STEPHANIE M. HINDS (CABN 154284)
Attorney for the United States
Acting Under Authority Conferred by 28 U.S.C. § 515
THOMAS A. COLTHURST (CABN 99493)
Chief, Criminal Division

ANDREW F. DAWSON (CABN 264421)
BENJAMIN KINGSLEY (CABN 314192)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-314192
FAX: (415) 436-7019
andrew.dawson@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JOSEPH SULLIVAN, Defendant.	CASE NO. 20-337 WHO UNITED STATES'S SENTENCING MEMORANDUM

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

GUIDELINES PROVISIONS

Defendant Sullivan was found guilty by a jury of two felonies: obstruction of an official proceeding of the Federal Trade Commission ("FTC") and misprision of a felony. As a necessary component of its verdict, the jury found that Sullivan "intentionally endeavored corruptly to influence, obstruct, or impede" the FTC's investigation into Uber Technologies, Inc. ("Uber"). Dkt. No. 219, at 17. The evidence at trial demonstrated that Defendant Sullivan prioritized his and his employer's selfish interests over the clear legal obligations owed to the FTC, and he thereby undermined the FTC's mission of protecting consumers. As this Court knows from the trial evidence, this case is not about the undisputed merits of bug bounty programs. It is not about difficult decisions made every day by cybersecurity professionals around the world. And it is not about a good-faith error made in the midst of a stressful security incident. Indeed, while the case arose in the context of cybersecurity incident, it is not ultimately about the details or merits of cybersecurity practices. Rather, it is about a powerful person's intentional exploitation of his position to cover up a deeply embarrassing event—an event that also happened to be a crime—over the span of nearly 12 months. Sullivan, a senior corporate executive with years of experience in both cybersecurity and the criminal justice system, harnessed the resources of a multinational corporation to silence witnesses, generated fraudulent corporate paperwork, ratified false statements to the FTC, and lied to Uber's new CEO and internal investigators. The government does not dispute any of Defendant's good deeds or general moral qualities as reflected in the many letters submitted on his behalf. Those same moral qualities only underscore that Defendant knew how wrong his conduct was, and the case stands as shocking proof that even such a revered figure in his community will resort to criminal activity when his reputation is on the line and he thinks no one is watching.

Every day in boardrooms across the country, corporate executives are faced with legal obligations that conflict with their self-interest. This is particularly so during government investigations: the investigated would prefer that damaging information not be uncovered. In most cases, neither the government nor the public has any visibility into decisions made behind the boardroom door. There is even less visibility when, as here, the decision-makers include attorneys whose communications are typically shielded from view. Unavoidably, we are left to trust that the people in those rooms will do the right thing, even when nobody is watching and even when it makes them look bad. Defendant Sullivan,

by all outward appearances, appeared to be well equipped to validate that trust. He failed. Instead of doing what he knew was the right thing, he engaged in a rigorous effort to ensure that the victims, the FTC, law enforcement, and the public never learned that he and his cybersecurity team had made mistakes that allowed two hackers to steal personal information associated with more than 50 million victims. Part of this Court's task is to ensure that every other well-connected corporate executive in a similar position, in the cybersecurity world and elsewhere, knows that the sanction for such a failure will be significant and meaningful. Given how rarely such decisions even come to light, the only adequate sanction is prison time. The government therefore recommends that the Court sentence Defendant to 15 months in prison.

I. The Evidence

After presiding over trial in this matter, the Court is no doubt quite familiar with the facts of the case. The government revisits certain facts here because they are critical to the Court's task at sentencing, and because those facts remain obscured from the public at large as a result of Defendant's own years-long misinformation campaign about what actually happened at Uber from November 2016 to October 2017. Many of the letters submitted on Defendant Sullivan's behalf evince that same widespread misunderstanding of the facts and of the evidentiary basis for the jury's verdicts—a misunderstanding that clearly originates with Defendant's own self-serving narrative that he first relied on when he was interviewed by internal investigators in August 2017. While the Court should—indeed must—take into account Defendant Sullivan's personal history and circumstances, the Court should not base its sentence on the false claim that Defendant Sullivan is being unfairly punished for a run-of-the-mill cybersecurity incident in which his good-faith actions are being unfairly second guessed. That claim is patently inconsistent with the evidence and with the jury's verdict, and it dangerously undermines the public-private partnerships that are necessary to enhance this country's cybersecurity.

