TMS/NSD: USAO 2022R00343

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
	*	
v.	*	**CRIMINAL CASE NO. TDC-25-314**
	*	
JOHN ROBERT BOLTON, II,	*	
	*	
Defendant.	*	
	*	

****

GOVERNMENT'S UNCLASSIFIED SENTENCING MEMORANDUM

TABLE OF CONTENTS

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 2

A. Role of the National Security Advisor 2

B. Offense Conduct 3

1. Background 3

2. Mr. Bolton Publishes a Book about his Tenure as National Security Advisor 3

3. The Iranian Hack of Mr. Bolton's Personal Email Account 4

4. Classified National Defense Information Found at Mr. Bolton's Washington, D.C. Office and Maryland Residence, And Within His Electronic Devices and Accounts 4

C. Arraignment, Rearraignment and Guilty Plea 7

D. Guidelines Calculations 8

E. Bolton's Compliance with Plea Agreement 8

III. PARTIES' RULE 11(c)(1)(C) PLEA 9

IV. GENERAL SENTENCING PRINCIPLES 10

V. SECTION 3553(a) SENTENCING FACTORS 10

A. Nature and Circumstance of the Offense 10

B. History and Characteristics of the Defendant 13

1. Mr. Bolton's Public Statements About The Handling of Classified Information 15

2. Pre-National Security Advisor Statements (2016 – 2017) 15

3. Post-Tenure/Iranian Hack Public Statements, Comments, and Commentary (2023 – 2025) 16

C. Promote Respect for the Law 24

D. Provide Just Punishment 24

E. General and Specific Deterrence 25

F. Similarly Situated Defendants 27

G. Supervised Release Conditions 29

CONCLUSION 30

TABLE OF AUTHORITIES

CASES

Gall v. United States, 552 U.S. 38 (2007) 9-10

Kimbrough v. United States, 552 U.S. 85 (2007) 10

United States v. Beckner, 166 F.4th 1240 (10th Cir. 2026) 27

United States v. Blue, 877 F.3d 513 (4th Cir. 2017) 10

United States v. Bolton, 468 F. Supp. 3d 1 (D.D.C. 2020) 30

United States v. Dotson, 324 F.3d 256 (4th Cir. 2003) 29

United States v. Ford, Cr. No. PJM-05-235 (D. Md. 2005) 29

United States v. Ford, 288 Fed. App'x 54 (4th Cir. Aug. 4, 2008). 29

United States v. Hale, 1:19-CR-59 (E.D.V.A, Mar. 31, 2021) 28-29

United States v. Martin, Cr. No. RDB-17-69 (D. Md.) 28

United States v. Lawson, 128 F.4th 243 (4th Cir. 2025) 27

United States v. Nghia Hoang Pho, Cr. No. GLR-17-631 (2018) 28

United States v. Withers, 100 F.3d 1142 (4th Cir. 1996) 27

STATUTES

18 U.S.C. § 793 32

18 U.S.C. § 793(e) 20

18 U.S.C. § 3553 2

18 U.S.C. § 3553(a) 10, 29

18 U.S.C. § 3553(a)(6) 29-30

18 U.S.C. § 3583(d) 31

18 U.S.C. § 3583(d)(1)-(3) 31

18 U.S.C. § 3661 10

50 U.S.C. § 3093(e) 11

OTHER AUTHORITIES

Bolton, John, THE ROOM WHERE IT HAPPENED: A WHITE HOUSE MEMOIR 26

Federal Rule of Criminal Procedure 11(c)(1)(C) ..... *passim*

Federal Rule of Criminal Procedure 11(c)(5) 9

Federal Rule of Criminal Procedure 11(c)(5)(B) 9

U.S.S.G. § 2M3.2 (2005) 8

U.S.S.G. § 3B1.3 (2005) 8

U.S.S.G. § 3E1.1(a) (2005) 8

U.S.S.G. § 3E1.1(b) (2005) 8

U.S.S.G. §§ 4C1.1(a), (b) 8

U.S.S.G. § 5B1.1 (2005) 8

U.S.S.G. § 5C1.1(f) (2005) 8

I. INTRODUCTION

For 17 months, John Robert Bolton, II held one of the highest non-Senate confirmed positions in the United States Government. As Assistant to the President for National Security Affairs (commonly referred to as the "National Security Advisor"), Mr. Bolton advised the President on "all exigent threats to the United States and other issues related to national security, including foreign relations, intelligence activities, and decisions regarding the use of military force." Presentence Investigation Report (PSR) ECF 87 at ¶ 13; *see also id*. ¶ 12 (describing role of National Security Advisor). As National Security Advisor, Mr. Bolton had access to "some of the U.S. Government's most sensitive and closely guarded national security secrets." *Id*. ¶ 13.

Mr. Bolton was appointed to be the National Security Advisor on April 9, 2018. *Id*. The day before he began his duties, Mr. Bolton established a text chain with two relatives who did not have security clearances or a need to know classified national defense information. Mr. Bolton used that text chain, over a non-governmental messaging application, to transmit classified national defense information to those unauthorized persons. He did so in furtherance of his plan to write a book about his time as National Security Advisor. The classified national defense information that Mr. Bolton transmitted to his relatives – and which he ultimately retained – concerned "meetings with senior members of the U.S. Government, intelligence briefings from members of the intelligence community and military, discussions with foreign leaders, foreign intelligence and military organizations, and intelligence products and reports." *Id*. ¶ 36; *see also id*. ¶ 44 (describing transmission of documents alleged in Counts One through Eight of the Indictment).

With blatant disregard for the consequences of his actions, and despite his decades of national security experience, government knowledge, and training in handling classified

information, Mr. Bolton directly jeopardized U.S. national security for personal gain. Most notably, Mr. Bolton's actions did not just create a hypothetical risk of harm: classified national defense information transmitted by him over his personal email account was obtained by a cyber hacker believed to be associated with the Islamic Republic of Iran. *Id.* ¶ 22. As a result, Mr. Bolton's actions placed our nation's most sensitive secrets directly in the hands of a significant geopolitical adversary who poses a relentless threat to U.S. national security.

As explained below and in the Government's classified supplemental sentencing memo, based on the applicable factors under Title 18, United States Code, Section 3553(a), including the nature and circumstances of the offense, Mr. Bolton's personal history and characteristics, the need to deter Mr. Bolton and others from committing similar crimes, and promotion of respect for the law, this Court should impose a sentence of 60 months imprisonment, three years of supervised release, the agreed-upon $2.25 million fine as set forth in the parties' Rule 11(c)(1)(C) plea agreement, and a $100 special assessment.

II. FACTUAL BACKGROUND

A. Role of the National Security Advisor

As the National Security Advisor, Mr. Bolton "advise[d] the President with respect to the integration of domestic, foreign, and military policies relating to the national security of the United States." *Id.* ¶ 12. He was also responsible for "assessing and appraising the objective, commitments, and risks of the United States in relation to the actual and potential military power of the United States[.]" *Id.*

B. Offense Conduct

1. Background

The Presentence Investigation Report ("PSR") accurately sets forth the offense conduct. From April 9, 2018, until September 10, 2019, Mr. Bolton served as the National Security Advisor. *Id*. ¶ 13. During his tenure, and through September 15, 2019, he transmitted documents (characterized by Mr. Bolton as "diaries") that contained classified national defense information to two individuals who had neither the security clearances nor the need to know the information. *Id*. ¶ 19. He did so by using "commercial non-governmental messaging applications." *Id*.

