adjusted offense level of 51, which is reduced to 43 pursuant to Chapter 5, Part A (PSR ¶¶ 152, 155), and a Criminal History Category of VI pursuant to U.S.S.G. § 3A1.4(b). Accordingly, the applicable Guidelines sentence is life imprisonment.

Schulte raises a number of objections to the Guidelines calculation in his sentencing submission, which the Court should reject.

A. The PSR Properly Applied the Terrorism Enhancement.

The PSR correctly determined that the enhancement set forth in USSG §3A1.4(a) applies because Schulte's convictions include an offense "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and is a violation of . . . 1030(a)(1) (relating to protection of computers) [or] 1030(a)(5)(A) resulting in damage as defined in 1030(c)(4)(A)(i)(II) through (VI) (relating to protection of computers)" (PSR ¶ 129.) Schulte does not dispute that his convictions under Sections 1030(a)(1) and (a)(5) are qualifying statutory offenses, but he asserts that his crimes were not intended to retaliate against government conduct because "[o]ne of Mr. Schulte's supervisors at the CIA transferring Mr. Schulte to another team hardly qualifies as 'government conduct,'" and that the enhancement therefore should not apply. (Schulte Ltr. at 3-4.) But this both misapprehends the applicable legal standard and understates the nature of the defendant's conduct.

First, Schulte offers nothing more than unsupported *ipse dixit* for his assertion that the personnel actions taken by the CIA do not qualify as "government conduct." Schulte was not merely transferred between branches at the CIA; there were a range of official actions taken that prompted his vendetta against the agency: in particular, following Schulte's initial misconduct, senior CCI supervisors directed that Schulte's administrative access to OSB projects and ultimately the entire Atlassian suite be formally revoked (PSR ¶¶ 50-52), and Schulte was formally

[6] The jury also found Schulte guilty of obstruction of justice, in violation of 18 U.S.C. § 1503, as to which count this Court later granted Schulte's motion for a judgment of acquittal. (D.E. 1101.)

admonished for exceeding his unauthorized access (PSR ¶ 60). The fact that Schulte's response was wildly disproportionate to the actions taken by the CIA to attempt to secure DevLAN from Schulte's misconduct does not make those actions any less official government conduct.

Second, Schulte's *conduct*—stealing and disseminating the CIA's entire arsenal of cyber tools—demonstrates that his purpose was to retaliate against the government as a whole. Schulte's retaliatory response was not to accost a supervisor in the break room; he did not hack a supervisor's email; he did not take the sort of personally targeted actions that might suggest a more limited purpose. Rather, he engaged in crimes of espionage that the jury expressly found that Schulte "had the intent or reason to believe . . . would be used to the injury of the United States." (D.E.. 879 at 28.) The fact that Schulte's particular motive for doing so was undeniably, unconscionably, personal and trivial does not preclude the application of the terrorism enhancement for that conduct. In assessing the definition contained in Section 2332b(g)(5), the Second Circuit has emphasized this distinction:

> Section 2332b(g)(5)(A) does not require proof of a defendant's particular motive. "Motive" is concerned with the rationale for an actor's particular conduct. "Calculation" is concerned with the object that the actor seeks to achieve through planning or contrivance. Calculation may often serve motive, but they are not, in fact, identical. Section 2332b(g)(5)(A) does not focus on the defendant but on his "offense," asking whether it was calculated, *i.e.*, planned—for whatever reason or motive—to achieve the stated object. Thus, as we noted in *Stewart*, the section is better understood as imposing a requirement "that the underlying felony [be] calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct." [*United States v.*]*Stewart*, 590 F.3d [93,] 138 [(2d Cir. 2009)]). Clearly, a person may intend and may commit an offense that is so calculated even if influencing or retaliating against government is not his personal motivation. Thus, a person who murders a head of state, for instance, sure in the knowledge that his crime will influence or affect the conduct of government, satisfies the terms of § 2332b(g)(5)(A) even if his particular motivation in committing the murder is to impress a more established terrorist with his abilities.

United States v. Awan, 607 F.3d 306, 316–17 (2d Cir. 2010). Schulte's objection to the PSR's application of the § 3A1.4(a) enhancement ignores this distinction. The *conduct* for which he was convicted—the theft and dissemination of the highly-sensitive classified cyber tools found in the DevLAN backups—was clearly calculated to retaliate against the United States as a whole. The fact that Schulte's reasons for committing that crime against the United States were far more personal and spiteful serves only to illustrate the heinous nature of his behavior; it does not preclude application of the enhancement.

Schulte also argues that the Court should elect not to apply the enhancement because its consequences on the applicable Guidelines calculation are severe. While the Court certainly has the power to entertain Schulte's arguments that a Guidelines sentence would be unnecessarily harsh, the Court must nevertheless "begin all sentencing proceedings by correctly calculating the applicable Guidelines range," *Gall v. United States*, 552 U.S. 38, 49 (2007), and a "bare assertion

of atypicality . . . cannot reasonably support the complete rejection of the terrorism enhancement." *Stewart*, 590 F.3d at 174 (Walker, J., concurring in part). As set forth in the PSR, the enhancement properly applies, thus must be included as part of the Court's Guidelines calculation, and warrants due consideration in the Court's assessment of the appropriate sentence. *Compare* Schulte Ltr. at 4 (quoting initial sentencing proceedings in *United States v. Stewart*, 02 Cr. 395 (JGK)), *with Stewart*, 590 F.3d at 151 (vacating that sentence and remanding with the "require[ment] that such a sentence, selected after the reconsideration we have directed, begin with the terrorism enhancement and take that enhancement into account").