Defendant Sullivan was hired by Uber in April 2015 to take control of its security apparatus in the wake of a 2014 data breach at the company (the "2014 Data Breach"). Within days of joining the company, Sullivan received a copy of the Federal Trade Commission's Civil Investigative Demand ("CID"). *See* Exhibit 275. That CID related in large part to the 2014 Data Breach, but it reflected that the scope of the FTC's investigation extended to Uber's entire cybersecurity program for protecting

consumer data. *Id.* Over subsequent months, Uber began issuing written responses to the FTC and producing documents. In a response dated September 25, 2015, Uber informed the FTC that Defendant Sullivan and John Flynn, who was Defendant's direct report, "supervised the preparation of Uber's response to this CID." Exhibit 292. In March 2016, Sullivan and Flynn travelled to Washington, D.C. to give a presentation to the FTC regarding Uber's cybersecurity program. Tr. at 338-39 (Rossen). Ben Rossen, who led the FTC investigation at that time, testified that the presentation communicated "the changes that had been implemented at Uber since Mr. Sullivan took over as CSO." *Id.* at 344:9-10. During the presentation, Sullivan addressed a number of more minor security issues that had occurred since the 2014 Data Breach. *Id.* at 346-49. On November 4, 2016, Defendant Sullivan sat for sworn testimony in an FTC investigational hearing. That testimony included in-depth analysis of Uber's data security practices as they related to the FTC's investigation—both those in place at the time of 2014 Data Breach and at the time of his testimony—such as encryption of personal data related to drivers and customers and how Uber stored its access keys for the company's Amazon Web Services ("AWS") data repositories. *See* Exhibit 340.

Ten days after his testimony, Sullivan learned that Uber had been breached again (the "2016 Data Breach"), due to some of the same deficient security practices that had led to the 2014 Data Breach, resulting in a loss of customer and driver data that dwarfed what was taken during the 2014 Data Breach. Contemporaneous business records establish that Defendant almost immediately recognized that this second breach revealed that Uber's prior representations to the FTC about encryption practices and the scope of Uber employees' access to such data —including those Defendant had made under oath—had been false. *See* Exhibit 29 (Preacher Tracker) at 11 ("Joe: This may also play very badly based on previous assertions."); *id.* at 18 ("Joe was just deposed on this specific topic and what the best or minimum practices that any company should follow in this area."); *see also* Tr. (Garbutt) 797:18-22 (testifying that "previous assertions" refers to prior assertions made to the FTC about data controls and access at Uber—assertions proven incorrect or incomplete by the 2016 Data Breach). Defendant then set about ensuring that the FTC never learned the truth, either about the 2016 Data Breach itself or the security vulnerabilities that had allowed it to happen. John Flynn testified that early in the 2016 incident response efforts and in the context of a conversation about the FTC's

investigation and Defendant's prior sworn testimony, Defendant directed him unequivocally that "this can't get out." *Id.* (Flynn) 604:2-22.

Subsequent events demonstrate Defendant's calculated efforts to conceal the incident, which included both lies to his team and the creation of false and misleading corporate documents. The Preacher Tracker,[1] for example, records Defendant's attempt to ensure that nobody on his team breathed a word about the breach outside the security group: "Joe Comments: 1. Information is extremely sensitive and we need to keep this tightly controlled. Discussion with other Engineers must be tightly controlled. Joe is communicating directly to the A-Team." Exhibit 29 at 14. Defendant's claim that he was "communicating directly to the A-Team" was a lie designed to create the impression that all relevant corporate stakeholders, to include the company's General Counsel, had been informed about the breach. The false claim had its desired effect: another of Defendant's direct reports, Craig Clark, testified that he understood Defendant to be claiming that, at a minimum, the General Counsel (Salle Yoo) and the Chief Technology Officer (Thuan Pham) were in contact with Defendant. That was not true. *See* Tr. (Yoo) 1608:9–14; id. (Pham) 1822:3–16.