2. Mr. Bolton Publishes a Book about his Tenure as National Security Advisor

The day after leaving his role as National Security Advisor, Mr. Bolton's literary agent emailed a publisher about Mr. Bolton's intention to publish a book about his tenure "in a meticulously observed manner with direct quotes from all parties based on contemporaneous notes." *Id*. ¶ 45. In return, Mr. Bolton was promised a $1.5 million advance.[1] *Id*. Approximately three months later, in December 2019, Mr. Bolton began sending drafts of portions of the book to both his publisher and literary agent. *Id*. Later that month, Mr. Bolton submitted a manuscript, which contained none of the classified national defense information charged in this Indictment, to the National Security Council ("NSC") for the pre-publication review process. *Id*. ¶ 48. The pre-publication review process, which any clearance holder must follow before publishing, is designed to ensure classified or national defense information is not unlawfully disclosed to the public.

In June 2021, the United States and Mr. Bolton entered into a settlement agreement resolving civil litigation arising from Mr. Bolton's book. *Id*. ¶ 49. In addition to having to return

[1] The final advance received by Mr. Bolton was less than this amount, in part due to the timing of the prepublication review process, although ultimately his total earnings from the book exceeded $1.5 million.

all classified information as a result of leaving government service, Mr. Bolton agreed as part of the civil settlement to "provide to the United States all materials in his possession, custody, or control that may contain any classified information." *Id.* ¶ *49.*

3. The Iranian Hack of Mr. Bolton's Personal Email Account

At some point between September 2019 (when Mr. Bolton left government service) and July 2021, after the civil settlement agreement was entered, *see* PSR ¶ 49, a cyber actor believed to be associated with the Islamic Republic of Iran hacked the personal email account that Mr. Bolton had used to transmit diaries containing classified national defense information. As a result, the cyber actor gained unauthorized access to classified national defense information which was contained in that account. *Id*. ¶ 22.

4. Classified National Defense Information Found at Mr. Bolton's Washinton, D.C. Office and Maryland Residence, And Within His Electronic Devices and Accounts

On August 22, 2025, law enforcement executed search warrants at Mr. Bolton's Maryland residence and his Washington, D.C. office. PSR ¶ 50. During those searches, law enforcement recovered folders with hard copies of the following documents, among others, containing classified national defense information (*id*. ¶ 50):

COUNT	DOCUMENT DESCRIPTION	HIGHEST CLASSIFICATION LEVEL
9	Document Av2: Reveals intelligence about future attack by adversarial group in another country.	TOP SECRET//SI [redacted]/NOFORN
10	Document Bv2: Reveals liaison partner sharing sensitive information with the U.S. intelligence community.	SECRET//NOFORN
11	Document Cv2: Reveals intelligence that a foreign adversary was planning a missile launch in the future; a covert action in a foreign country that is related to sensitive inter-governmental actions; sensitive sources and methods used to collect human intelligence.	TOP SECRET//HCS [redacted] [redacted]//ORCON/NOFORN

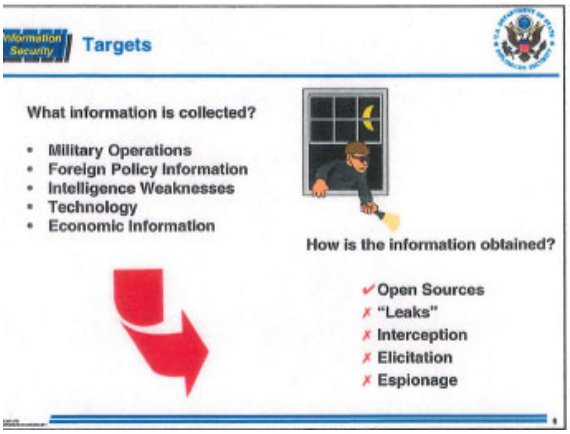
12	Document Dv2: Reveals intelligence about an adversary's knowledge of planned U.S. actions; intelligence about adversary's plans for attack conducted against U.S. Forces in another country; human intelligence using sensitive sources and methods; a covert action program; intelligence collected on the leader of an adversary nation's military group.	TOP SECRET//SI [redacted] [redacted]//ORCON/REL TO USA GBR
13	Document Ev2: Reveals intelligence on an adversary's leaders.	TOP SECRET//SI [redacted] [redacted]//HCS [redacted] [redacted]//ORCON/NOFORN
14	Document Fv2: Reveals intelligence concerning a foreign country's interactions with an adversary; in quotation marks direct statement collected via intelligence sources and methods on a foreign country; foreign country's intelligence describing an adversary's planned attack on a facility; sensitive sources and methods used to collect intelligence on a foreign country; a covert action and sources and methods used.	TOP SECRET/SI [redacted] [redacted]//HCS [redacted]//ORCON/NOFORN
15	Document Gv2: Reveals covert action planned by the U.S. Government; intelligence confirming a foreign adversary was responsible for an attack.	TOP SECRET//SI [redacted] [redacted]//HCS [redacted]// ORCON/NOFORN
16	Document Hv2: Reveals a covert action conducted by the U.S. Government, a liaison partner country, and specific information about the action.	TOP SECRET//HCS [redacted]// ORCON/NOFORN
17	Document I: Reveals sources and collection used to obtain statements of a foreign adversary; covert action conducted by the U.S. Government in a foreign country.	TOP SECRET//SI [redacted] [redacted]//ORCON/NOFORN
18	Document J: Reveals intelligence that a foreign country was considering specific force against another country.	TOP SECRET//SI [redacted] [redacted]// ORCON/NOFORN

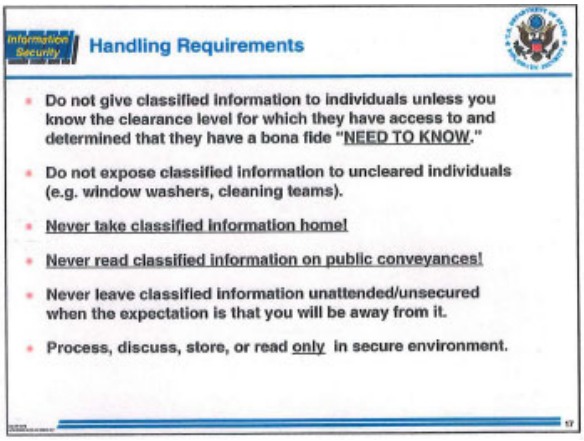
Court-authorized searches of electronic devices and accounts uncovered evidence that Mr. Bolton had transmitted the following documents, among others, containing classified national defense information to his two uncleared relatives via a non-governmental messaging application between September 23, 2018, and September 15, 2019:

COUNT	DOCUMENT DESCRIPTION	HIGHEST CLASSIFICATION LEVEL
1	Document A: Reveals intelligence about future attack by adversarial group in another country.	TOP SECRET//SI [redacted]/NOFORN
2	Document B: Reveals liaison partner sharing sensitive information with the U.S. intelligence community.	SECRET//NOFORN
3	Document C: Reveals intelligence that a foreign adversary was planning a missile launch in the future; a covert action in a foreign country that is related to sensitive inter-governmental actions; sensitive sources and methods used to collect human intelligence.	TOP SECRET//HCS [redacted] [redacted]//ORCON/NOFORN
4	Document D: Reveals intelligence about an adversary's knowledge of planned U.S. actions; intelligence about adversary's plans for attack conducted against U.S. Forces in another country; human intelligence using sensitive sources and methods; a covert action program; intelligence collected on the leader of an adversary nation's military group.	TOP SECRET//SI [redacted] [redacted]//HCS[redacted] [redacted]//ORCON/REL TO USA GBR
5	Document E: Reveals intelligence on an adversary's leaders.	TOP SECRET//SI [redacted] [redacted]//HCS [redacted] [redacted]//ORCON/NOFORN
6	Document F: Reveals intelligence concerning a foreign country's interactions with an adversary; in quotation marks direct statement collected via intelligence sources and methods on a foreign country; foreign country's intelligence describing an adversary's planned attack on a facility; sensitive sources and methods used to collect intelligence on a foreign country; a covert action and sources and methods used.	TOP SECRET//SI [redacted] [redacted]//HCS [redacted]//ORCON/NOFORN
7	Document G: Reveals covert action planned by the U.S. Government; intelligence confirming a foreign adversary was responsible for an attack.	TOP SECRET//SI [redacted] [redacted]//HCS [redacted]// ORCON/NOFORN
8	Document H: Reveals a covert action conducted by the U.S. Government, a liaison partner country, and specific information about the action.	TOP SECRET//HCS [redacted]//[redacted]// ORCON/NOFORN

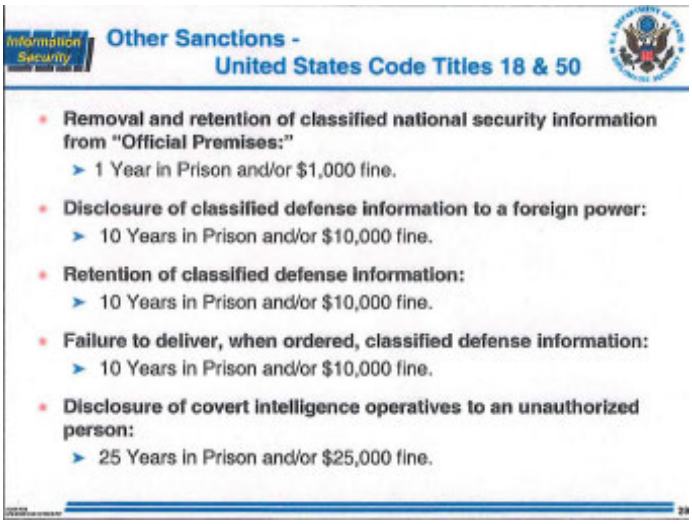
At Mr. Bolton's Washington, D.C. office, law enforcement recovered a 2001 State Department transition team introductory security briefing binder. The binder included slides

addressing security threats and handling requirements for classified information (USA-000370, 000377):





The binder also addressed the dangers of mishandling classified information, and a discussion about the potential consequences of mishandling classified information, including criminal penalties (USA_000383):



C. Arraignment, Rearraignment and Guilty Plea

On June 26, 2026, Mr. Bolton pled guilty to Count Twelve of the Indictment, pursuant to a plea agreement submitted to the Court under Federal Rule of Criminal Procedure 11(c)(1)(C). PSR ¶¶ 2, 4. In the plea agreement, the Government did not oppose a two-level reduction for acceptance of responsibility pursuant to U.S.S.G. § 3E1.1(a), and agreed to move for an additional

one-level reduction ("third point"), pursuant to 3E1.1(b). Plea Agreement (ECF 81) at 5-6, ¶ 5(h). The Government moves for the additional one-level reduction.

D. Guidelines Calculations

The PSR accurately calculates Mr. Bolton's offense level, criminal history category, and advisory Guidelines range. It reflects the plea agreement's stipulations as to the base offense level of 35, pursuant to U.S.S.G. § 2M3.2. PSR ¶ 56. After a two-level upward adjustment for Abuse of Position of Trust pursuant to U.S.S.G. § 3B1.3, given Mr. Bolton's position as National Security Advisor, his adjusted offense level, before acceptance of responsibility, is 37. PSR ¶¶ 59, 61.

In the plea agreement, the Government did not oppose a two-level reduction for acceptance of responsibility pursuant to U.S.S.G. § 3E1.1(a) and agreed to move for an additional one-level reduction ("third point") pursuant to 3E1.1(b). Plea Agreement (ECF 81) at 5-6, ¶ 5(h). The Government moves for the additional one-level reduction. After the three-level reduction for acceptance of responsibility, and a two-level Zero-Point Offender reduction under Chapter Four (U.S.S.G. §§ 4C1.1(a), (b)), PSR ¶¶ 62-64, the total offense level is 32. PSR ¶ 65. Under the Sentencing Guidelines, because Mr. Bolton's applicable range falls within Zone D, Mr. Bolton is ineligible for a probationary sentence. *Id.* ¶ 98 (citing U.S.S.G. § 5B1.1, cmt n.2); *see also* U.S.S.G. § 5C1.1(f) ("If the applicable guideline range is in Zone D of the Sentencing Table, the minimum term shall be satisfied by a sentence of imprisonment.").

E. Bolton's Compliance with Plea Agreement

On August 12, 2026, Mr. Bolton and his counsel met with the Government and representatives of the U.S. Intelligence Community ("USIC") pursuant to paragraph 10 of the plea agreement. During that debrief, Mr. Bolton answered all questions to the best of his ability. Mr. Bolton also provided additional requested information through consultation with members of his

family.

III. PARTIES' RULE 11(c)(1)(C) PLEA

The parties submitted the proposed plea agreement in this matter pursuant to Federal Rule of Criminal Procedure 11(c)(1)(C). Under this rule, the parties "agree that a specific sentence or sentencing range is the appropriate disposition of the case." As a party to the agreement, the Court has the option to accept or reject the plea agreement. *See* Plea Agreement ¶ 8.

If the Court chooses to reject the plea agreement, the Court must inform the parties and advise the defendant and the Government that either party has the opportunity to withdraw from the plea agreement under Rule 11(c)(5). *Id.* If a defendant then chooses not to withdraw his plea, the Court must advise the defendant that it may "dispose of the case less favorably toward the defendant than the plea agreement contemplated." FED. R. CRIM. P. 11(c)(5)(B).

For the reasons set forth in this memorandum, Mr. Bolton's conduct was serious and jeopardized national security in extraordinary ways, as will be discussed in the Government's classified sentencing submission. Viewed against his age and public service, the Government believes that a sentence of 60 months of imprisonment followed by three years of supervised release is sufficient but not greater than necessary to satisfy the goals of sentencing as set forth by Congress. Absent Mr. Bolton's record of public service, his mishandling of such highly classified information—in his regular, detailed transmissions—and the damage to national security resulting from his actions would warrant a sentence of imprisonment well in excess of 60 months.

IV. GENERAL SENTENCING PRINCIPLES

In *Gall v. United States*, 552 U.S. 38 (2007) and subsequent cases, the Supreme Court has set forth a multi-part procedure that sentencing courts should follow when imposing sentence. First, the court must correctly calculate a defendant's sentencing range under the advisory

guidelines. *See id*. at 51. Next, the district court must allow "both parties an opportunity to argue for whatever sentence they deem appropriate." *Id*. at 49. After hearing argument, the court must then "consider all of the § 3553(a) factors," *id*. at 49, keeping in mind the "overarching provision instructing district courts to 'impose a sentence sufficient, but not greater than necessary,' to accomplish the goals of sentencing," *Kimbrough v. United States*, 552 U.S. 85, 102 (2007) (quoting 18 U.S.C. § 3553(a)). *See United States v. Blue*, 877 F.3d 513, 517-18 (4th Cir. 2017).