Nor are Schulte's arguments that the terrorism enhancement overstates the seriousness of his offense any more availing. While his crimes may not appear to be "terrorism" in the colloquial sense, Congress's inclusion of violations of § 1030(a)(1)—in effect, espionage by computer—in the enumerated list of covered crimes and the nature of Schulte's conduct reflect the same concerns for national security as do more traditional crimes of terrorism. "[E]spionage is one of this nation's most serious offenses." *United States v. Schulte*, No. 21-3113, 2022 WL 1316210, at *3 (2d Cir. May 3, 2022) (quoting *United States v. Whitworth*, 856 F.2d 1268, 1289 (9th Cir. 1988)). The enhancement reflects both the unusual severity of Schulte's crimes and the particular need to incapacitate those, like Schulte, who commit them:

> The import of this enhancement "could not be clearer": It reflects Congress' and the Commission's policy judgment "that an act of terrorism represents a particularly grave threat because of the dangerousness of the crime and the difficulty of deterring and rehabilitating the criminal, and thus that terrorists and their supporters should be incapacitated for a longer period of time."

Stewart, 590 F.3d at 172-73 (Walker, J., concurring in part) (quoting *United States v. Meskini*, 319 F.3d 88, 91-92 (2d Cir. 2003)); *accord United States v. Ceasar*, 10 F.4th 66, 79 (2d Cir. 2021); *United States v. Mumuni*, 946 F.3d 97, 112 & n.64 (2d Cir. 2019). The fact that Schulte committed his crimes with a keyboard and mouse rather than with explosives or firearms does not alter the catastrophic consequences that they had for national security. And Schulte's conduct following his commission of those crimes, as discussed further below, demonstrates the particular "difficulty of deterring and rehabilitating" him—precisely the type of concern that animates the inclusion of the enhancement in the first place. The PSR's calculation is correct and should be adopted.

B. The Obstruction of Justice Enhancement Properly Applies.

Schulte asserts that the Government has not shown that the false statements for which he was found guilty of violating 18 U.S.C. § 1001 "significantly obstruct[ed] or impede[d] the official investigation or prosecution of the instant offense." (Schulte Ltr. at 5.) His false statements are the subject of a separate count of conviction, and application of the enhancement is therefore mandatory. Application Note 4 to § 3C1.1 makes clear that the enhancement applies to "any other obstructive conduct in respect to the official investigation, prosecution, or sentencing of the instant offense where there is a separate count of conviction for such conduct." *See also* U.S.S.G. § 3C1.1 App. n.5 ("[I]f the defendant is convicted of a separate count for such conduct, this adjustment will apply and increase the offense level for the underlying offense."). In *United States v. Crisci*, 273 F.3d 235 (2d Cir. 2001), the Second Circuit rejected the defendant's challenge to the application of the enhancement on grounds, like those Schulte asserts here, that "his false statements were not

significant and did not deter the FBI's investigation." *Id.* at 240. The Court held, "[t]he application notes to the guideline state that the adjustment applies to any conduct regarding the official investigation of the instant offense 'where there is a separate count of conviction for such conduct.' In this case, Crisci's separate count of conviction for making false statements to the FBI agent investigating the instant offense compelled the district court to apply Section 3C1.1." *Id.*; *see also, e.g.*, *United States v. Riquene*, 552 F. App'x 940, 945–46 (11th Cir. 2014) (rejecting defendant's argument that enhancement did not apply because "his statements did not obstruct, significantly or otherwise, the investigation," holding that because Riquene was convicted under a separate count for making false statements, the § 3C1.1 enhancement applies even if his false statements would not otherwise warrant this adjustment"); *United States v. Williams*, 160 F. App'x 582, 586 (9th Cir. 2005) ("Williams was convicted of a separate count for making a false material statement under 18 U.S.C. § 1001, which is sufficient under U.S.S.G. § 3C1.1, Application Note 5(b) to warrant an obstruction of justice enhancement."); *United States v. Armstrong*, 842 F. Supp. 92, 94 (S.D.N.Y. 1994) (same). The same analysis applies here, and the PSR properly includes the enhancement for obstruction of justice based on Schulte's conviction for violating 18 U.S.C. § 1001.

C. The Enhancement for Gathering Top Secret Information Properly Applies.

Schulte's argument against applying the enhancement for gathering or transmitting information classified at the Top Secret level under USSG § 2M3.1(a)(1) is frivolous. He does not dispute—nor could he—that the national defense information he was charged with stealing and disseminating was in fact classified Top Secret. Schulte not only knew that from his employment at the CIA, but properly marked, Top Secret materials from the Stolen CIA Files were produced to him in discovery. Some of that information was in fact presented to the jury. (*See, e.g.*, 2022 Tr. 469 (describing DevLan as holding information classified "[a]t least top secret"); 2022 GX 3009 at 2 (excerpt of leaked information bearing markings "TS" and "TS/SCI").) To the extent that the specific classifications were not put before the jury, that is a function of Schulte's own objection—with limited exceptions—to the jury being made aware of those classifications at the risk of prejudicing its independent fact-finding with respect to whether the material qualified as "national defense information."[7] Instead, Schulte now asserts—without any support—that the Government has the burden of proving "that the materials were properly classified as top secret." (Schulte Ltr. at 5.) As the Court has previously observed, "there is neither authority nor basis to second guess the Executive Branch's classification determinations." (D.E. 622 at 1.) The undisputed fact that the information was classified Top Secret suffices to support application of the enhancement.

The facts of this case plainly demonstrate that the information is properly classified as Top Secret, meaning that "the unauthorized disclosure of [the information] reasonably could be expected to cause exceptionally grave damage to the national security." E.O. 13526 § 1.2(a)(1). Here, not only was that expectation reasonable, it was proven by the consequences of Schulte's theft and unauthorized disclosure. "[T]his was a digital Pearl Harbor. . . . It was devastating. It

[7] For example, 2022 GX 1, the laptop containing the WikiLeaks Disclosures, was classified Top Secret/Sensitive Compartmented Information, and admitted as a classified exhibit at trial, but the classification marking was blocked out at the defendant's request.

was pulling off operations overnight, the vast majority of the operations that we were conducting." (2022 Tr. at 1681, 1686.) As set forth in more detail in the CCI Letter, WikiLeaks' disclosures of the information stolen and disseminated by Schulte had precisely the sort of specific harms to national security that a Top Secret classification is intended to prevent. And as the Deputy Director of the CIA appropriately summarized, "the crimes committed by Mr. Schulte caused exceptionally grave harm to U.S. national security." Ex. A at 1. The "devastating" consequences of Schulte's unauthorized disclosure amply suffice to demonstrate the propriety of the undisputed Top Secret classification of that information in the first place.

