UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION

UNITED STATES OF AMERICA,

vs.

DONALD J. TRUMP,
WALTINE NAUTA, and
CARLOS DE OLIVEIRA,

Defendants.

Case No. 23-80101-CR
CANNON/REINHART

PRESIDENT TRUMP'S MOTION TO DISMISS THE INDICTMENT BASED ON SELECTIVE AND VINDICTIVE PROSECUTION

TABLE OF CONTENTS

INTRODUCTION

President Donald J. Trump respectfully submits that the Indictment must be dismissed on the basis of the Office's selective and vindictive prosecution.[1] "With one exception, there is no record of the Department of Justice prosecuting a former president or vice president for mishandling classified documents from his own administration." Hur Report at 10-11.[2] The exception is President Trump. The basis is his politics and status as President Biden's chief political rival. Thus, this case reflects the type of selective and vindictive prosecution that cannot be tolerated. Accordingly, further discovery and a hearing are necessary, and the Superseding Indictment must be dismissed. [3]

DISCUSSION

I. Relevant Facts

American history is chock full of public examples involving alleged mishandling of classified information and documents, which did not result in the type of politically motivated charges that the Special Counsel's Office has brought against President Trump and his co-defendants. Set forth below are some of the most glaring and egregious examples.

---

[1] President Trump reserves the right to supplement this motion and file any other motions based on discovery provided as a result of the motions to compel. *See* ECF No. 314.

[2] U.S. Dep't of Justice Special Counsel's Office, Report on the Investigation Into Unauthorized Removal, Retention, and Disclosure of Classified Documents Discovered at Locations Including the Penn Biden center and the Delaware Private Residence of President Joseph R. Biden, Jr., (Feb. 5, 2024) (the "Hur Report"), *available at* www.justice.gov/storage/report-from-special-counsel-robert-k-hur-february-2024.pdf.

[3] For purposes of this motion, President Trump respectfully incorporates by reference Part I of the Discussion Section from the Defendants' reply in further support of the Defendants' motion to compel discovery ("Compel Reply"), ECF No. 300. Certain authorities cited in the Compel Reply are included below for purposes of clarity. "Compel Mot." refers to the Defendants' opening motion to compel discovery, ECF No. 262. "Compel Oppn." refers to the Special Counsel's Office's response to the Compel Motion, ECF No. 277.

A. President Joseph Biden

After President Biden concluded his term as vice president in January 2017, "boxes containing classified documents, vice presidential records, and other items were stored in three different locations around the Washington, D.C. area, including an office near the White House, an office in Chinatown, and eventually the Penn Biden Center" in Washington, D.C. Ex. 1. The boxes at the Penn Biden Center "were not in a 'locked closet' . . . and remained accessible to Penn Biden employees as well as potentially others with access to the office space." *Id.*

On May 24, 2022—the same month that DOJ issued a grand jury subpoena to President Trump's Office—White House counsel Dana Remus instructed Kathy Chung, President Biden's former executive assistant, to retrieve the boxes from the Penn Biden Center. *See* Ex. 2 at 2; *see also* Hur Report at 257. On June 28, 2022, Ms. Chung packed 13 boxes at the Penn Biden Center, which "would later be found to have contained classified materials." Ex. 2 at 5; *see also* Hur Report at 259, 262 (Chung emailed Remus "13 boxes. There are clearly marked boxes with correspondence throughout 4 years.").

On October 13, 2022, Ms. Chung sent text messages to one of President Biden's personal attorneys indicating that the 13 boxes remained at the Penn Biden Center. Ex. 2 at 6-7. The messages indicated that "Dana" Remus "went there in June, but decided it was too much to take . . . ." *Id.* at 7; *see also* Hur Report at 262. The attorney responded that another lawyer for President Biden, who was based in Boston, had "begun to sort through" the boxes. Ex. 2 at 7; *see also* Hur Report at 258 ("Remus decided to ship material that could be relevant to future congressional inquiries to Patrick Moore . . . in Boston . . . .").

In early November 2022, President Biden's personal attorneys turned over classified documents that they claimed had been "discovered" at one of President Biden's personal offices.

Ex. 3 at 1. According to the Hur Report, on November 2, 2022, President Biden's attorneys found a "manila envelope marked 'EYES ONLY' for the Vice President" that contained "documents with classification markings." Hur Report at 266. The attorney contacted the White House Counsel's Office, which "notified" NARA's General Counsel, Gary Stern. *Id.* NARA determined that the boxes from the Penn Biden Center "included nine documents with classification markings totaling 44 pages." *Id.* at 271. The FBI later determined that the boxes contained 10 "classified or potentially classified" documents rather than nine. *Id.* at 273.