The district court has broad discretion in deciding what reliable evidence it may consider in imposing sentence: "No limitation shall be placed on the information concerning the background, character, and conduct of a person convicted of an offense which a court of the United States may receive and consider for the purpose of imposing an appropriate sentence." 18 U.S.C. § 3661.

V. SECTION 3553(a) SENTENCING FACTORS

A. Nature and Circumstances of the Offense

Mr. Bolton engaged in a 17-month scheme to write a book based on his meticulous contemporaneous notes documenting his daily activities as the National Security Advisor—notes that he knew contained significant amounts of classified information obtained through high-level briefings and highly classified intelligence reports. The documents found in Mr. Bolton's residence nearly six years after the end of his government tenure were not created or maintained by him for his official duties as National Security Advisor. Rather, these documents were selected so he could publish a bestseller. Despite Mr. Bolton's extensive training on handling classified information, Mr. Bolton used unsecure computers and documents to type his notes containing highly classified information. Further, Mr. Bolton subsequently sent these notes to his uncleared relatives via an unsecure, non-governmental messaging application. As a result of his actions, Mr.

Bolton willfully jeopardized U.S. national security, and compromised the nation's most sensitive secrets. As Mr. Bolton has explained elsewhere,

> There are two kinds of communication when you're in one of these senior administration positions: There's communications over the government secure telecommunications network, on which we have spent billions of dollars and decades of effort to make impenetrable by our adversaries . . . and then there is every other option, and every other option is not acceptable.[2]

Mr. Bolton was the highest level advisor to the President on issues of national security, including foreign relations, intelligence gathering, military actions by our allies and adversaries, arms negotiations, and covert actions, which are "activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[3]

That position required Mr. Bolton to have access to the most sensitive and highly classified information within the United States Government. By necessity, this position also gave Mr. Bolton the ability (and the obligation) to seek out and review the most sensitive, highly classified information from all corners of the USIC to fully and accurately advise the President. Mr. Bolton, as National Security Advisor, had access to classified information at all times; indeed, the NSC installed a Sensitive Compartmented Information Facility (SCIF) in his home. PSR ¶ 15. Mr. Bolton understood the sensitivity of the information he had at his fingertips, and the consequences if that information was not properly protected. "I do know what kinds of documents were put in front of the President during my time," Mr. Bolton told CNN in June 2023. "And they did go to absolute the most important secrets that the United States has, directly affecting national security,

---

[2] *See* POLITICO – Who will be Trump's Fall guy for Signalgate? https://youtu.be/c4Y-6Dt5wOQ?si=hq2AtUhHVyGyvZCy, available at (last viewed Oct. 28, 2026). Exhibit 1 at 3:03-3:41.

[3] 50 U.S.C. § 3093(e).

directly affecting the lifes [sic] and lives and safety of our service members and our civilian population."[4]

Given this level of responsibility, Mr. Bolton's history of government service, and his experience with the rules governing classified information gained over the course of decades, it is inconceivable that he failed to grasp the security risks associated with his actions. Mr. Bolton transmitted reams of classified national defense information spanning an array of the most critical national security issues, such as foreign relations, military operations, and covert actions, in regular transmissions to two relatives not authorized to access that information, and did so using unauthorized, non-governmental communication systems. Additionally, he kept paper copies of this highly sensitive information in his residence, where others also lived and visited and could have accessed them. Given Mr. Bolton's extensive knowledge concerning the rules governing the safeguarding of classified information, his status as a high-value target to numerous foreign adversaries, and the consequences should any information possessed by him fall into the wrong hands, Mr. Bolton must have known that his actions while National Security Advisor increased the probability that a foreign power (or other malicious actors seeking the most sensitive information available to U.S. Government officials) could gain access to the nation's most sensitive information. That probability unfortunately became a reality in this case; as a direct result of Mr. Bolton's conduct, an Iranian government cyber hacker obtained much of the classified national defense information that Mr. Bolton unlawfully retained and transmitted.

Federal employees and government contractors working on matters of national security are given significant responsibility and trust in handling information that will, by definition, if not

[4] CNN, Bolton makes prediction on Trump's political career after indictment, available at https://youtu.be/b-tXafdTrgI?si=Myn1_CMPShd3uwDo (June 12, 2023) (last viewed Sept. 8, 2026).

properly maintained, lead to security risks. To protect the national security, those individuals must comply with the careful and comprehensive rules for safeguarding classified information.

A security clearance holder's failure to adhere to those rules endangers national security, and Mr. Bolton's willful failure to do so must be met with a meaningful sanction. His failure undermines confidence in the government's ability to conduct national security affairs, including sharing information with other nations as well as domestic and foreign intelligence partners. Moreover, the rank or position of the person who mishandles classified information does not diminish the risks to national security; The information determines the gravity of the breach. Here, Mr. Bolton's willful conduct over his 17-month tenure as National Security Advisor, and continuing for nearly next six years after his tenure, fell exceedingly short of meeting that high standard which so many federal employees and contractors must meet every day.

The course of conduct detailed in the parties' Statement of Facts demonstrates more than a one-time mistake or a momentary lapse in judgement. Mr. Bolton's course of conduct was not the product of a decision made in the heat of the moment or under exigent, unforeseeable circumstances. The facts before this Court lay out a long-running and continuous plan to unlawfully transmit and retain the nation's most highly classified information and thereby enable Mr. Bolton to write a bestselling book – a plan that would have continued but for Mr. Bolton's departure from government.

B. History and Characteristics of the Defendant

Mr. Bolton has a decades-long record of government service. Throughout Mr. Bolton's government career, he has had access to classified information through his official duties as a State Department official (Under Secretary of State for Arms Control and International Security), Assistant Attorney General within the Justice Department, United States Permanent

Representative to the United Nations, and, finally, National Security Advisor.[5]

The Government is aware of the positive aspects of Mr. Bolton's background, including his four decades of public service, and has considered as much in its below-guidelines sentencing recommendation. The positive aspects of his career, however, must be weighed against the course of conduct to which he pleaded guilty. Notwithstanding his decades of experience with the rules governing the safeguarding of classified information (and his enthusiasm to address what he perceived to be others' shortcomings in that area, *see infra* at § V.B.2), Mr. Bolton willfully disregarded those rules when they applied to him by sending highly classified national defense information classified concerning the nation's most sensitive secrets to uncleared relatives, all to write a lucrative book after leaving government service.

The Government has weighed Mr. Bolton's government service in determining a significantly below-guidelines term of imprisonment of 60 months is appropriate under the applicable sentencing factors. Were it not for Mr. Bolton's decades-long career in public service and his age, his course of conduct would warrant a sentence well in excess of the Rule 11(c)(1)(C) sixty-month cap on the term of imprisonment proposed by the parties.

1. Mr. Bolton's Public Statements About The Handling of Classified Information

Over the course of many years, dating back to 2016, Mr. Bolton has spoken publicly about (1) the sensitivity of classified information; (2) the adverse impacts on national security if classified information is mishandled; (3) Mr. Bolton's personal experience and practices in handling classified information; (4) his opinions about how other government officials have handled (or mishandled) classified information, including whether an officials' actions constituted

[5] Exhibit 3, U.S. Department of State Archive, available at https://2001-2009.state.gov/outofdate/bios/b/53920.htm; Exhibit 4, Hon. John R. Bolton, Federalist Society, Speaker and Author Bios, *available at* https://fedsoc.org/bio/john-bolton.

a federal crime. Those public statements are too numerous to fully catalog; however, a summary of these statements (in chronological order) provides insight into how Mr. Bolton would have judged the propriety of his own conduct—before, during, and after his time as National Security Advisor. These statements emphasize the need to protect—and the consequences of mishandling—the very type of highly classified national defense information Mr. Bolton himself compromised and underscore the need to deter Mr. Bolton and others from the conduct for which he now faces sentencing.