D. The Enhancement for Abuse of a Position of Trust or Use of a Specialized Skill is Properly Applied.

Schulte objects to the application of the enhancement pursuant to U.S.S.G. § 3B1.3 on the grounds that the Government has not proven that the computer skills used by Schulte "to copy the classified information required 'substantial education, training or licensing;'" and that Schulte's administrator access had already been removed by the time he took the Stolen CIA Files, and therefore he was not in a position of trust to abuse. (Schulte Ltr. 5-6.) Both arguments equally misapprehend the facts and the law.

With respect to Schulte's use of specialized computer skills, the Second Circuit has rejected the suggestion that licensing or formal education and/or training is a prerequisite to application of the enhancement. *See, e.g., United States v. Spencer*, 4 F.3d 115, 120 (2d Cir. 1993) ("[W]e find no basis for limiting the increase to only those with formal educations or professional skills."). Nevertheless, the PSR makes clear that Schulte does in fact have "substantial education, training, or licensing." In addition to a bachelor's degree in electrical engineering with a specialty in computer engineering, Schulte received various computer-related certifications, including in the type of networking and computer forensics directly relevant to his theft of the Stolen CIA Files. (*See* PSR ¶¶ 183, 185.) Courts have routinely applied the enhancement to situations that closely parallel this one, regardless of the formality of the defendant's training or expertise. *See, e.g., United States v. Chinniah*, 173 F.3d 846 (2d Cir. 1999) ("The enhancement was supported by the showing that the defendant used his knowledge of computers and of his employer's internal computer controls in committing the offense."); *United States v. Lavin*, 27 F.3d 40, 41 (2d Cir. 1994) ("[T]he electronics skills employed by Lavin were plainly 'not possessed by members of the general public' and 'significantly facilitated' his crimes, Judge Keenan properly imposed a special skills enhancement."); *United States v. Petersen*, 98 F.3d 502, 507 (9th Cir. 1996) ("[S]ophisticated computer skills reasonably can be equated to the skills possessed by pilots, lawyers, chemists, and demolition experts for purposes of § 3B1.3.").

Moreover, as the testimony at trial made clear, Schulte's crimes required exceptionally sophisticated knowledge of the CIA's networks and means of evading controls designed to limit his access. Schulte's theft did not entail merely sitting down at his computer and performing the sorts of functions any normal computer user would be capable of. It required sophisticated knowledge and use of, among other specialized skills, (i) Linux root permissions and SSH key sessions (PSR ¶ 61); (ii) virtual machine manipulation, including the creation, restoration, and deletion of system snapshots (PSR ¶ 66); (iii) the interconnection between the OSB server and the Atlassian backups (PSR ¶ 55); (iv) the locations, content, and manipulation of log files of numerous types (PSR ¶ 68); and (v) the use of anonymizing tools like Tor and Tails and secure

deletion techniques to conceal user activity (PSR ¶ 69.) Presenting evidence of Schulte's conduct required extensive forensic exhibits and expert testimony from some of the FBI's foremost computer scientists—the testimony of Patrick Leedom regarding Schulte's manipulation of the Confluence virtual server, for example, spans more than 350 pages of the trial transcript. (2022 Tr. 697-1094.) It is frivolous to suggest that Schulte did not "use[] a special skill[] in a manner that significantly facilitated the commission or concealment of the offense." U.S.S.G. § 3B1.3.

Schulte also did in fact abuse a position of trust to commit his crimes. At the highest level, his employment at the CIA and the very fact of his access to the CCI office, the DevLAN network, and the classified information and sensitive national security tools it housed reflected a position of trust. (*See, e.g.*, 2022 GX 405 (Secrecy Agreement signed by the defendant, stating in paragraph 2 "I accept that by being granted access to such information or material I will be placed *in a position of special confidence and trust* and will become obligated to protect the information and/or material from unauthorized disclosure.") (emphasis added); 2022 Tr. 457 (describing the "huge role" that trust plays in protecting classified information).) With respect to Schulte's specific position, there is no question that his position of trust as an administrator of the Atlassian suite enabled him to commit the offense. Indeed, the very heart of how Schulte stole the CIA's cyber-tool arsenal was by using a series of reversions to snapshots of the Confluence server in order to restore to himself the administrator access that the CIA had previously revoked—because he had already once before abused that position of trust. The fact that Schulte's use of those administrator privileges was unauthorized does not make it any less an abuse of the trust that had been reposed in him. Accordingly, under either prong of § 3B1.3, the enhancement is properly applied.

IV. A Sentence of Life Imprisonment Is Necessary to Satisfy the Section 3553(a) Factors.

A. Applicable Law.

Although no longer mandatory, the Guidelines still provide strong guidance to the Court following *United States* v. *Booker*, 543 U.S. 220 (2005), and *United States* v. *Crosby*, 397 F.3d 103 (2d Cir. 2005). Although *Booker* held that the Guidelines are no longer mandatory, it held also that the Guidelines remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. 543 U.S. at 264. As the Supreme Court explained, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," and that "should be the starting point and the initial benchmark." *Gall*, 552 U.S. at 49. After calculating the Guidelines, the Court must consider the seven factors outlined in Title 18, United States Code, Section 3553(a): "the nature and circumstances of the offense and the history and characteristics of the defendant," 18 U.S.C. § 3553(a)(1); the four legitimate purposes of sentencing, *id.* § 3553(a)(2); "the kinds of sentences available," *id.* § 3553(a)(3); the Guidelines range itself, *id*. § 3553(a)(4); any relevant policy statement by the Sentencing Commission, *id*. § 3553(a)(5); "the need to avoid unwarranted sentence disparities among defendants," *id*. § 3553(a)(6); and "the need to provide restitution to any victims," *id.* § 3553(a)(7). *See Gall*, 552 U.S. at 49-50 & n.6. In determining the appropriate sentence, the statute directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