On January 12, 2023, President Biden disclosed that private attorneys had located another classified document in a garage at one of his residences in Delaware.[4] The same day, the Attorney General appointed Mr. Hur as Special Counsel to investigate these circumstances.[5] Two days later, the White House Counsel's Office disclosed that five additional classified documents had been recovered from one of President Biden's "Delaware residences." Ex. 4 at 2. On January 20, the FBI seized additional classified documents during a consensual search of President Biden's home in Delaware.[6] Whereas NARA issued a public statement regarding the illegal Mar-a-Lago raid, NARA General Counsel Gary Stern acknowledged during an interview later in January 2023 that

---

[4] Brett Samuels, *Five More Classified Documents Found at Biden's Wilmington Home, Lawyer Says*, THE HILL (Jan. 14, 2023, 12:02 pm), https://thehill.com/homenews/administration/3813424-five-more-classified-documents-found-at-bidens-wilmington-home-lawyer-says/.

[5] U.S. Dep't of Justice, Appointment of Robert K. Hur As Special Counsel (Jan. 12, 2023), *available at* https://www.justice.gov/d9/2023-01/Order.Appointment%20of%20Robert%20Hur.11223%20%28002%29.pdf.

[6] Zeke Miller, Michael Balsamo, and Colleen Long, *FBI Searched Biden Home, Found Items Marked Classified*, AP NEWS (Jan. 21, 2023, 11:34 PM), https://apnews.com/article/biden-politics-delaware-0827b59ee141b33af95023377713e075.

"someone outside of NARA" had blocked NARA's release of a public statement relating to the investigation of President Biden. Ex. 5 at 1.

In January 2023, the FBI found "roughly a dozen marked classified documents that are currently classified at the Secret level" in the garage of President Biden's home in Delaware. Hur Report at 175.

Between January and February 2023, the FBI also found seven "marked classified documents" in a collection of President Biden's Senate-era papers at the University of Delaware's Biden Institute. Hur Report at 318. In February 2023, the FBI retrieved a two-page State Department cable from 1987, which was marked classified but "determined" to have been "declassified in 2012," from President Biden's Senate papers at a University of Delaware library. Hur Report at 314. In June 2023, the FBI identified five additional "marked classified documents" during a consent search at the library. *Id.* at 315. The FBI also found additional "marked classified documents" in three notebooks, two binders, and a free-standing document at President Biden's home in Delaware. *E.g.*, Hur Report at 326-33.

Further, President Biden talked to Mark Zwonitzer, his ghost writer, about the contents of notebooks that contained information "classified up to the Top Secret level." *Id.* at 101. "[D]uring his dozens of hours of interviews with Zwonitzer, Mr. Biden read from notebook entries related to many classified meetings, including National Security Council meetings, CIA briefings. Department of Defense briefings, and other meetings and briefings with foreign policy officials." *Id.* at 106; *see also id.* at 103 ("Mr. Biden read his notes from classified meetings to Zwonitzer nearly word-for-word."). For example, during a February 2017 meeting at President Biden's rental home in Virginia, President Biden explained to Zwonitzer that he "just found all the classified stuff downstairs." *Id.* at 110.

In 2023, Zwonitzer "deleted digital audio recordings of his conversations with President Biden." Hur Report at 334. During a subsequent interview in 2023, Zwonitzer told Mr. Hur that "he 'was aware that there was an investigation' when he deleted the recordings and continued, 'I'm not going to say how much of the percentage it was of my motivation.'" *Id.* at 337-38.

B. Former Vice President Mike Pence

On January 18, 2023, counsel for Mike Pence disclosed to NARA that "a small number of documents bearing classified markings . . . were inadvertently boxed and transported to the personal home of the former Vice President at the end of the last Administration." Ex. 6. Pence had undertaken a search for those records in response to reports relating to President Biden's mishandling of classified information. *Id.* The following day, DOJ "bypassed the standard procedures" under the Presidential Records Act ("PRA"), "requested direct possession" of the documents, and sent FBI agents to Pence's Indiana residence to collect the documents late at night. Ex. 7 at 1.

On January 20, 2023, Pence's counsel agreed to turn over to NARA four additional boxes "containing copies of Administration papers": two boxes "in which a small number of papers appearing to bear classified markings had been found, and two separate boxes containing courtesy copies of Vice Presidential papers." Ex. 7 at 2. On February 10, 2023, the FBI conducted a consensual search of Vice President Pence's residence, which resulted in the seizure of an

additional classified document.[7] On June 2, 2023, DOJ reportedly notified Pence that no charges would be filed related to the classified documents.[8]

C. Former President Bill Clinton

As discussed above in connection with the *Judicial Watch* litigation, 845 F. Supp. 2d 288, 290-91 (D.D.C. 2012), President Clinton worked with historian Taylor Branch on a "secret project" to record President Clinton's observations and work as president between 1993 and 2001. Taylor Branch, *The Clinton Tapes: Wrestling History With the President* (2009) (the "*Clinton Tapes*").