2. *Pre-National Security Advisor Statements (2016 – 2017)*

In a March 2016 television interview, Mr. Bolton recognized the risks of using unsecure communications devices: "Anything on an unsecure device, phone, laptop, whatever it is, is subject to being hacked."[6] During a September 2016 television interview, Mr. Bolton discussed his knowledge of the rules governing classified information: "I remember those sorts of things because if you're conscious of the need to protect classified information, you'll remember what the rules are[.]"[7]

During a January 2017 television interview, Mr. Bolton addressed the seriousness of the allegation involving Russian hacking of Democratic National Committee computer servers, and his belief about the significant consequences that should ensue for someone who mishandles classified information: "Look, as I've said before, I believe it's still to this day, if I had done at the

[6] MTPAmerica, Hillary Clinton Email Scandal – John Bolton (Mar. 17, 2016), *available at* https://youtu.be/mf4osHNpSYY?si=7tauzvLFss0MTdhE (last viewed October 30, 2026). Exhibit 5 at 1:34-1:40.

[7] John Bolton: Clinton displayed gross negligence with her emails. Fox Business Network https://youtu.be/20sSuoFHcGI?si=Qs-bFGLAaGXmw8QA (last viewed October 30, 2026). Exhibit 6 at 0:44-0:52.

State Department what [she] did, I'd be wearing an orange jumpsuit now."[8]

3. Post-Tenure/ Iranian Hack Public Statements, Comments, and Commentary (2023 – 2025)

Between September 2019 (after Mr. Bolton's time as National Security Advisor), and July 2021, a cyber actor believed to be associated with the Iranian government hacked Mr. Bolton's personal email account. As a result, the cyber hacker obtained unauthorized access to classified national defense information which Mr. Bolton had sent and stored in that account using unsecure, non-government communication channels. PSR ¶ 22. The following statements all occurred after Mr. Bolton knew that his account had been hacked by a malicious cyber hacker, and while he possessed more than a thousand pages of documents containing classified national defense information, all unsecured within his personal residence.

In a January 2023 interview, Mr. Bolton addressed how mishandling of classified information by high-level officials, without any consequence, sends a poor message to other security clearance holders who are expected to follow those same rules: "If [those employees] are not sensitive to the risks involved, we're going to get a lot more dispersion of classified documents and a lot more damage. And this really is the power of example. If a former President and a former Vice President aren't careful with classified information, what is the lesson that teaches?"[9]

During a June 2023 television interview, in the context of discussing the President's declassification authority, Mr. Bolton emphasized that the critical issue was the information itself, not the format of the information. "[R]eally what's classified is not the piece of paper or the

[8] Did Comey mishandle the Clinton email case? Fox Business Network (Jan. 16, 2017), *available at* https://youtu.be/LNMfTa3I2BA?si=uK9RZyqW-Mo6rZ23 (last viewed Oct. 30, 2026). Exhibit 7 at 1:01-1:10.

[9] NewsNation, Bolton: Biden classified documents probe a "gift" for Trump, *available at* https://www.newsnationnow.com/cuomo-show/bolton-biden-trump-classified-documents/ (Jan. 23, 2023) (last viewed Oct. 30, 2026). Exhibit 8 at 2:22-2:40.

electrons, it's the information."[10] When asked during this same interview about the risk to the national security, Mr. Bolton discussed how the critical question is not whether an adversary gained access to the information, but whether the person's actions increased that probability:

> In this case the reason the mishandling of classified information was serious because it put at risk these sensitive pieces of information making it more likely that a foreign adversary could get their hands on it. It's not enough to say, well, the Russians and the Chinese don't have it-although we don't know that for sure. It's that it increased the danger they could get it. That's why the criminal statutes are written the way they are and for very prudent reasons.[11]

During a June 2023 interview, Mr. Bolton addressed the importance of securing classified information—especially information that comes before the President—and the consequences of failing to secure that information:

> [T]he President was given uncounted amounts of information about American military capabilities, capabilities of our adversaries, threats from terrorists, proliferation of nuclear, chemical and biological weapons, enormous amounts of information about sensitive diplomatic, economic matters. And the level of things the President sees, by definition, is at the highest you could get. No small problems come to the President. By the time they get to him, there's nobody else below who's able to make the final decision. So to give him the information he needs, they're simply no ceiling on how much or how sensitive it could be.[12]

Asking whether the information fell into the wrong hands, according to Mr. Bolton, is not enough; it is the risk of compromise that is the relevant concern: "[N]obody's alleging here that they these documents have fallen into the hands of Russia or China, but that's not the point. The

---

[10] MS NOW, John Bolton to Jen Psaki: Trump's retention of classified documents was 'very disturbing', *available at* https://youtu.be/1F5Y6lM5yMY?si=78kc0n_fmuvDno7z (June 18, 2023) (last viewed October 30, 2026). Exhibit 9 at 5:04-5:09.

[11] *Id*. at 8:31-8:58.

[12] Scripps News, Trump's Mar-a-Lago Indictment: John Bolton's Perspective | Nat Sec Concerns (June 12, 2023) https://youtu.be/GHjtyG5Ou2k?si=e2mXunLKN4tY-sDf (last viewed Oct. 22, 2026). Exhibit 10 at 2:10-2:50.

issue is if you don't safe hold the documents, if you don't look out for their security, you dramatically increase the risk of compromise[.]"[13]

In March of 2025, Mr. Bolton spoke on national television about his shock that a high-level government official would communicate sensitive information using a non-government means of communication—even if that means was encrypted:

> [W]ell, I was shocked and I really I was without words and I say that not because I'm more virtuous than anybody who was in that group. I just couldn't imagine it was happening. I couldn't imagine anybody would use Signal. You know, some of the guests have commented that Signal is highly encrypted. I'll just say this: if you think Signal is equivalent to U.S. government secure telecommunications, think again. So, all the consequences you've been discussing are obviously going to be enormously important, but I just can't, to this moment, get over the idea that during the days that group was going on, not one of the participants said we shouldn't be doing this on Signal.[14]

During this same interview, while knowing that he had used a non-governmental messaging application to send reams of highly classified national defense information, Mr. Bolton then responded that this incident was worse than a 2016 incident involving the former Secretary of State:

> I was very critical then and, you know, we call this process learning, that when somebody does something like what she did, whether she deserved to be prosecuted or anything else—that goes into the memory and the body politic. How can you then turn around and conduct—let's forget the classification issue—how could you conduct official government business over a non-official channel? Maybe there's some in extremis situation when you're on Samoa or something and there aren't any official channels, but it's-that's they were-they were in Washington, probably in their offices. I just, as I say, words fail me here. I cannot even imagine this happening.[15]

During another March 2025 television interview, Mr. Bolton explained how the inadvertent

---

[13] *Id*. at 2:53-3:08.

[14] CNN, John Bolton reacts to news of Trump officials texting war plans to reporter, *available at* https://youtu.be/cbYsnwLvNcY?si=lr0msmSPWYBXTbru (Mar. 24, 2025)(last viewed Oct. 22, 2026). Exhibit 11 at 0:33-1:23.