- to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
- to afford adequate deterrence to criminal conduct;
- to protect the public from further crimes of the defendant; and
- to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

Courts may not presume that the appropriate sentence necessarily lies within the Guidelines range, but "the fact that § 3553(a) explicitly directs sentencing courts to consider the Guidelines supports the premise that district courts must begin their analysis with the Guidelines and remain cognizant of them throughout the sentencing process." *Gall*, 552 U.S. at 50, n.6. Their relevance throughout the sentencing process stems in part from the fact that, while the Guidelines are advisory, "the sentencing statutes envision both the sentencing judge and the Commission as carrying out the same basic § 3553(a) objectives," *Rita* v. *United States*, 551 U.S. 338, 348 (2007), and the Guidelines are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions," *Gall*, 552 U.S. at 46. To the extent a sentencing court varies from the Guidelines sentence, "[it] must consider the extent of the deviation and ensure that the justification is sufficiently compelling to support the degree of the variance." *Id.* at 50.

B. A Guidelines Sentence of Life Imprisonment Is Necessary to Vindicate the Unprecedented Seriousness of Schulte's Offenses and the Need for Just Punishment.

Schulte's crimes of espionage are virtually unprecedented in their scope and harm to the national security of the United States. He committed "the largest data breach in CIA history, and one of the largest unauthorized disclosures of classified information in the history of the United States." (Ex. A.) To satisfy a personal vendetta, he "cost the [CIA] hundreds of millions of dollars; degraded its ability to collect foreign intelligence against America's adversaries; placed directly at risk CIA personnel, programs, and assets; and jeopardized U.S. national security by degrading the CIA's ability to conduct its mission." (Ex. A.) As set forth in additional classified detail in the CCI Letter, and as shown through evidence at trial, these costs were tangible and direct. "The impact on the CIA was immediately catastrophic." (PSR ¶ 78.) The entire development network was shut down, and taken into evidence by the FBI. The mission of AED "grinded to a halt," and the tools on which the CIA relied became instantly "essentially unusable." (2022 Tr. 575.) Schulte "destroyed all of" the work that his fellow officers had spent entire careers building. (2022 Tr. 1656.) Personnel at home and abroad were exposed as "[p]ast operations were put at significant risk," creating the very real fear that human beings who worked to protect this nation could "be executed for being a CIA spy." (2022 Tr. 1366-67.) Former Deputy Director of Digital Innovation Sean Roche summarized some of these consequences:

> [O]ur teams in the field, the partner intelligence services that we had worked on on these operations and, most importantly, most sensitively, where there were human beings involved in enabling the use of these tools because our digital cloak—our

> cloak that allowed us to remain clandestine—clandestine means there is no sign of what is going on—was gone. So, to me, the analogy was this was a digital Pearl Harbor. We were dead in the water.

(2022 Tr. 1681.)

These were not incidental effects of Schulte's conduct—they were his design. As the jury found, Schulte committed his theft of the Stolen CIA Files with the express "intent or reason to believe that the information [that he stole] *would* be used to the injury of the United States, not just that it *could* be so used." (D.E. 879 at 28 (emphasis in original).) Schulte did not act out of any misguided altruism, in some false belief that he would be a whistleblower; he acted out of pure spite and ego, and he chose to take his perceived grievance out on the country that he swore to defend. Schulte's theft and dissemination of the Stolen CIA Files represents one of the worst sorts of crimes of betrayal—he turned against his nation, his coworkers, and his friends.

While less astounding in scope than the unprecedented theft of the Stolen CIA Files, the classified information that Schulte disclosed and sought to disclose while incarcerated was itself uniquely damaging. By releasing information about the numbers of CIA officers assigned to particular groups, Schulte enabled America's adversaries to build "a mosaic of information" revealing among other things "who in the foreign field might be associated with a particular mission" and how adversaries could "target those individuals." (2022 Tr. 1671.) Likewise, by attempting to disclose the specifics of the tool named Bartender and its affiliation with the CIA, Schulte directly put human beings at risk of harm from America's enemies. As one of the developers directly involved in the production of that tool explained:

> So, and especially so for Bartender, a lot of the tools that we develop, there's a human operator involved that is either involved in the deployment or the operation to some degree. If you highlight the fact that it is a CIA tool that the vendor report is talking about, then there's now renewed motivation for both the vendor and/or other intelligence agencies to go searching for that data elsewhere to try to reveal, you know, the human involved in that operation as well as other operations and other humans involved in other operations. . . .
>
> [T]he humans involved in our operations are—are—there are several that are still around. And not only that—right—the historic holding of data that they can then use to unravel this operation, where it's deployed, they may be able to signature tradecraft as well as find people or individuals that were involved in that operation and link them to current operations.

(2022 Tr. 1654-55.) Schulte stole, and then disseminated, an unprecedented volume of information that shuttered crucial intelligence-gathering efforts, exposed capabilities and operations to foreign adversaries who were their targets, and thereby created untold damage to national security. A minimal sentence like the 108 months that Schulte seeks (which would be, in essence, a sentence of only 48 months in addition to the mandatory minimum resulting from the child pornography offenses) would make a mockery of the seriousness of these offenses and undermine the very concept of just punishment that Section 3553(a)(2)(A) demands.