Clark further testified that after the team had learned that 600,000 driver's license numbers had been stolen in the 2016 Data Breach, Defendant directed him to come up with a way to conceal the breach by falsely portraying it as a standard interaction with security researchers within Uber's bug bounty program. Tr. (Clark) 1320:2-6; 1320:19–24. At this time, the terms of Uber's "bug bounty" program clearly excluded the precise technique employed by the hackers. Exhibit 16 at 4 (excluding from program "use of AWS access key to dump user info"). Following Defendant's direction, Clark nonetheless communicated a potential theory to Defendant, which involved pretending that the extortive hackers were instead somehow, "nunc pro tunc," agents of the company. *Id.* (Clark) 1322:3–14. Defendant then reported back to Clark that the "A-Team" had decided to treat the incident as a bug bounty. This, of course, was a lie, since the broader A-Team, distinct from just the company's CEO, had not even been informed of the 2016 Data Breach.

Defendant's decision to treat the 2016 Data Breach and accompanying $100,000 extortion

[1] The Court will recall the Preacher Tracker, which was a Google document used by Defendant's team to record, in real time, the response effort to the 2016 Data Breach. *See* Exhibit 29.

payment as a bug bounty report was, in reality, a convenient mechanism to draw attention away from the incident, to make it appear to be a matter of little importance, and to find a convenient way to pay the hackers' extortion demand and buy their silence. For example, had Defendant truly believed it fit within the bug bounty program, there would have been no reason to direct Craig Clark to introduce demonstrably false language in the draft Non-Disclosure Agreement ("NDA") with the hackers. Exhibit 144 ("You promise that you did not take or store any data during or through your research . . . ." (emphasis added)); Tr. (Clark) 1345:9–10 (Q: Whose idea was that language?; A: That was Joe's idea."). That lie had no purpose other than to minimize the significance of the 2016 Data Breach and to make it appear to fit within the bug bounty program. Defendant knew that this language was in the NDA and knew it was a lie. His knowledge was amply demonstrated both by his extensive line edits to the document (Exhibits 100 through 115) and his later blatantly false statements to Randall Lee and other outside counsel for Uber, where he falsely claimed he did not "remember the details" of why a separate NDA was drafted and that he "wasn't involved" in drafting the NDA. Exhibit 1111 at 8; *see also* Tr. (Lee) at 2182:21–2183:14 ("My recollection is that he essentially said he didn't have any role in it.").

Defendant's understanding that the data breach could not legitimately be treated as a bug bounty disclosure was further demonstrated when he rewrote language for an email to Dara Khosrowshahi, who was appointed as Uber's new CEO in August 2017, in which Defendant deleted information establishing that the 2016 Data Breach had, in fact, been a massive data breach. Exhibit 212 (Consolidated Preacher Report Google document version with Sullivan edits); Exhibit 218 (later version with more Sullivan edits). Among other lies about the circumstances of the 2016 Data Breach response, Sullivan's email to Khosrowshahi falsely suggested that the hackers responsible for the 2016 Data Breach had never actually taken any data, let alone personally identifiable data ("PII"), and that they had been identified before they were paid. Exhibit 623. Of course, the evidence showed that the hackers had in fact stolen vast quantities of PII and were paid $100,000 when they were still anonymous, on the condition that they not tell anyone else what they had done. In other words, having instructed his team to keep silent about the breach, Defendant then paid hush money to the hackers to ensure that they never disclosed what they had done. *See* Exhibit 144 ("You promise that you have not and will not disclose anything

about the vulnerabilities or your dialogue with us to anyone for any purpose without our written permission."). Such an agreement was unprecedented within Uber's bug bounty program, and Rob Fletcher testified that he could not recall such an agreement in any other bug bounty program in which he had participated. Tr. (Fletcher) 973:19–23. Defendant's insistence on such an agreement further supports the jury's finding that he was acting to conceal and cover up the breach.