[15] *Id*. at 3:03-3:46.

disclosure of information to a magazine editor risked national security:

> I think clearly the kind of information that was disclosed [by government officials] in these latest revelations by the Atlantic, if they fell into the hands of an American adversary, would be extremely dangerous for American forces about to enter into combat. And the whole, the whole definitional structure of classified information is the amount of harm it would cause to the United States—varying amounts of aren't for various levels of classification. There's simply no doubt with this information that we've seen that potential harm to American forces was real, and, and that makes it classified, and that makes its release in a non-classified channel a serious matter. [16]

When asked about his opinion on why government officials did not move their conversation to a secure government communications network, Mr. Bolton expressed a binary view of where and how to conduct sensitive government communications: "[H]ere's communication of sensitive information for dummies, the way I would look at it. You're either on a secure governmental system or you're not. You're not on a secure governmental system, you got a problem."[17]

During this interview, Mr. Bolton went on to discuss how the mishandling classified information by senior officials, without accountability, affects the USIC generally:

> [T]he question is what was the potential damage to the United States this kind of behavior caused and I think the potential damage was real. The second matter this doesn't necessarily go to criminal prosecution but it does go to accountability and consequences for the people involved. What does this say to the thousands of people in the military and in the intelligence community and the State Department and other government agencies, that the very top levels of the U.S. government make this kind of mistake and, so far at least, have not faced consequences. What does it say to them? What does it do to their morale? What does it do to their effectiveness? What does it do to their respect for their leadership? And beyond that, what does the rest of the world say when senior government officials in the United States behave so irresponsibly? What were they doing off of secure government channels? That is the original sin here.[18]

---

[16] John Bolton Reacts to War Group Chat Leak - Channel 4 News, Mar. 26, 2025, found at https://youtu.be/13n1577TBk4 (last viewed Oct. 22, 2026). Exhibit 12 at 0:10-0:55.
[17] *Id*. at 3:39-3:50.
[18] *Id*. at 4:57-5:51.

Mr. Bolton went on to discuss how any amount of classified information can be useful to foreign adversaries, both in the short- and long-term, which subsequently damages U.S. national security interests:

> You just referred to potential damage: has actual damage been done, though I think actual damage is possible because of the way foreign intelligence services operate, the way our own intelligence services operate. You take everything you can get. You take every piece of information, in this case, about American military operations against the Houthis in Yemen. It tells you something that otherwise you wouldn't know about American capabilities, American tactics, American approaches to this kind of thing, and that is useful to the Russians, the Chinese, the Iranians, the North Koreans, and others as well. How that fits into the body of knowledge they already have is a question I can't answer, but it can't help, that's for sure.[19]

In a 2025 interview, Mr. Bolton responded to congressional testimony by a senior Cabinet official about the use of a non-government means of communication for official military business:

> I think the key point is that the Federal Government, over decades, has spent billions of dollars to create the world's most secure telecommunications capabilities. And why these senior officials, virtually all of whom are 24/7 able to get onto a secure phone, secure computer, why they would shift off of that, for any reason, to any commercial system? That the first-that's the original sin. Everything after that just makes things worse.[20]

In response to a question about whether the non-government employee who was on this chain should have published the information communicated in the group chat, Mr. Bolton focused on the risks of not using government communications systems:

> The whole point of staying in the government-approved communications channels is you can say anything you want. You can say, you can talk about today's newspapers. You can talk about top secret, codeword information. You can talk about anything in between. You don't worry about it. Once you're on Signal, once you're on any nongovernmental, nonsecured channel, you're at risk of saying something if you're not careful.[21]

---

[19] *Id*. at 6:02-6:41.
[20] CNN, "I think they're very nervous." Bolton on Trump admin's reaction to group chat scandal, available at https://youtu.be/LnBEr4prUYw?si=2RCycNtFMO8FEyJB (last viewed Oct. 22, 2026). Exhibit 13 at 0:48-1:21.
[21] *Id*. at 3:12-3:37.

On a podcast in March of 2025 podcast, Mr. Bolton described in unequivocal terms the proper binary approach to the handling of classified information:

> I took a pretty simplistic approach to things. . . . I would say that there are two kinds of communication, when you're in one of these senior administration positions: there's communications over the government secure telecommunications network, on which we have spent billions of dollars and decades of effort to make impenetrable by our adversaries. So there's that option, and then there is every other option. And every other option is not acceptable.[22]

Mr. Bolton emphasized that an unclassified conversation could take a turn which requires the parties to use a secure means to discuss classified information:

> You don't know how any given conversation is gonna go. If I wanted to speak to the Secretary of Defense, I could have something purely non-classified to talk about, but the conversation could shift very quickly to something else. If you're on a secure line, it doesn't matter. If you're on a non-secure communication platform, then you're at risk.[23]

Mr. Bolton emphasized during these public statements that the rules to handle classified information were designed for safety and security, not convenience. When asked during the interview how high-level national security personnel discuss classified information on a weekend, or outside of regular work hours: "Look, if you want a group chat, there's a place for it. It's called the Situation Room, and if it's Saturday or Sunday, that's too damn bad isn't it?"[24]

During that same interview, Mr. Bolton addressed the immediate and long-term impact of the mishandling of classified information, and how that information can benefit foreign adversaries, especially when added to information obtained by those adversaries from other sources:

> [Y]ou know, just because a foreign government gets intelligence doesn't mean they act on it. It may mean they piece it together with other things. They want to see if

[22] POLITICO – Who will be Trump's Fall guy for Signalgate?, *available at* https://youtu.be/c4Y-6Dt5wOQ?si=hq2AtUhHVyGyvZCy (last viewed Oct. 22, 2026). Exhibit 14 at 3:03-3:40.
[23] *Id*. at 3:40-4:01.
[24] *Id.* at 4:18-4:26.

> information they're getting from that source will produce more information in the future. You don't reveal where you know something and risk blowing the source. So understanding what harm may have come to the United States as a result of these Signal chats, first, this one on Yemen, but perhaps others. I mean, that is a very serious question I haven't heard anyone ask about.[25]

Mr. Bolton was aware of the capabilities provided to certain high-level government officials (including himself) when handling classified information:

> [F]or the Secretary of State, Secretary of Defense, Director of National Intelligence, Director of the CIA, National Security Advisor, they are never more than an arm's length away from secure telecommunications. I had that kind of capability built into my house. I had a SCIF built in my basement by the National Security Council staff[.][26]

During a podcast in April of 2025, Mr. Bolton expressed his shock about a report that discussion occurred over a nongovernment communications application: "Initially, I was totally without words. I couldn't-I couldn't find-I couldn't find a way to express how stunned I was that anybody would do this. You simply don't use commercial means of communication, whether it's supposedly an encrypted app or not, for these kinds of discussions."[27] Later in that interview, Mr. Bolton addressed his concerns that the mishandling of classified information by high-level government officials would have negative downstream consequences:

> [T]his is not just for the people who are directly involved in that group chat. It's for the thousands of other people in the federal government who handle sensitive information and are held to a higher standard, and they need to know that those standards apply up and down the line.[28]

During an April 2025 interview on national television, Mr. Bolton explained that a person's eligibility to access classified information was a function of both the person's security clearance

---

[25] *Id*. at 12:46-13:15.
[26] *Id*. at 4:39-4:58
[27] LEMON DROP – Bolton on Signal-Gate, Trump, and the Constitutional Crisis, available at https://youtu.be/7QLsu2fMpRc (Apr. 18, 2025) (last viewed Oct. 22, 2026). Exhibit 15 at 10:27-10:49.
[28] *Id*. at 15:43-15:59.