Schulte's offenses relating to his trove of CSAM are of an entirely different type of crime than his national security offenses, but also caused, and continue to cause, grave harms. "Child pornography permanently records the victim's abuse, . . . causes the child victims of sexual abuse continuing harm by haunting those children in future years," and "inflames the desires of . . . pedophiles . . . who prey on children, thereby increasing . . . the sexual abuse and exploitation of actual children who are victimized as a result of the existence and use of [child pornography] materials." *Schulte*, 2022 WL 1316210, at *3 (quoting Child Pornography Prevention Act of 1996, Pub. L. No. 104–208, sec. 121, 110 Stat. 3009, 3009-26, 3009-27 (codified as amended at 18 U.S.C. § 2251)); *see also Paroline v. United States*, 572 U.S. 434, 439–40 (2014) ("The demand for child pornography harms children in part because it drives production, which involves child abuse. The harms caused by child pornography, however, are still more extensive because child pornography is a permanent record of the depicted child's abuse, and the harm to the child is exacerbated by its circulation." (cleaned up)). As noted in the PSR, Schulte collected images depicting the horrifying sexual abuse of children by parents and grandparents, children who "will be repeatedly re-victimized by the individuals like the defendant who possess, trade, and/or distribute their child sex abuse images." (PSR ¶ 119.)[8] As one of the victims starkly put it: "If you are looking at pictures or videos of me, or any child for that matter, then you are hurting everyone you look at. YOU are the one abusing us. YOU are the one keeping my pain going for the rest of my life." The Court, and the jury, saw a selection of these CSAM materials first-hand during Schulte's 2023 trial—their horrific details hardly require elaboration.

While it is appropriate for the Court to consider in assessing the appropriate sentence for these crimes the criticisms of the child pornography Guidelines that the Second Circuit has noted in *United States v. Jenkins*, 854 F.3d 181 (2d Cir. 2017), and *United States v. Dorvee*, 616 F.3d 174 (2d Cir. 2010), the grouping analysis of the defendant's crimes ultimately renders that specific Guideline calculation of little significance to the ultimate offense level. As the PSR correctly determines, because the offense level for the grouped CSAM-related counts, whatever disagreements may be levied with it, is dwarfed by that applicable to Schulte's crimes of espionage, it ultimately does not result in any unit-increase in the applicable combined adjusted offense level. (*See* PSR ¶¶ 149-52.)

Nor does the criticism described in *Dorvee* and *Jenkins* suggest that only a sentence at the mandatory minimum applicable to the CSAM crimes here would be appropriate—on the contrary, the Second Circuit has repeatedly affirmed higher sentences even in cases involving only possession of child sexual abuse materials. *See, e.g.*, *United States v. Braden*, 796 F. App'x 10, 12 (2d Cir. 2019) (affirming sentence of 97 months' imprisonment for possession and receipt of child pornography, collecting cases affirming sentences of 87, 97, 84, and 90 months' imprisonment for similar conduct). Whether or not the Court chooses to deviate from the metrics of the Guidelines in assessing the just punishment for these offenses, the sentence imposed must account for the fact that Schulte, while engaged in some of the most serious crimes of espionage

[8] As described in the PSR, 18 of the identified victims of the CSAM found on Schulte's Desktop Computer have written victim impact statements to be submitted in cases involving the images of their abuse. (PSR ¶ 120.) These statements are attached as exhibits to this submission, and, consistent with the PSR's recommendation, the Government respectfully requests that they be filed under seal.

ever prosecuted, was also collecting and viewing a staggering cache of some of the most despicable abuse of children imaginable. That conduct too demands a severe sentence to serve as just punishment.

In sum, the Court is faced with a defendant convicted of three discrete courses of conduct: (1) one of the largest espionage offenses ever committed, to satisfy Schulte's personal thirst for revenge and desire to retaliate against the United States government as a whole; (2) more espionage offenses, coupled with blatant defiance of the Court's orders and the law, in an attempt by Schulte to retaliate against his prosecution for crimes of which he is, in fact, guilty; and (3) a years-long drive for Schulte's personal gratification through the collection and viewing of thousands upon thousands of videos and images of children being subject to the most sickening abuse. Any of these alone would be extremely serious and demand lengthy imprisonment. Taken together, only a Guidelines sentence of life imprisonment will suffice to show due regard for the seriousness of these offenses and provide just punishment for them.

C. A Guidelines Sentence of Life Imprisonment Is Also Necessary to Afford Adequate Deterrence and to Protect the Public from Further Crimes by Schulte.

A Guidelines sentence of life imprisonment is also warranted to deter conduct both of the type Schulte committed and prevent further crimes by Schulte himself. The assessment of the need for general deterrence is closely linked to the seriousness of the offense evaluated under the first Section 3553(a) factor; put simply, "more serious crimes require greater deterrence." *Stewart*, 590 F.3d at 181 (Walker, J., concurring in part). This need for general deterrence is particularly heightened with respect to Schulte's crimes of espionage. As the Court heard repeatedly at trial, an element of trust is essential to the operations of our Nation's clandestine services. (*See, e.g.*, 2022 Tr. at 457, 516-21, 1403, 1683 ("[E]verything in the intelligence business is about trust.").) Concomitant with that reliance, however, is the need for stern penalties for breaches of that trust. Those who swear an oath to defend this country and to protect its secrets must know that they do not have the right to jeopardize the security of all of us simply to serve some personal end, as Schulte did. And adversaries must be put on notice that breaches of that security will be punished to the fullest extent of the law. Given the extraordinary nature of Schulte's crimes, general deterrence demands a substantial sentence.

Moreover, that sentence is necessary both to incapacitate and deter Schulte specifically from committing future crimes. Schulte dismisses the need for "any additional term of imprisonment" to serve this factor, in light of his conditions of confinement and his purported inability to commit future crimes of espionage. (Schulte Ltr. at 14). But that simply ignores his very pattern of conduct. Arrest did not deter Schulte. Revocation of his bail did not deter Schulte. Court orders and explicit reminders from the Court did not deter Schulte. The imposition of SAMs served to incapacitate, but not to deter, Schulte. These measures all merely gave him another source of festering grievance, another reason to retaliate against the country he once swore to protect. Schulte doubled down from jail, declaring his "information war," and committing the further crimes of espionage for which he also stands convicted. He has promised to do worse, to "look to breakup diplomatic relationships, close embassies, end U.S. occupation across the world." (2022 GX809 at 2.) Schulte compared his imprisonment to "taking a soldier in the military, handing him a rifle, and then begin beating him senseless to test his loyalty and see if you end up getting shot in the foot or not. It just isn't smart." (2022 GX820-430 & -431.) After having been

caught violating the Protective Order and being expressly warned by Judge Crotty and affirming his understanding of the Protective Order, he chose to violate that order and the law—simply because it served his purpose to do so.