Evidence of Defendant's intent to obstruct the FTC investigation continued even into the spring and summer of 2017. Most damningly, Defendant received via email a summary of the FTC's initial draft of settlement documentation, in which it was apparent that the FTC was relying on false claims previously provided by Uber—claims proven to be false by the 2016 Data Breach itself. *See* Exhibit 703. There can be no dispute that Defendant read the email, as he drafted and sent a lengthy response. *Id.* But, in this response, Defendant omitted any reference to the fact that Uber had falsely told the FTC that it had ceased storing unencrypted personal information on AWS after March 2015, and that the FTC was relying on this false representation in negotiating a settlement. Defendant, of course, knew that the truth was far worse: unencrypted personal information remained on AWS until at least November 2016, when two hackers stole a huge quantity of that data.

Finally, evidence of Defendant's intent was extensively demonstrated by his many lies during his interviews with Randall Lee and other outside counsel for Uber, who were conducting an internal investigation. These lies—which the letters submitted by Defendant demonstrate have been adopted by many in the cybersecurity industry, despite the sworn testimony at trial and verdict in this matter—were motivated by a guilty conscience and Sullivan's awareness that he had corruptly obstructed the FTC proceeding. For example, during those interviews, Sullivan told false and shifting stories about the legal justification for not disclosing the data breach to the FTC. *See, e.g.*, Exhibit 1051 at 9 (during an August 2017 interview, Sullivan said he did not disclose the breach "Because we were able to ensure that no data was out in the wild"); Exhibit 1055 at 7 (September 2017 interview, said decision not to disclose was "Same call we made 100 times"); Exhibit 1111 at 2 (October 2017 interview, said he did not recall discussing the "issue of disclosure" and that he hadn't "reviewed" Craig Clark's "work" on the "legal issues, analysis that needed to be done" on disclosure). He lied about where he was during the incident response. Exhibit 1055 at 3 ("Not physically part of the team"), *id.* at 7 ("That week I wasn't at 555,

was in prep, in east coast."). He refused to answer as to "what PII was at stake" and falsely said he "wasn't involved" in the analysis of whether the incident was a reportable data breach. Exhibit 1111 at 6; *see also* Exhibit 29 at 13, 15–16, 17, 20–21 (evidencing that Defendant repeatedly asked about and was told what data and PII was stolen). In response to a question about whether he remembered "discussions with any other a-team member about this incident," he falsely said that they "Went big very fast." Exhibit 1111 at 3. *Compare with* Exhibit 29 at 9–10 (Preacher Tracker statement that: "Our common story has to be: -This investigation does not exist."). And, as noted above, he lied about his role in both the inception of the NDA and its drafting. Exhibit 1111 at 8.

Ultimately, the breach was disclosed to the FTC and to the public in November 2017 by Uber's new leadership. The FTC's lead investigator, Ben Rossen, testified that when Uber's counsel belatedly informed him of the new breach in November 2017, it was "probably the single most frustrating experience that I had at my time at the Federal Trade Commission." Tr. (Rossen) at 445:3-5.

II. Guidelines Calculation

As noted in the Presentence Report, the applicable guideline is U.S.S.G. § 2J1.2, which provides a base offense level of 14. As explained further below, the government believes two enhancements apply: (1) a three-level increase pursuant to § 2J1.2(b)(2) because the offense resulted in substantial interference with the administration of justice, and (2) a two-level increase pursuant to § 2J1.2(b)(3)(C) because the offense was extensive in scope, planning, or preparation.[2] The government also does not oppose a two-level downward variance to account for an anticipated amendment to the Guidelines that, if it were in effect today, would result in a two-level downward adjustment to the overall offense level.

A. The Court should apply a three-level enhancement because of Defendant's "substantial interference with the administration of justice".