level and their need to know such information:

> [C]ommunicating with the people in this group in particular who have absolutely no need to know about any upcoming U.S. military operation leads me to wonder what he's doing on the job on a minute to minute, hour by hour, basis that he's got time to knock out Signal messages to friends and family.[29]

Finally, in considering the defendant's history and characteristics, it bears noting that Mr. Bolton did not admit to his wrongdoing on several critical occasions, despite ample opportunities to do so. Despite his promise in the June 2021 book settlement agreement to return all materials containing classified information, Mr. Bolton did not return the paper copies of the diaries containing volumes of classified national defense information that he had in his home. PSR ¶ 49. And when the FBI interviewed Mr. Bolton in July 2021 about the Iranian government hacker who gained access to Mr. Bolton's personal email account, Mr. Bolton had another opportunity to tell the FBI about his misconduct, which would have allowed federal officials to attempt to remediate the harm. PSR ¶ 22. Yet he did not tell the FBI or anyone else in the U.S. Government that his account "contained national defense information, including classified information, that Mr. Bolton had placed in the account from his time as National Security Advisor," or that he had shared classified national defense information with unauthorized persons using an unsecure, non-government communications platform. *Id.* As such, while Mr. Bolton pursuant to the plea agreement has agreed to debrief with the government, this agreement and willingness to do so simply comes years too late.

[29] CNN, Trump's NSA RIPS INTO His SLOPPY Defense Secretary on A Fresh Signal SCANDAL, *available at* https://youtu.be/z_OJ0uphV1E?si=_pNesP122dyYYXYQ (Apr. 25, 2025) (emphasis added) (last viewed Oct. 16, 2026). Exhibit 16 at 0:48-1:08.

C. Promote Respect for the Law

The Court's sentence must consider that those entrusted with protecting the national security will be treated appropriately when they abuse that trust. This Court should consider Mr. Bolton's prior work in government, and his extensive national security background, in assessing the need to promote respect for the law.

As someone who took an oath to protect and defend the Constitution, with a deep knowledge of the law's requirements, Mr. Bolton's actions are concerning—and inexplicable. The sentence imposed by this Court should send the message that no one is above the law. Former public servants—whatever their rank, position, stature, or history of service—must follow the same laws, rules and requirements as every other security clearance holder. They must also know that their transgressions will be addressed in a court of law the same as any other public servant.

D. Provide Just Punishment

A review of Mr. Bolton's financial assets demonstrates that he did not engage in this criminal conduct out of financial necessity. *See* PSR ¶ 91. He did not commit this crime out of personal desperation. Instead, Mr. Bolton did so in pursuit of what would become a seven-figure book deal. He engaged in this course of criminal conduct, knowing to a moral certainty that the risks he created over and over again by repeatedly compromising highly sensitive classified national defense information. There is no excuse for Mr. Bolton's actions, and the Court's sentence should reflect the heightened need to promote just punishment.

Every security clearance holder learns several basic principles before he or she ever gains access to classified information: (1) you store classified information only in designated, approved locations, identified and authorized by government security professionals; (2) you send, receive, or work on classified information only in secure locations; (3) you must not transmit that

information to someone not authorized to receive that information; and (4) you must not send or receive classified and national defense information using an unauthorized, non-government communications platform. Mr. Bolton knew well all of these principles, yet time after time, document after document, he repeatedly transmitted classified information to unauthorized persons over a non-government communications system and kept paper copies in his home where classified information was not permitted to be stored.

E. General and Specific Deterrence

All aspects of this investigation and prosecution, including the execution of residential and office search warrants, indictment, and guilty plea, have been the subject of worldwide attention. The Court's sentence must deter Mr. Bolton and, perhaps even more importantly, send a general deterrence message to the millions of U.S. security clearance holders that courts will not tolerate the willful mishandling of national defense information.

Another perspective on general deterrence comes from Mr. Bolton himself. As previewed above, Mr. Bolton's own words are instructive on the issue of deterrence, specifically, on the deterrent effect of prosecuting high-level government officials: "I think it's also a question of discipline within the ranks. If people who are subjected to considerable potential penalties including imprisonment . . . don't follow the security regulations, see their boss at the very top get away scot-free, I do think that has a material effect, negative effect on morale."[30] The National Security Advisor, at the very minimum, sets the standard for the rest of the 350-430 person staff of the National Security Council who are responsible for providing the National Security Adviser with the means necessary to fulfil his official duties.[31]

---

[31] Bolton, John, THE ROOM WHERE IT HAPPENED: A WHITE HOUSE MEMOIR 39.

Here, a sentence that does not include a significant term of imprisonment would send the message that crime does pay. A lower sentence would imply that one can abuse their duty and obligation to safeguard classified national defense information so long as they are in a high-level government position. The Court's sentence should send the message that high-level officials must treat classified national defense information with great care, just as they expect everyone underneath them to handle it, knowing that the willful mishandling of that information jeopardizes national security, and therefore will result in severe penalties.

Mr. Bolton engaged in this course of criminal conduct knowing better than anybody that his actions created a significant risk to national security—in his words—solely by increasing the likelihood that a foreign adversary could gain access to the information. Notably, this was not a case in which Mr. Bolton took classified national defense information home for work use. This is also not a case where the risk to national security did not ultimately result in harm. Here, the conduct resulted in much worse: Mr. Bolton's conduct directly enabled a foreign adversary (Iran) to obtain classified national defense information.[32] When subsequently faced with the FBI's notification of the account breach, Mr. Bolton made the conscious decision not to tell law enforcement that he had more than a thousand pages of hard copy documents at his residence or the duplicate copies he retained on various electronic devices which contained national defense information.

Risks caused by the mishandling of national security are a function of the information exposed, not the title or rank of the person who mishandled the information. A significant sentence would also send the deterrence message not just to this former public servant, but to other public

[32] The Government relies on its classified sentencing memorandum and related documents in submission to support this argument.

officials who might believe that their work in public service somehow excuses them from having to follow the same rules as everyone else.

Given Mr. Bolton's conduct here, he is unlikely to ever hold a security clearance again. However, he retains knowledge of a significant amount of classified national defense information which he learned during his tenure as National Security Advisor. This knowledge could jeopardize national security if such information is transmitted to persons not authorized to receive it.

Mr. Bolton's crimes were not the subject of some isolated, snap decision, or a singular exercise of bad judgment. His actions were the product of careful, thoughtful, and deliberate decisions to disregard well-established rules to safeguard classified information—rules he often highlighted when discussing the actions of others.[33] Despite his years of training and knowledge—and his public statements on this topic—he decided that those rules did not apply to him, and that he was the ultimate arbiter of the national security.

F. Similarly Situated Defendants

The proposed 60-month sentence aligns with the sentences imposed in numerous analogous cases, particularly when considering the specifics of Mr. Bolton's conduct. The primary purpose of section 3553(a)(6) is to "fulfill the 'Guidelines' goal' 'to eliminate unwarranted sentencing disparities nationwide." *United States v. Lawson*, 128 F.4th 243, 257 (4th Cir. 2025) (emphasis omitted) (quoting *United States v. Withers*, 100 F.3d 1142, 1149 (4th Cir. 1996). "[T]he concern of the guidelines is disparities between similarly situated defendants—that is, defendants with similar criminal histories who commit similar offenses." *United States v. Beckner*, 166 F.4th 1240, 1255 (10th Cir. 2026) (quoting 18 U.S.C. § 3553(a)(6).