The Court is already well familiar with the need to incapacitate Schulte. After this Court denied Schulte's renewed application for bail on December 20, 2021, the Second Circuit affirmed, in an opinion that "discussed—and endorsed—the district court's thorough analysis of the 'overwhelming evidence' of Schulte's dangerousness," taking into account the "sophisticated theft and dissemination of highly classified information, his violations of protective orders, and his continued disclosures and attempted disclosures of classified information, even from jail." *Schulte*, 2022 WL 1316210, at *2-4. Indeed, by returning a guilty verdict against Schulte, the jury found beyond a reasonable doubt that Schulte engaged in, among other things, this very conduct. Schulte's continued sense of grievance, and his unquenched need to vindicate it, was palpable during his trials, as the Court even observed. (2022 Tr. 685 (noting that Schulte was "making clear to the jury that even today you remain aggrieved by you as being mistreated").)

Nor has Schulte's misconduct stopped there, as the Court is also aware. Schulte's discovery laptop at the Metropolitan Detention Center ("MDC") had evidence of unauthorized usage, including changes to the system settings, and the creation of a large, encrypted partition, which led to the issuance of a warrant authorizing the FBI to seize and search the laptop. (PSR ¶¶ 109-10.) As a result of that review, the FBI found multiple files depicting child pornography, as well as forensic artifacts reflecting that files containing child pornography were accessed and viewed in a media player from Schulte's prison discovery laptop at MDC, including during his 2022 trial. (D.E. 1093.) It appears likely that Schulte obtained this contraband by abusing his access to the Courthouse Sensitive Compartmented Information Facility ("SCIF"), where CSAM discovery was made available to him under strict controls and monitoring that Schulte set out to evade, and in fact evaded. Schulte has also repeatedly threatened to continue to disclose classified information in his various post-trial filings. In January 2023, Schulte filed a Rule 29 motion describing how he "retains so much real national defense information that would be extremely damaging to the national security of the United States." (D.E. 992 at 23-24.) In that same filing, Schulte wrote, "If and when Mr. Schulte ever decides to wage a war against the United States, he could easily cause true, catastrophic damage." (*Id.*) Similarly, in May 2023, Schulte filed a letter complaining about lack of SCIF access, which claimed that "if the Court prevents Mr. Schulte from using the SCIF to write potentially classified information or from bringing his material to be reviewed by standby counsel in the SCIF, then the protective order is essentially null and void—and neither the court nor the government can blame or take action against Mr. Schulte for any incidental disclosure of classified information." (D.E. 1040.)

In short, Schulte has repeatedly both demonstrated and affirmed his desire to unlawfully disclose whatever classified information he may still know, an intent to do so to harm the United States in revenge for perceived wrongs against him, a craving to continue to view and access child pornography in spite of even the severe restrictions made necessary by his conduct, and a willingness to simply defy rules and orders to get what he wants. Schulte has repeatedly shown the Court who he really is—the Court should believe him. He did not engage in defiance once, twice, or even three times, but over and over again. His pattern of unlawful conduct makes clear that only total incapacitation will suffice to protect the public from his continued crimes.

D. Schulte's History and Characteristics Do Not Warrant Leniency.

As set forth in the PSR and in the letters from Schulte's family members, he enjoyed a comfortable upbringing in which he was afforded almost every advantage. He grew up in a loving home, surrounded by those who cared about him, provided with excellent education, and able to pursue whatever career he sought in life. It is indeed laudable that he chose to enter public service and seek to protect our national security. But these factors do not warrant leniency—if anything, they serve to highlight the enormity of the extraordinary crimes he perpetrated for no reason other than vindictiveness and ego and serve as a militating factor *against* leniency. Schulte did not commit his crimes from desperation—he knew no poverty that would drive him to crime, no abuse that would warp his sense of right and wrong, no injustice that made him a victim. Indeed, when he experienced setbacks at the CIA, he chose to reject the familial support network that has bravely continued to support him. He did not call his mom to vent about a boss he didn't like; he did not take advantage of his education and skills to pursue a different career; he chose to burn our nation's security to the ground because he did not get his way. The perseverance of Schulte's family is a credit to them—Schulte's rejection of them and their values only highlights the severity of his crimes.

Moreover, the evidence at Schulte's trials has revealed a different side of him that he hid from his closest family and friends. For example, they make no mention, and were presumably unaware, of his large collection of violent CSAM. Even while Schulte's family was traveling to attend his trial in 2022, he chose to retreat to his cell to view the child pornography that he had secreted on his prison laptop. (*See* D.E. 1093-1 at 3-4 (describing examples of times when videos were played).) The positive attributes that Schulte has shown to his family are certainly something the Court should take into account, but "the true test of a man's character is what he does when no one is watching."[9] When he thought no one was watching, Schulte sought to derive vengeance by torching some of the most vital tools of our national security, and to obtain gratification by reliving some of the most horrifying moments of young children's lives. Neither Schulte nor his loved ones make any effort whatsoever to grapple with that conduct. Indeed, reading Schulte's sentencing submission and the letters submitted along with it, one might almost be unable to determine what offenses he has been found guilty of committing. He has shown no remorse in any setting, and nothing in his history would explain, much less justify, his conduct.