President Clinton relied on the tapes for his 2004 autobiography, *My Life*, and Branch described them in *The Clinton Tapes*. The tapes obviously contain classified information, but President Clinton has been permitted to maintain them personally as a "unique verbatim record under his control." *Id.* at 13. Branch's published account confirms that the tapes contain the type of information that the Special Counsel's Office and the Intelligence Community have repeatedly contended are classified and sensitive, such as military operations, intelligence assessments, communications with foreign leaders, and the dates on which President Clinton was briefed on particular issues.

For example, according to Branch, the recordings reflect the following:

- During a meeting in 1996, President Clinton explained that, "[w]ith support only from England, [President] Clinton attacked [Iraq's] capability for larger military offensives. . . . [H]e sent cruise missiles against air-defense installations. B-52

[7] Ximena Bustillo, *FBI Finds an Additional Classified Document During 'Consensual' Search of Pence's Home*, NPR (Feb. 11, 2023, 7:14 AM), https://www.npr.org/2023/02/10/1154177170/mike-pence-fbi-search-home-office.

[8] Jeremy Herb and Katelyn Polantz, *Justice Department Will Not Seek Criminal Charges in Pence Classified Document Probe*, CNN (June 2, 2023, 10:46 AM), https://www.cnn.com/2023/06/02/politics/mike-pence-justice-department-documents/index.html.

bombers, flying round-trip from Guam, reinforced the missile strikes near Baghdad for two days." *Clinton Tapes* at 393.

- During a meeting in early 2000, President Clinton explained that "[o]ur experts . . . were convinced that an Algerian recently arrested in Seattle with bomb materials was a bin Laden disciple, indicating that bin Laden was 'up to stuff' in the United States. And India asserted that Pakistan was behind a spectacular Christmas Eve hijacking of an Indian jetliner into Kandahar, Afghanistan . . . ." *Id.* at 581.

- In late 2000, "on tape," President Clinton "discussed the October 12[, 2000] suicide attack against the *Cole* in the port of Aden, Yemen . . . The president said they thought the instigator was bin Laden. Our people knew where part of the bomb was made." *Id.* at 627.

- During a meeting in January 2001, President Clinton told Branch that President Bush "had listened without comment to most of Clinton's extensive briefing on foreign affairs. Unexpectedly, when asked, [President Bush] encouraged Clinton to seize any opening to stop the North Korean missile program. Bush said he could not imagine going there for at least the first year of his presidency, and if it took a presidential trip to seal the deal, he would hold no ill will toward Clinton for stealing the limelight or boxing in the new administration. *Id.* at 639.

As discussed in more detail in President Trump's motion to dismiss pursuant to the PRA, despite all of this, neither DOJ nor NARA even thought it possible to try to recover the tapes. There was no criminal investigation. There was no prosecution.

D. Hillary Clinton

Hillary Clinton was the Secretary of State between January 2009 and February 2013. In 2014, the House Committee investigating the September 2012 terrorist attack at the CIA Annex in Libya, which killed four Americans, requested records from the State Department. Horowitz OIG Report at 37.[9] While preparing to respond to the congressional inquiry, the State Department (and later DOJ) learned that Clinton had used a personal email account and three servers stored at her

[9] Office of the Inspector General, U.S. Dep't of Justice, A Review of Various Actions by the Federal Bureau of Investigation and Department of Justice in Advance of the 2016 Election (June 2018) (the "Horowitz OIG Report"), *available at* https://www.justice.gov/file/1071991/download.

private residence to conduct official business in that role. *See, e.g.*, Horowitz OIG Report at 76-77.

The first server was abandoned in March 2009 and "ultimately discarded," along with the records and data it contained. *See id.* Between March 2009 and June 2013, the second server was used to store data relating to email accounts used by Secretary Clinton and certain other State Department personnel for official business. *See id.* In December 2013, at Secretary Clinton's direction, a private vendor "migrated" the email accounts to a third server and removed Microsoft Exchange from the device. *See id.* This process involved the use of a laptop and a thumb drive to transfer the data, which Secretary Clinton's staff instructed the vendor to "wipe" and were never recovered. *See id.* at 78. By the time the FBI got access to the second server, the records and data were stored in the server's "unallocated space." *Id* at 77. The location was consistent with data deletion, and the FBI found that emails on the second server were "were often fragmented and difficult to reconstruct." *Id.*; *see also United States v. Rivenbark*, 748 F. App'x 948, 952 (11th Cir. 2018) ("Deleted files go into unallocated space on the hard drive . . . .").