The government agrees with Probation's application of a three-level enhancement under Section 2J1.2(b)(2), which applies upon a showing that "the offense resulted in substantial interference with the administration of justice." The application notes to Section 2J1.2 provide that this category "*includes* a premature or improper termination of a felony investigation; an indictment, verdict, or any judicial

[2] While the probation officer initially agreed that this enhancement should apply, the final PSR removed it from the calculation. *See* PSR Addendum, ¶ 1.

determination based upon perjury, false testimony, or other false evidence; or the unnecessary expenditure of substantial governmental or court resources" (emphasis added). The Application Notes do not provide a limiting definition of the term, but rather an illustrative list. And in any event, courts "ascribe somewhat less legal weight to the Application Notes than to the Guidelines proper: if the Guideline and Application Note are inconsistent, the Guideline prevails." *United States v. Kirilyuk*, 29 F.4th 1128, 1136 (9th Cir. 2022) (quoting *United States v. Prien-Pinto*, 917 F.3d 1155, 1157 (9th Cir. 2019)).

The evidence recounted above establishes that Defendant's conduct resulted in substantial interference with the administration of justice in at least two ways—one, targeting the FTC and its agency proceedings, and two, targeting the FBI. First, by not reporting the entirety of the 2016 Data Breach to the FTC, Sullivan prevented the FTC from learning that the event had happened at all. As a result, his obstruction caused the improper and premature termination of the FTC's investigation and a settlement with the FTC based on false evidence. In the context of § 1505, which targets obstruction of administrative agencies generally, these are directly analogous to the judicial circumstances described in the Application Notes—"the premature or improper termination of a felony investigation" or a "judicial determination based upon . . . false evidence."

Second, Defendant not only hid a data breach, he covered up a crime—and his conviction for misprision of a felony reflects the seriousness of that conduct. The 2016 Data Breach was a serious crime, and one for which both Brandon Glover and Vasile Mereacre ("the Hackers") were subsequently prosecuted. Rather than comply with the law, Defendant Sullivan sought to cover up that crime by paying the Hackers $100,000 in exchange for their silence. Defendant realized that the FBI and federal law enforcement authorities would be acutely interested in such a hack, and documentary evidence reflects Defendant's goal that evidence of the hack be withheld from the FBI. See Exhibit 195 at 1 (reflecting the goal that the hacked data not be "caught up in that [FBI] seizure"). By purchasing the hackers' silence, Defendant Sullivan "prevented proper legal proceedings from occurring by taking matters completely outside the purview of the administration of justice." *United States v. Amer*, 110 F.3d 873 (2d Cir. 1997).

//

B. The Court should apply a two-level enhancement because Defendant's obstruction was "extensive in scope, planning, or preparation".

Section 2J1.1 separately includes a possible two-level enhancement for three categories of offenses. The enhancement applies if the offense:

> (A) involved the destruction, alteration, or fabrication of a substantial number of records, documents, or tangible objects; (B) involved the selection of any essential or especially probative record, document, or tangible object, to destroy or alter; or (C) was otherwise extensive in scope, planning, or preparation . . . .

U.S.S.G. §2J1.1(b)(3). The text of the enhancement is structured with the first two categories, under (A) and (B), having specific definitions, with category (C) playing the role of a residual clause, applying to offenses that are "*otherwise* extensive in scope, planning, or preparation." *Id.*

Defendant's offense was extensive in scope, and the Court should apply the two-level enhancement. As noted in detail in the evidentiary summary above, Defendant harnessed the resources of a major, international corporation in order to accomplish his goals. From deploying surveillance teams in both the United States and Canada, to six-figure hush money payments, to falsified corporate documentation, to calculated lies told to corporate executives and internal investigators, the crime at issue here was undoubtedly extensive in scope.