Schulte and his family members also cite to what he calls "an undiagnosed neurodivergence" akin to Autism Spectrum Disorder ("ASD"), and speculates that it is "impossible to know how Mr. Schulte's life, and quality of life, would have changed if he had been treated." (Schulte Ltr. at 11-12.) That suggestion is as offensive as it is unhelpful. As Schulte concedes, he has not been diagnosed with anything, and no records support his claim other than observations that his antisocial behavior might be consistent with that diagnosis. Whatever difficulty Schulte may have had "fitting in," it certainly did not inhibit his ability to perform in school, to form close relationships with family and friends, and to work productively, and to offer merely that he "struggles socially" provides no basis for a "significan[t] downward variance" (Schulte Ltr. 13-14.) This proffer too fails to grapple with the nature—and scale—of the conduct in which Schulte engaged. At most, it is pure speculation to suggest that Schulte's conduct is somehow linked to a

[9] Commonly attributed to John Wooden.

disorder that he might or might not have. And it is offensive to the many people who lead productive, law-abiding lives with even severe ASD for Schulte to offer the pregnant implication that, if he had been diagnosed with ASD, that would somehow explain, and mitigate how he came to commit one of the gravest crimes of espionage in American history.

E. The Conditions of the Defendant's Confinement Do Not Warrant a Reduction in His Sentence.

A significant portion of Schulte's submission is devoted to his claims that his sentence should be reduced because of the conditions of his confinement at the MCC and, later, the MDC, focusing almost entirely on the SAMs to which Schulte has been subject. (Schulte Ltr. at 1, 7-11.) What Schulte completely omits, however, is that the imposition of those SAMs is entirely a product of his own continued criminal conduct. After being charged in this case, Schulte's initial application for bail was granted by Judge Crotty, and he remained at liberty from September through December 2017. His bail was only revoked after Judge Crotty found that Schulte had violated his bail conditions by, at a minimum, using his cousin to evade restrictions on his use of the Internet, including continued use of Tor throughout his period of release. Once detained, Schulte was not reflexively subjected to SAMs or segregation—he resided in general population with other inmates. But there too, Schulte treated the rules as a challenge to be beaten or overcome. He procured contraband cell phones, established covert communications accounts, and violated court orders and committed further crimes of espionage from his jail cell. It was only after Schulte was charged with committing these further crimes that SAMs were imposed on October 26, 2018—in direct response to his own conduct.

Moreover, "Schulte has subsequently exhausted—and re-exhausted—seemingly every possible judicial avenue to try to rid himself of these restrictions." (D.E. 552 at 2.) On May 10, 2019, Schulte, through his attorneys at the time, moved to vacate the SAMs, arguing that the SAMs were unconstitutional and not reasonably necessary to prevent the disclosure of classified information. (D.E. 92.) Judge Crotty largely denied Schulte's motion, granting the motion only in limited respects regarding certain communications involving non-attorney members of his legal team and monitored contacts with non-immediate family members. (*See* D.E. 127.)

Judge Crotty made clear that the SAMs were warranted based on Schulte's pattern of escalating disclosures and continued threat to disclose more:

> The SAMs are undoubtedly restrictive, but generally they are reasonably necessary to avoid further disclosure of classified information. Despite escalating restrictions on Schulte's freedom prior to his isolation in 10 South, Schulte continued to flout Court orders and his bail conditions, protective order, BOP rules, and procedures for handling classified information. If the Government's allegations against Schulte are true, Schulte intended to engage in an information war which would involve leaking classified information to the news media. Restrictive measures needed to be placed on Schulte to prevent unauthorized disclosure of classified information.

(*Id.* at 8.)

On June 24, 2021, Schulte, again through his then-attorneys, filed a second motion to vacate the SAMs. (*See* D.E. 474.) On October 6, 2021, Judge Crotty denied Schulte's motion in its entirety. (*See* D.E. 527.) The Court held that Schulte had "failed to undermine the original factual underpinnings for the SAMs." *Id.* Rather, "[t]o the contrary, since the SAMs were imposed, Schulte, inter alia, has been convicted of violating this Court's protective orders, and has intentionally disclosed information he knows to be classified—including in a recently publicly-filed motion seeking declassification of that very information." *Id.* Accordingly, the Court held, "as it did in 2019, that the SAMs are justified by a demonstrable danger that Schulte will disclose classified information." *Id.* (alterations and internal quotation marks omitted). Indeed, Judge Crotty specifically considered the potential effect on Schulte's mental health that his sentencing submission now reiterates at length, *see id.* at 3 and n.3, but rejected the implication that this warranted removal of the SAMs, noting that "these measures, although hard, are reasonably related to legitimate penological objectives," citing the fact that Schulte is "continuing his troubling pattern of disrespect for the Court's protective orders and other directives regarding classified information." *Id.* at 3. Schulte appealed Judge Crotty's ruling; the Government moved for summary affirmance of Judge Crotty's ruling upholding the SAMs, which the Second Circuit granted on December 15, 2022. *United States v. Schulte*, No. 21-2877, Dkt. 142 (Dec. 15, 2022), *cert. denied,* June 26, 2023.[10]

Even more broadly, throughout this case, the Court has taken acute care to monitor the conditions of Schulte's confinement, and to take steps to ensure that it does not infringe on Schulte's rights as a defendant. Thus, although under SAMs, Schulte has nevertheless been afforded extraordinary accommodations, including—prior to the 2022 trial—frequent visits to the Courthouse SCIF, access to a laptop in his cell, special provisions to expedite certain of his mail, and others. Schulte has, however, found ways to abuse even these accommodations, and continue to threaten to cause further harm to national security in spite of the SAMs. As discussed above, Schulte abused his access to a discovery laptop to continue viewing child pornography while in jail, and has threatened in multiple filings that he still retains the capacity to "wage a war against the United States, [in which] he could easily cause true, catastrophic damage." (D.E. 992 at 23-24.)