The handling of data from the third server reflects even more astonishing levels of obstruction and evidence destruction. In December 2014, Clinton provided the State Department with hard copies of approximately 30,490 emails from her personal email account, which her attorneys recovered from the third server. Horowitz OIG Report at 1. Secretary Clinton's counsel claimed they had determined that those emails were "work related." *Id.* Around the same time—after the congressional inquiry was public—Secretary Clinton "decided she no longer wished to retain on her [third] server emails that were older than 60 days," and Secretary Clinton's staff accessed the vendor to "remove former Secretary Clinton's emails from their laptops." *Id.* at 38.

The technician used a program called "BleachBit" to "permanently remove or wipe" the emails from the laptops. *Id.*

On March 3, 2015, Congress sent a preservation order to Secretary Clinton. Horowitz OIG Report at 39. Secretary Clinton's attorneys advised the vendor of the order. *Id*. The technician told the FBI that, "despite the intervening issuance of a congressional preservation order," "he 'had an oh shit moment'" and "wiped" Secretary Clinton's emails from the third server at a point "between March 25 and March 31, 2015." Horowitz OIG Report at 79. By using "BleachBit"—a program designed to "shred" files and "prevent recovery"—Secretary Clinton's vendor "permanently remove[d]" approximately 31,830 emails from the third server. *Id.* at 38 n.48 and 39.

During the investigation that followed, the FBI, "with the assistance of other USIC agencies, identified 81 email chains containing approximately 193 individual emails that were classified from the CONFIDENTIAL to TOP SECRET levels at the time the emails were drafted on UNCLASSIFIED systems and sent to or from Clinton's personal server.'" *Id.* at 74 (cleaned up).

> In other words, the USIC agencies determined that these 81 email chains, although not marked classified, contained information classified at the time the emails were sent and should have been so marked. Twelve of the 81 classified email chains were not among the 30,490 that Clinton's lawyers had produced to the State Department, and these were all classified at the Secret or Confidential levels. Seven of the 81 email chains contained information associated with a Special Access Program ("SAP"), which witnesses told us is considered particularly sensitive. The emails containing Top Secret and SAP information were included in the 30,490 provided to the State Department.

Horowitz OIG Report at 74. The FBI also "assess[ed] that hostile actors gained access to the private commercial email accounts of people with whom Secretary Clinton was in regular contact from her personal account," and that it was "possible that hostile actors gained access to Secretary Clinton's personal email account." *Id.* at 75-76.

During the summer of 2016, through consultation with the Attorney General, a team of DOJ prosecutors led by George Toscas—who is also participating in this prosecution, *see, e.g.*, Compel Mot. Ex. 35—decided not to charge Secretary Clinton (or anyone else) with crimes relating to (1) the use of private email accounts and a private server to transmit classified information, (2) the subsequent deletion of classified information and official State Department records, and (3) obstruction of the congressional inquiry, including by violating the preservation order. *See* Horowitz OIG Report at 253-57.

E. James Comey

Between January and April 2017, former FBI Director James Comey wrote seven emails or memoranda that he claimed memorialized interactions with President Trump. JC OIG Report at 1.[10] The FBI later determined that four of the documents contained information that was classified at the Secret and Confidential levels. *See id.* at 1, 42-46. Comey wrote one of the classified memoranda on his personal computer. *Id.* at 11 (Memo 2).

On May 9, 2017, President Trump removed Comey from his position. Comey subsequently used a personal scanner and his personal email account to send two of the classified memoranda to his personal attorneys. JC OIG Report at 12, 36-37 (Memos 2, 7). On May 12, FBI agents went to Director Comey's residence to "inventory and retrieve all FBI property from Comey's home SCIF." *Id.* at 34. "Comey did not tell the FBI that he had copies of" four of the memoranda, including two classified documents, "in his personal safe." *Id.* (Memos 2, 4, 6, 7).

[10] Office of the Inspector General, U.S. Department of Justice, Report of Investigation of Former Federal Bureau of Investigation Director James Comey's Disclosure of Sensitive Investigative Information and Handling of Certain Memoranda (Aug. 2019) (the "JC OIG Report"), *available at* https://www.oversight.gov/sites/default/files/oig-reports/o1902.pdf.

Comey had previously provided copies of the memoranda to FBI personnel, and they preserved those documents. *Id.* An FBI whistleblower provided the memoranda to DOJ-OIG. *Id.* at 37.

On June 7, 2017, when the FBI informed Director Comey of its classification decisions, he "provided the [FBI agent] who came to his home" with "signed originals" of the four memoranda he had "retained at his residence"—including the two classified documents. JC OIG Report at 48 (Memos 2, 4, 6, 7). Director Comey "never informed the FBI" that he had used his private scanner and private email account to transmit the same four memoranda, including the two classified documents, to his personal attorneys. JC OIG Report at 49. Rather, the FBI learned of that conduct through another witness.