[33] *See supra* § V.B.

In *United States v. Nghia Hoang Pho*, the defendant pled guilty to the willful retention of national defense information under 18 U.S.C. § 793(e). *See United States v. Pho*, Cr. No. GLS-17-631 (D. Md., Dec. 12, 2017) (ECF No. 9). Pho held a Top Secret/SCI security clearance through his employment with the National Security Agency ("NSA"). *Id*. at 12. Throughout the course of his official duties, Pho "worked on highly classified, specialized projects and has access to government computer systems, programs, and information, including classified information." *Id*. Over the span of approximately five years, Pho removed and retained highly classified documents within his residence in the District of Maryland, some of which could have caused exceptionally grave damage to the national security if disclosed without authorization. *Id*. at 12-13. Pho was sentenced to a term of 66 months imprisonment, with a three year term of supervised release. ECF 30.

Separately, in *United States v. Harold T. Martin, III*, the defendant pled guilty to one count of willful retention of national defense information under 18 U.S.C. § 793(e). *See United States v. Martin*, Cr. No. RDB-17-69 (D. Md., Mar. 28, 2019) (ECF No. 204). Martin had previously served in the U.S. Navy and was later employed by at least seven different private companies working with components of the U.S. Department of War and the USIC. *Id*. at 12. Starting in the late 1990s and continuing through August 31, 2016, Martin willfully retained highly classified documents "in his residence (including surrounding property), on his person, and in his vehicle." *Id*. at 13. The unlawfully retained documents included materials from the NSA, U.S. Cyber Command, the National Reconnaissance Office, and the Central Intelligence Agency. *Id.* Martin was sentenced to 108 months of imprisonment, and three years of supervised release. ECF. 219.

In *United States v. Daniel Everette Hale*, the defendant pled guilty to one count of willful retention national defense information under 18 U.S.C. § 793(e). *See United States v. Hale*, No.

1:19-CR-59 (E.D.V.A, Mar. 31, 2021) (ECF 197). Hale previously served in the U.S. Air Force prior to working as a defense contractor for the National Geospatial Intelligence Agency ("NGA"). *Id*. at 2. During the course of his employment, and over the span of four- to five-months, Hale deliberately printed, retained, and transmitted eleven classified documents which were then published by a reporter. *Id*. Hale also "authored an essay, attributed to 'Anonymous,' that became a chapter in a book" that would be published. *Id*. at 3. Hale was subsequently sentenced to 45 months imprisonment with three years of supervised release. ECF 249.

In *United States v. Kenneth Wayne Ford*, Cr. No. PJM-05-235 (D. Md. 2005), the defendant, a 34 year old NSA employee, was convicted after trial of Willful Retention of National Defense Information under 18 U.S.C. § 793(e) and False Statements. 288 Fed. App'x 54 (4th Cir. Aug. 4, 2008). Mr. Ford was sentenced to 72 months imprisonment. *Id*. at 59.

Given these comparable cases, a sentence of 60 months imprisonment is not only appropriate, but necessary to reflect similarly situated 18 U.S.C. § 793(e) offenders. This sentence considers the gravity of the offense, the exceptional harm to U.S. national security, and reflects similar sentences imposed.

G. Supervised Release Conditions

A district court has "broad latitude" to impose conditions of supervised release. *United States v. Dotson*, 324 F.3d 256, 259-260 (4th Cir. 2003). In addition to complying with pertinent Sentencing Guidelines policies, Title 18, United States Code, Section 3583(d) requires that any condition of supervised release be "reasonably related" to the nature and circumstances of the offense, and the history and characteristics of the defendant, and "involve[] no greater deprivation of liberty than is reasonably necessary" to meet those same factors. 18 U.S.C. §§ 3583(d)(1)-(3).

The Government believes that one additional special condition is appropriate: "You must comply with all requirements contained in paragraphs 12 and 13 of the Plea Agreement." This additional condition incorporates Mr. Bolton's existing obligations to comply with his non-disclosure agreements (Plea Agreement ¶ 12), and to submit any future publications to the USIC for pre-publication review (Plea Agreement ¶ 13). Given the nature of his conduct, and his pre-existing obligations, this condition does not involve a deprivation of any liberty interest.

This revised condition would allow the Probation Department to more effectively supervise Mr. Bolton and will minimize the potential for any future disclosure of classified or national defense information.

VI. CONCLUSION

"Defendant Bolton has gambled with the national security of the United States. He has exposed his country to harm[.]" *United States v. Bolton*, 468 F. Supp. 3d 1, 7 (D.D.C. 2020) (Lamberth, J.).[34] As National Security Advisor, Mr. Bolton was entrusted with real-time access to this nation's most sensitive, classified national defense information so that he could fully advise the President on national security matters. Mr. Bolton was entrusted with this position, at least in part, because of his national security background, including his knowledge of how to handle such sensitive information. He also had the unique placement to access any and all of the most highly classified information, to inform both himself and the President. In the wrong hands, this information could cause incalculable damage to the national security, including by jeopardizing foreign relations, intelligence sources and methods, and military personnel. Over the course of 17 months, Mr. Bolton systematically exposed this nation's most sensitive of secrets to cyber theft

[34] Of course, Judge Lamberth issued his opinion without knowing about the documents found in Mr. Bolton's residence—documents that were never cleared for removal by any government entity.

and exploitation by our adversaries, risking foreign affairs, military actions, sources and methods of intelligence gathering, and the successful execution of covert actions (along with the fates of those executing those actions).

Given his decades of experience with classified information, Mr. Bolton's actions during his tenure as National Security Advisor—coupled with his retention of that information in unsecured physical and electronic spaces for several years—demonstrate aggravated, willful conduct. And unlike many cases involving violations of 18 U.S.C. § 793, this Court does need not to speculate whether harm to national security ultimately materialized. By sending and storing classified national defense information using his personal email account, which was then hacked, Mr. Bolton's actions had the direct and predictable effect of giving classified national defense information to a hacker associated with one of the nation-states most reviled by Mr. Bolton—the Islamic Republic of Iran. And when given the opportunity to come clean and admit what he had done—which could have allowed the government to attempt remediation of the ongoing damage he caused—Mr. Bolton said nothing.

The only conceivable explanation for Mr. Bolton's brazen conduct is that he thought he was above the law. Mr. Bolton's sentence should send the message that senior federal officials like him are not above the law; they must follow the same rules, regulations, and laws as everyone else. The consequences of mistakes in this arena are the same regardless of the clearance holder's position or stature. Mr. Bolton's ongoing exposure of real-time classified national defense information, by transmission over unsecure, non-governmental communications jeopardized the

most sensitive information held by the United States. A sentence of 60 months imprisonment, with a three-year term of supervised release, and the agreed-upon fine is sufficient, but not greater than necessary, to satisfy the goals of sentencing.

Respectfully submitted,

KELLY O. HAYES
United States Attorney

By: /s Thomas M. Sullivan
Thomas M. Sullivan
Assistant United States Attorney

CHRISTIAN J. NAUVEL
Acting Chief
Counterintelligence and Export Control Section
National Security Division
U.S. Department of Justice

By: /s Tanner Kroeger
Tanner Kroeger
Deputy Chief

By: /s Garrett Coyle
Garrett Coyle
Trial Attorney

cc: Erik Finneyfrock, U.S. Probation Officer (by email at Erik_Finneyfrock@mdp.uscourts.gov)