Analysis of Subsection C in context with the rest of the enhancement buttresses this conclusion. As noted above, Subsection C is drafted as a residual clause, applying to offenses that are "otherwise" extensive in scope, planning, or preparation, which impliedly refers to the previous subsections. Subsection B, for example, applies to the alteration or destruction of "any essential or especially probative record, document, or tangible object." Section B therefore would apply to an offense involving the destruction of a single document, so long as that document was "essential or especially probative." While Defendant's conduct here did not focus on a single essential document or record, it did focus on suppression of "especially probative" evidence that would have been critical to the FTC's investigation: the existence of the 2016 Data Breach. As noted above, the FTC's investigation was triggered by the 2014 Data Breach and expanded to encompass a review of Uber's entire cybersecurity apparatus, with a particular focus on AWS and encryption of personal information. In that context, news of a new and larger data breach, which also highlighted AWS access and unencrypted personal

information, this time on a massive scale, was clearly "especially probative" to the FTC's investigation. Had Defendant and Uber disclosed the 2016 Data Breach promptly, it obviously would have been a hugely significant revelation and it would have changed the course of the investigation—as it ultimately did when the 2016 Data Breach was ultimately disclosed in 2017. If alteration of a single "especially probative" document is sufficient to trigger the enhancement, a twelve-month campaign to suppress evidence of an "especially probative" data breach is sufficient as well. The Court should therefore apply a two-level enhancement because Defendant's offense was "extensive in scope, planning, or preparation."

C. "Zero-Point Offender" variance.

The Sentencing Commission has proposed an amendment to the Guidelines, applicable to certain defendants with zero criminal history points, which would call for a two-level decreased in the offense level (specifically, Section 4C1.1). Probation has assessed that Defendant meets the criteria for the proposed amendment, but notes that the amendment is not set to take effect until November 2023. PSR ¶ 105.

While the amendment has not yet taken effect, the government does not oppose a two-level downward variance to account for the anticipated amendment.

As a result, the government recommend an adjusted offense level of 14 + 3 + 2 -2, which results in an Adjusted Offense Level of 17, which yields a Guidelines range of 24 to 30 months.

III. Argument

Congress has provided that a sentencing court must look beyond simply the individual standing before the Court at sentencing. Section 3553(a) requires the Court to consider the effect its sentence will have on others, both in terms of deterring others from similar crimes and in terms of promoting respect for the law. These considerations, applied to the facts of this case and the context in which it arises, call for a prison sentence.

A. White collar crimes are difficult to detect, and the prospect of incarceration is necessary to afford adequate deterrence.

Defendant Sullivan is not the first former Uber executive to stand before a court of the Northern District of California for sentencing. On August 4, 2020, approximately two months after the indictment

was returned in this case, Anthony Levandowski stood for sentencing before Judge Alsup, having pleaded guilty to one count of trade secret theft. As here, dozens of letters had been submitted on Levandowski's behalf, noting all the good qualities of his character. Levandowski's able counsel highlighted all the good deeds he had done through his life, including assistance offered to the government. Counsel went on to list all the collateral consequences that had already been visited upon Levandowski prior to sentencing, arguing that his fall from grace—including having been fired by Uber—was more than adequate to deter future crimes, and that prison time would be gratuitous and more than necessary. Defense counsel in this matter will no doubt offer up the same arguments here.

In that case, Judge Alsup acknowledged the mitigating import of those arguments, but he emphatically rejected the argument that prison time was unnecessary:

> The question is -- the key question here is deterrence and whether someone in the future, who is in Mr. Levandowski's position, with billions -- not just millions -- billions of dollars in some new technology are in play, and that person in the future, that engineer in the future, who, let's say, is brilliant, has the opportunity to go start their own company and they're thinking to themselves: "Do I steal these trade secrets so it'll give me a heads-up? Maybe I won't get caught" -- so they're factoring in the risk of detection – "and if I do get caught, well, they'll just give me probation like they gave Mr. Levandowski."

Case No. 3:19-cr-00377 WHA, Docket No. 102, at p. 43.

As Judge Alsup observed, deterrence in the white-collar context must account for the fact that sophisticated defendants know that their crimes must be uncovered before they can face any consequences. The concern applies with even more force in this case, where the crime at issue is precisely the effort to avoid detection, and where the participants know that their communications are shielded by legal privileges and are unlikely to ever see the light of day. Judge Alsup hit upon the only available answer: "Prison time is the answer to that." *Id.* at 44.