F. General David Petraeus

In 2015, former CIA Director General David Petraeus was permitted to plead guilty to a misdemeanor violation of 18 U.S.C. § 1924 based on his handling of eight notebooks that "contained classified information regarding the identities of covert officers, war strategy, intelligence capabilities and mechanisms, diplomatic discussions, [and] quotes and deliberative discussions from high-level National Security Council meetings." Ex. 8 ¶ 17. General Petraeus "personally retained" the notebooks rather than turning them over to a Defense Department historian, and he later maintained the materials at private residences. *Id.* ¶ 20. In 2011, General Petraeus told his "biographer" that the notebooks were "highly classified" and contained "'code word' information," and he allowed the "biographer" to access the notebooks at his private residence in Washington, D.C. *Id.* ¶¶ 22, 24-25. The FBI seized the notebooks from General Petraeus's home. *Id.* ¶ 29. Based on the misdemeanor guilty plea, General Petraeus was sentenced principally to two years' probation.

G. Samuel "Sandy" Berger

Sandy Berger, President Clinton's National Security Advisor, was also permitted to plead guilty to a misdemeanor violation of § 1924, even though NARA has listed Berger's case on its website as one of the "Notable Thefts From The National Archives."[11]

In 2003, Berger stole five classified Presidential Records from NARA relating to the 9/11 Attack. Ex. 9 at ¶ 3-5. Berger concealed the records at an office, and he "cut three of the documents into small pieces and discarded them." *Id.* ¶ 4. When NARA confronted Berger, he "[i]nitially . . . did not tell NARA that he had taken the documents." *Id.* ¶ 6. Berger later claimed that "he had accidentally misfiled documents and had found two." *Id.* Based on the misdemeanor guilty plea, Berger was sentenced principally to two years' probation.

H. John Deutch

John Deutch served as CIA Director for President Clinton between 1995 and 1996. In that role, Deutch "continuously processed classified information on government-owned desktop computers configured for unclassified use," which "were connected to or contained modems that allowed external connectivity to computer networks such as the Internet" and thus "vulnerable to attacks by unauthorized persons." Ex. 10 at 3. In addition, while working at the Defense Department between 1993 and 1994, Deutch "routinely entered data on Government-owned computers, at his office and home not designated to process classified information," including "a

[11] *Notable Thefts from the National Archives*, NAT'L ARCHIVES, www.archives.gov/research/recover/notable-thefts.html ("During his visits to the Archives, it was determined that Berger folded the documents in his clothes, walked out of the National Archives building in Washington, D.C., and placed them under a nearby construction trailer for retrieval later on. Two years later Berger was sentenced to 100 hours of community service and probation and fined $50,000.").

daily journal containing classified information that was almost 1,000 pages in length, [maintained] on computer memory cards, that he reportedly transported in his shirt pocket." Ex. 11 at 2.

Although Deutch had reportedly agreed to plead guilty to a misdemeanor violation of § 1924, President Clinton pardoned Deutch on his last day in office.[12]

I. Deborah Birx

Deborah Birx acted as the White House Coronavirus Response Coordinator between 2020 and 2021. On September 6, 2021, NARA's General Counsel wrote in an internal email that NARA was "arranging to pick up the PRA materials from Dr. Birx on Tuesday (tomorrow)." Ex. 12. A separate internal NARA email thread on September 16 noted that Birx had at least "six boxes," and that "[s]canning Dr. Birx'[s] correspondence has been slowed because they found a classified document in the mix." Ex. 13. To our knowledge, Dr. Birx is not under investigation and is not being prosecuted.

II. Applicable Law

A. Selective Prosecution

The government may not pursue cases "with an evil eye and an unequal hand so as practically to make unjust and illegal discrimination between persons in similar circumstances . . . ." *Yick Wo v. Hopkins*, 118 U.S. 356, 373-74 (1886). Prosecutors "must exercise their charging discretion within constitutional constraints, including those imposed by the equal protection component of the Due Process Clause of the Fifth Amendment." *United States v. Smith*, 231 F.3d 800, 807 (11th Cir. 2000) (cleaned up). Under the Due Process Clause, a prosecution decision "may not be based on an unjustifiable standard . . . or arbitrary classification." *Id.* "In order to

[12] Bill Miller and Walter Pincus, *Deutch Had Signed Plea Agreement, Sources Say*, WASH. POST (Jan. 23, 2001, 7:00 PM), https://www.washingtonpost.com/archive/politics/2001/01/24/deutch-had-signed-pleaagreement-sources-say/dcebcd40-24d5-47e9-8c3c-6fe2c3c3c8a0/.

establish unconstitutional selective prosecution, the claimant must show [1] that the prosecution has a discriminatory effect and [2] that it was motivated by a discriminatory purpose." *United States v. Emmanuel*, 2007 WL 9705934, at *2 (S.D. Fla. July 3, 2007) (cleaned up).