Schulte thus stands decidedly apart from defendants to whom downward variances have been granted to account for conditions of their confinement that were neither individually applied nor particularly justified. For example, in this Court's opinion in *United States v. Chavez*, No. 22 Cr. 303 (JMF), 2024 WL 50233 (S.D.N.Y. Jan. 4, 2024), the Court highlighted as problematic that "inmates at the MDC spend an inordinate amount of time on 'lockdown,'" and that while "[c]onfining inmates to their cells in this manner may have been justified during the height of the COVID-19 pandemic to prevent the spread of a deadly disease[, . . .] that is no longer the case." *Id.* at *4-5. Here, by contrast, Schulte's comparative isolation under SAMs is, as the Court has repeatedly found, a necessary individualized response to the continued threat to national security that he poses. The Court has rightly taken substantial interest throughout this litigation in ensuring

[10] Schulte has continued to litigate his conditions of confinement, and the application of the SAMs in particular, through a petition pursuant to 28 U.S.C. § 2241 that is currently pending in the Eastern District of New York. *See Joshua Adam Schulte v. United States of America*, 22 Civ. 766 (ERK) (E.D.N.Y.).

that the Bureau of Prisons lives up to its obligations to provide adequate treatment for those it houses, particularly as applied to the defendant. But it is indeed perverse for Schulte to now argue that the severity of his individual conditions of confinement, which have been imposed and escalated only because every attempt at lesser strictures proved insufficient to prevent him from committing further crimes, justifies leniency that will result in him receiving less incapacitation overall.

F. A Guidelines Sentence of Life Imprisonment Will Not Create Unwarranted Sentencing Disparities.

In evaluating "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct," 18 U.S.C. § 3553(a)(6), it is challenging to identify appropriate comparators for Schulte's offenses. As repeatedly observed, his crimes of espionage are by volume some of the largest ever committed in American history, and their damage to national security concomitantly severe. Moreover, Schulte was convicted of violating 18 U.S.C. § 793(b), which required the Government to prove as an element that Schulte had the "intent or reason to believe that the information [that he stole] *would* be used to the injury of the United States, not just that it *could* be so used." (D.E. 879 at 28.) Those two facts: the scope of information stolen in Schulte's offense and his motive in so doing set him apart from the comparators that Schulte tries to offer. For example, Schulte cites to the 63-month sentence imposed in *United States v. Reality Winner*, 17 Cr. 034 (JRH) (S.D. Ga.).[11] But there, the defendant printed and mailed to a media outlet a single intelligence report and accepted responsibility for "my . . . crucial betrayal of my nation's trust placed in me." (17 Cr. 034 D.E. 328 at 10, 18 (sentencing transcript).). Likewise, in *United States v. Jeffrey Sterling*, 10 Cr. 485 (LMB) (E.D. Va.), on which Schulte also relies, the defendant disclosed information to a reporter pertaining to one particular classified program and asset, the Court did not "think there's any danger . . . that [the defendant was] going to recidivate," and was not convicted under § 793(b) so the only proof required was that "the disclosure was potentially damaging to the United States." (10 Cr. 485 D.E. 475 at 8, 24-25).

Indeed, it is the proof that Schulte carried out his conduct with the specific intent that his theft *would* harm the United States that sets his case apart. In virtually all cases identified in the Government's research in which violations of § 793(b) have been prosecuted, that charge has been paired with violations of 18 U.S.C. § 794, which penalizes the delivery of national defense information to a foreign government with the same intent requirement. That offense does not apply to Schulte's conduct, because he chose to transmit the Stolen CIA Files to WikiLeaks, rather than directly to a foreign state. But Schulte's intent to harm the United States, the scope of his theft and disclosure, and the consequences of his conduct, more closely parallels cases prosecuted under § 794 than so-called "leak" cases in which comparatively small amounts of information are shared with media organizations with a misguided sense of the public interest. In such cases, Courts have routinely, albeit gravely, concluded that terms of life imprisonment are the only appropriate sanction for such devastating crimes, notwithstanding the fact that many similarly situated individuals accepted responsibility for their crimes. *See, e.g.*, *United States v. Robert*

[11] In addition to the differences discussed herein, that sentence was also the term stipulated to by the parties in that case pursuant to a plea agreement under Fed. R. Crim. P. 11(c)(1)(C).

Hanssen, 01 Cr. 1088 (E.D. Va. 2002) (life imprisonment for FBI supervisor who pled guilty to selling classified information to Russia); *United States v. Aldrich Ames*, 94 Cr. 166 (E.D. Va. 1994) (life imprisonment for CIA officer who pled guilty to selling classified information to Russia); *United States v. Arthur James Walker*, 85 Cr. 92 (E.D. Va. 1985) (life imprisonment for former Navy officer convicted of selling documents for transmission to Russia); *United States v. Andrew Daulton Lee*, 589 F.2d 980 (9th Cir. 1979) (life imprisonment for contractor convicted of selling classified information regarding CIA project to Russia).

It is, in some sense, fortunate that there are comparatively few examples of individuals who have chosen to betray the United States as completely and vilely as Schulte did, with the particular intention to harm the nation they swore to protect. Schulte's motive in doing so—to wreak vengeance in return for petty slights that existed only in his imagination—was just as venal as those who sold secrets to line their own pockets. The consequences of his disclosures were every bit as grave—after all, as discussed further in the CCI Letter, by disseminating the Stolen CIA Files to WikiLeaks, Schulte not only gave closely guarded national defense information to one adversary, he gave it to every adversary that was a target of CIA cyber operations, with cascading effects perhaps greater than merely betraying our country to a single hostile power. In those few cases in which the scope, harm, and intent of the conduct at issue are analogous to this, courts have rightly found that life imprisonment is the appropriate sentence under the Section 3553(a) factors. This Court should reach the same conclusion for Schulte.

V. Conclusion

For these reasons, the Government respectfully submits that a Guidelines sentence of life imprisonment is the only sentence sufficient to achieve the objectives of sentencing.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

by: /s/
David W. Denton, Jr. / Michael D. Lockard /
Nicholas S. Bradley
Assistant United States Attorneys
(212) 637-2744 / -2193 /-1581

cc: Defense counsel (by ECF and hand through the Classified Information Security Officer)