Defendant Sullivan, like Anthony Levandowski before him, has a spotless history. He is respected in his community. He is an innovator in his field. He is loyal to his friends and has supported those less fortunate. But, when given the opportunity to choose between himself and adherence to the law, he chose himself. Worse than that, Defendant Sullivan prioritized his and Uber's interests over those of the tens of millions of Uber users and riders who trusted their personal information to the company. He prioritized his and Uber's interests over the structural need for honesty and transparency in federal investigations. He undermined the ability of the FTC to fulfill its essential mission of

protecting American consumers. Corporate leaders are called upon to do the right thing even when it is embarrassing, even when it is bad for the company's bottom line. Nobody, neither corporations nor the executives who lead them, is above the law.

And Defendant Sullivan almost got away with it. If not for the fortuitous arrival of new leadership at Uber, there is every reason to believe the tens of millions of victims of the 2016 Data Breach never would have learned about it. This case is a cautionary tale of how many unwitting corporate employees can be enlisted into a coverup without even appreciating what is going on. Since knowledge of the FTC investigation and Uber's cybersecurity program was siloed within the company, a small number of people appreciated the significance of the 2016 Data Breach and what they were doing in response to that breach. Only Defendant Sullivan could see everything. That too is not uncommon in corporate America, particularly in large corporations, where visibility is broadest at the top, and those who report up do not necessarily see the full significance of their actions. Defendant Sullivan, like any corporate executive in his shoes in similar circumstances, would have every reason to think he could get away with it. Indeed, he almost did.

While the collateral consequences outlined by defense counsel are real, to the corporate executive acting in the moment, they are highly speculative. Companies like Uber and others in Silicon Valley have flourished based on an industry-wide willingness to take risk. But prison is a risk too far. As Judge Alsup observed, prison time is a deterrent like none other, and a sentence of custodial time in this case will communicate to others in the industry that the willful interference with government investigations, even when they are uncomfortable or costly, is not amenable to a cost-benefit analysis because the sanction—incarceration—is unacceptable. The government therefore recommends that the Court sentence Defendant to a prison term of 15 months.

B. A sentence of 15 months in prison promotes respect for the law.

Separate and apart from the goal of deterrence, a prison sentence in this case will promote respect for the law. There is a justifiable narrative in this country that corporate executives get away with criminal activity—and that when they are caught, because of their resources, they rarely face actual prison. As discussed above, given the extraordinarily difficult nature of detecting and prosecuting criminal activity by senior corporate executives, who like Defendant Sullivan in this very case, commit

their crimes under the cover of attorney-client privilege and have the power to cover it up, there is some truth in this. Probationary or token prison sentences for corporate executives in general undermine respect for the law and the criminal justice system at large, and disregard the core principle that all defendants are equal before the law regardless of their position and power.

Beyond this general concern, though, there is a very specific need in this case for a prison sentence that sufficiently sanctions Defendant for his conduct. One of the themes that becomes evident in reviewing the letters submitted on Defendant Sullivan's behalf is that many in the cybersecurity industry are not aware of the egregious conduct Defendant Sullivan has been proved guilty off—the witness tampering, the fraudulent corporate paperwork, the many lies. Letter after letter submitted to this Court suggests that this prosecution reflects simple second-guessing of a difficult decision, that Defendant Sullivan is nothing more than a scapegoat, and that neither the government nor the jury really understands cybersecurity. *See* Defendant's Sentencing Submission to Probation, Appendix 1, Ex. G, at 9, 10, 18-19, and 29; Ex. H at 003, Ex. I at 1, 3, 6-7, 11-12, 15, 17. As the Court is aware after presiding over the trial in this matter, none of this is true. Additionally, as the Court may be aware, this false narrative has the real potential to drive a wedge between the cybersecurity community and law enforcement at precisely a time when our country is facing an unprecedented array of cyber threats that require those two communities to work hand-in-glove.