"The first prong, discriminatory effect, is demonstrated by a showing that similarly-situated individuals were not prosecuted for the same crime." *Id.* (cleaned up). "[A] 'similarly situated' person for selective prosecution purposes as one who engaged in the same type of conduct . . . ." *Smith*, 231 F.3d at 810.

"The second prong, discriminatory purpose, is demonstrated by a showing that the decision to prosecute was invidious or in bad faith." *Emmanuel*, 2007 WL 9705934, at *2 (cleaned up). This includes prosecutions "predicated on a constitutionally impermissible motive, such as on the basis of race or religion, or in retaliation for her exercise of constitutional rights." *United States v. Ndiaye*, 434 F.3d 1270, 1288 (11th Cir. 2006).

"A defendant may obtain discovery in support of a selective prosecution claim where the defendant provides some evidence tending to show the existence of the essential elements of the defense." *United States v. Williams*, 684 F. App'x 767, 777 (11th Cir. 2017) (cleaned up).

B. Vindictive Prosecution

"The government violates a defendant's due process rights when it vindictively seeks to retaliate against him for exercising his legal rights." *United States v. Schneider*, 853 F. App'x 463, 469 (11th Cir. 2021). "A defendant can establish actual prosecutorial vindictiveness if he can show that the government's justification for a retaliatory action is pretextual." *Id.*

"To establish prosecutorial vindictiveness, a defendant must show, through objective evidence, that (1) the prosecutor acted with genuine animus toward the defendant and (2) the

defendant would not have been prosecuted but for that animus." *United States v. Simbaqueba Bonilla*, 2010 WL 11627259, at *5 (S.D. Fla. May 20, 2010) (cleaned up).

III. Discussion

"Nothing is so politically effective as the ability to charge that one's opponent and his associates are not merely wrongheaded, naive, ineffective, but, in all probability, 'crooks.' And nothing so effectively gives an appearance of validity to such charges as a Justice Department investigation and, even better, prosecution." *Morrison v. Olson*, 487 U.S. 654, 713 (1988) (Scalia, J., dissenting). Through two lawless prosecutions initiated at the express urging of the Biden Administration, including this case, the Special Counsel's Office seeks to "become a de facto campaign voice for the Democrats in the general election," and Jack Smith is "probably less concerned now with whether a Trump conviction will survive appeal than with whether Trump can be convicted ahead of the November 2024 election."[13]

Despite decades of similar conduct, no former president has been charged with the crimes the Special Counsel's Office has alleged in this case. Dozens of public officials have faced allegations relating to the handling of classified information without being charged with the types of felonies alleged in the Superseding Indictment. In this case, the record adequately demonstrates

[13] *See, e.g.*, Opinion, *Jack Smith and the Supreme Court*, WALL ST. J. (Dec. 15, 2023, 6:40 PM), https://www.wsj.com/articles/jack-smith-and-the-supreme-court-57d78846 ("If that trial date [in the District of Columbia] holds, Mr. Smith will . . . then become a de facto campaign voice for the Democrats in the general election. This is one of the reasons that trying to disqualify Mr. Trump by prosecution was such a mistake."); *see also* Steven Calabresi, *Donald Trump is the Victim of Selective Prosecution*, THE VOLOKH CONSPIRACY (Feb. 10, 2024), https://reason.com/volokh/2024/02/10/donald-trump-is-the-victim-of-selective-prosecution/; Jason Willick, *Politics Are Now Clearly Shaping Jack Smith's Trump Prosecution*, WASH. POST (Dec. 12, 2023, 1:33 PM), https://www.washingtonpost.com/opinions/2023/12/12/special-counsel-jack-smith-politicized-prosecution ("Smith is probably less concerned now with whether a Trump conviction will survive appeal than with whether Trump can be convicted ahead of the November 2024 election.").

impermissible prosecutorial motives, driven in an unprecedented fashion by a sitting president to serve his political objective of prosecuting his predecessor and opponent. The selective and vindictive prosecution doctrines forbid such behavior. Accordingly, the Court require the Special Counsel's Office to produce relevant discovery, hold a hearing, and then dismiss the Superseding Indictment. *See, e.g.*, *Williams*, 684 F. App'x at 777 (reasoning that the threshold for a hearing on selective and vindictive prosecution is a defense proffer of "some" evidence).

A. Impermissible Bias And Animus

With respect to selective prosecution, there is ample evidence that this case has been brought based on impermissible considerations relating to President Trump's candidacy and First Amendment-protected speech relating to his campaign. *See United States v. Falk*, 479 F.2d 616, 620 (7th Cir. 1973) ("[J]ust as discrimination on the basis of religion or race is forbidden by the Constitution, so is discrimination on the basis of the exercise of protected First Amendment activities, whether done as an individual or, as in this case, as a member of a group unpopular with the government."); *United States v. Crowthers*, 456 F.2d 1074, 1079 (4th Cir. 1972) ("What the government has done here is to undertake to suppress a viewpoint it does not wish to hear under the guise of enforcing a general regulation prohibiting disturbances on government property."); *United States v. Judd*, 579 F. Supp. 3d 1, 4 (D.D.C. 2021) ("[T]he Government cannot base its decision to prosecute on some unjustifiable standard, such as a defendant's political beliefs."). The prosecution is "vindictive" because it has been brought in an effort to punish President Trump for exercising those rights on behalf of the American people. *See United States v. Barner*, 441 F.3d

1310, 1315 (11th Cir. 2006) ("Vindictiveness in this context means the desire to punish a person for exercising his rights.").[14]

The record contains much more than "some" evidence on this issue. *Williams*, 684 F. App'x at 777. In April 2022, the Biden Administration leaked to the *New York Times* President Biden's view that President Trump "should be prosecuted" and his instruction that Attorney General Garland should "take decisive action." Compel. Mot. Ex. 62. The following month, DOJ issued a grand jury subpoena to President Trump's Office seeking additional records. Less than four months later, DOJ worked with the FBI to raid Mar-a-Lago, with Toscas—the same DOJ official who helped oversee the non-prosecution of Hillary Clinton—declaring that he did not "give a damn about the optics." Compel. Mot. Ex. 35.

After President Biden's subordinates had started to gather classified records from the Penn Biden Center during the summer of 2022, Biden endorsed the Mar-a-Lago raid during a September 2022 *60 Minutes* interview in which he presumed President Trump guilty. In that session, with unappreciated irony, President Biden characterized the circumstances as "totally irresponsible,"

[14] With respect to the First Amendment freedoms implicated by this impermissible prosecution, see, for example, *Snyder v. Phelps*, 562 U.S. 443, 451-52 (2011) ("[S]peech concerning public affairs is more than self-expression; it is the essence of self-government." (cleaned up)); *Rosenberger v. Rector & Visitors of Univ. of Virginia*, 515 U.S. 819, 829 (1995) ("When the government targets not subject matter, but particular views taken by speakers on a subject, the violation of the First Amendment is all the more blatant."); *Meyer v. Grant*, 486 U.S. 414, 425 (1988) (reasoning that speech "at the core of our electoral process" is "an area … where protection of robust discussion is at its zenith" (cleaned up)); *see also* Packingham v. North Carolina, 582 U.S. 98, 104 (2017) (recognizing the right to "speak and listen, and then . . . speak and listen once more," as a "fundamental principle of the First Amendment"); *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 757 (1976) ("Freedom of speech presupposes a willing speaker. But where a speaker exists, . . . the protection afforded is to the communication, to its source and to its recipients both.").

asked "[h]ow that could possibly happen[?]," and expressed concern about "[w]hat data was in there that may compromise sources and methods?" *See* Hur Report at 7.[15]

In November 2022, through remarks that were plainly timed based on rumors of President Trump's candidacy, President Biden declared just days before that announcement that he was "making sure" President Trump "will not take power" and "does not become the next President again." In stark contrast, and without credibility, Attorney General Garland claimed at the time that Smith's appointment "underscore[d]" DOJ's "commitment" to "independence."[16] The same Attorney General confirmed DOJ's backing of Smith's improper actions during an interview last month in which he inappropriately sought to place DOJ's imprimatur behind the Office's untenable demand for a "speedy trial" in this case and on the lawless charges filed in the District of Columbia.[17]

Without question, this is a "high-profile prosecution with international ramifications no less," which has a "far greater potential to give rise to a vindictive motive." *United States v. Slatten*, 865 F.3d 767, 799-800 (D.C. Cir. 2017). Thus, the record is sufficient to establish—on a *prima facie* basis, at minimum—that Jack Smith "was prevailed upon to bring the charges by another with animus such that the prosecutor could be considered a 'stalking horse.'" *United States v. Sanders*, 211 F.3d 711, 717 (2d Cir. 2000).

---

[15] *See* Scott Pelley, *President Joe Biden: The 2022 60 Minutes Interview*, CBS NEWS (Sept. 18, 2022, 7:43 PM), https://www.cbsnews.com/news/president-joe-biden-60-minutes-interview-transcript-2022-09-18.

[16] DOJ, Appointment of a Special Counsel (Nov. 18, 2022), https://www.justice.gov/opa/pr/appointment-special-counsel-0.