Defendant Sullivan is solely responsible for seeding this false narrative nearly six years ago, when he began lying to Uber executives and investigators about the events surrounding the 2016 Data Breach and his role in those events. His defense at trial was premised on the same argument—that other people made difficult decisions under tremendous pressure and that he simply trusted they were following appropriate protocols under Uber's cybersecurity policies. The jury rejected that defense, but the false narrative remains visible in the letters submitted to the Court, buoyed by the esteem in which many in the cybersecurity hold Defendant Sullivan. The letter writers are no doubt sincere in their admiration for Defendant Sullivan, but Defendant has exploited that esteem, first by lying about his conduct, and now by permitting others to rely on those lies in their submissions to this Court.

A sentence of probation in this case would tacitly affirm those lies. It would, like Sullivan's unsuccessful defense at trial, suggest to the public that Defendant Sullivan simply made an innocent

mistake. That any wrongful conduct was minimal or inadvertent. That everything Defendant Sullivan has been saying since August 2017 was true. And that obstruction of a federal investigation designed to protect the broader public ultimately does not matter. A sentence of probation would also ratify the lie that this case represents some drastic change in standards applicable to the cybersecurity industry and the government's desire to partner with the private sector, including victims, in countering cyber threats. That is simply not the case. The case arises in the context of cybersecurity, but it is not about cybersecurity. It is about old-fashioned obstruction of justice, which has always been illegal, no matter what industry one works in. It is about hiding a felony from law enforcement, which has been a crime since the common law and which was codified into federal law in 1790 by the First Congress. *See United States v. Olson*, 856 F.3d 1216, 1221–22 (9th Cir. 2017). Just as the subject of a narcotics investigation cannot tamper with witnesses or evidence, neither can a chief security officer of a massive technology company under an FTC investigation. There should be nothing surprising in this. The scope of this case is thus far broader than Defendant would have it be, and the lines he crossed much clearer and more vivid than his supporters have been led to believe. A meaningful prison sentence is necessary to refocus the public—and the cybersecurity industry—on the truth and promote respect for the rule of law.

C. White-collar defendants are not entitled to special treatment.

Defendant Sullivan has submitted more than 100 letters penned by his friends and colleagues. Obviously, the Court should take into account all the laudatory things said about Defendant Sullivan in his other pursuits, which the government does not doubt are true and which are unrelated to his criminal conduct in this case. But the government notes that white-collar defendants in general, and successful corporate executives in particular, will almost always have deep networks of supporters to call upon in difficult times. One does not become an executive at a company like Uber without having such a network. Indeed, Anthony Levandowski made a very similar presentation to Judge Alsup prior to his sentencing.

These letters only underscore Defendant's extraordinarily privileged position among the many individuals the Department of Justice prosecutes—and the many defendants this Court sentences. They mainly demonstrate that Defendant is a wealthy, powerful man, with a strong network of family and

friends that has benefited him throughout his life. To place considerable weight on such submissions systematically privileges successful defendants over unsuccessful ones, wealthy defendants over impoverished ones, and defendants who had the means to make better choices over those with few other options. An undocumented drug dealer sentenced in federal court is unlikely to have had the opportunity to whitewash his criminal record by volunteering to help war-torn Ukrainians, nor the network or resources to make an extensive showing of other good deeds in his life, even if that individual is just as critical to his or her family and community. There cannot be two different systems of justice, one for the privileged and another for the rest. Any such perception would do grievous damage to public respect for the law, and it would be inconsistent with the values towards which our system of justice strives.

IV. Conclusion

For the foregoing reasons, the United States recommends that Defendant Sullivan be sentenced to 15 months in prison.

DATED: April 27, 2023

Respectfully submitted,

STEPHANIE M. HINDS
Attorney for the United States
Acting Under Authority Conferred by 28 U.S.C. § 515

_____/s/_____
ANDREW F. DAWSON
BENJAMIN KINGSLEY
Assistant United States Attorneys