[17] Evan Perez, Holmes Lybrand and Hannah Rabinowitz, *Exclusive: Attorney General Merrick Garland Says There Should Be 'Speedy Trial' of Trump as 2024 Election Looms*, CNN (Jan. 19, 2024, 8:25 AM), https://www.cnn.com/2024/01/19/politics/merrick-garland-trump-speedy-trial/index.html.

B. Similarly Situated Cases Support Defendants' Motion

There are several "similarly situated individuals [who] were not prosecuted." *Smith*, 2321 F.3d at 810. The comparators were alleged to have "committed the same basic crime in substantially the same manner" as the allegations in the Superseding Indictment, which President Trump disputes, and "the evidence was as strong or stronger than" than what the Special Counsel's Office has collected in this case during an investigation that involved abusing the grand jury, raiding Mar-a-Lago in an unconstitutional fashion, and illegally violating President Trump's attorney-client privilege. *Id.*

In 2015, the Society of American Archivists observed that, "[d]espite the fact that records management laws and regulations have been on the books for decades, non-compliance with the letter and spirit of accountability and transparency, which are inherent in these statutes, is a regular occurrence." In February 2022, [redacted] Per. 53 [redacted], told the FBI that "it is not uncommon for NARA to receive materials, over time, from senior US Government leaders which contain some level of classified materials and information." Compel Mot. Ex. 2 at USA-00813152. During congressional testimony in March 2023, Mark Bradley from NARA's Information Security Oversight Office explained that, since 2010, NARA has received "over 80 calls" from libraries where "mostly Members of Congress have taken papers" that included classified information. Intelligence Committee Tr. 12-13.[18] At the same hearing, Bosanko explained that for "every PRA administration from Reagan forward," NARA has "found classified information in unclassified boxes." *Id.* at 63. Bosanko added that "[c]lassified [information] has

[18] Transcript – U.S. House of Rep., Permanent Select Comm. on Intelligence, Washington, D.C. (Mar. 1, 2023) (the "Intelligence Committee Tr."), *available at* https://intelligence.house.gov/uploadedfiles/3.1.23_nara_briefing_transcript.pdf.

been going outside of government control for an extended period of time," and that "[m]ore often than not it is not due to a lack of care or respect for classified [information." *Id.* at 32.

Evidence of non-prosecution in instances of high-profile mishandling of classified information dates back to at least *New York Times v. United States*, 403 U.S. 713 (1971). There, Chief Justice Burger noted that the *New York Times* had "unauthorized possession" of a "classified study entitled 'History of U.S. Decision-Making Process on Viet Nam Policy'" for "three to four months." 403 U.S. at 750 (Burger, C.J., dissenting); *id.* at 714. No charges resulted, and we are unaware of the federal government using criminal processes such as subpoenas or search warrants to recover the materials.

> A congressionally commissioned study found in 1977 that, when leaving office, past presidents routinely took national security files including briefing materials for the President, records of negotiations with foreign governments, correspondence with foreign heads of state or governments, and correspondence with or directives to agencies within the Executive branch on foreign affairs.

Hur Report at 192 (cleaned up). No prosecutor brought charges, under the Espionage Act or otherwise, based on this established practice.

"[T]here is some reason to think" that diaries authored by Presidents Carter and Geroge H.W. Bush during their presidencies, and subsequently retained as their personal records, "contained classified information." Hur Report at 194 n.783. They were not prosecuted. The "historical record is clear" that President Reagan's diaries contained classified information "up to the Top Secret/Sensitive Compartmented Information level." *Id.* at 194 & n.783. "The Department of Justice, the National Archives, and others knew that President Reagan treated [President Reagan's] diaries (containing classified information) as personal property, but no agency took action to recover the classified materials or to investigate or prosecute the former president." *Id.* at 193-94. It was common knowledge that President Reagan kept the diaries "at

his private home, apparently outside of facilities that were authorized to store Top Secret information." *Id.* at 196. No charges were filed, and it does not appear that there was even an investigation. After President Reagan died, NARA confirmed through work with the National Security Council that several pages of material from President Reagan's diaries was "still classified up to the Top Secret/Sensitive Compartmented Information level." *Id.* at 198.

More recently, President Biden spread out classified documents across non-SCIF residences, garages, and private office space in three states and the District of Columbia dating back decades to his time in the Senate. In contrast to President Biden's *60 Minutes* interview following the Mar-a-Lago raid, he joked to the press that he had stored classified documents "in a locked garage" with his "Corvette."[19] The photographs of that garage in the Hur Report demonstrate that it was far less secure than Mar-a-Lago, which is and was under the constant protection of the United States Secret Service and private security. And Mr. Hur found that President Biden acted "willfully":

> There is evidence that, after his vice presidency, Mr. Biden willfully retained marked classified documents about Afghanistan and unmarked classified handwritten notes in his notebooks, both of which he stored in unsecured places in his home. He had no legal authority to do so, and his retention of these materials, and disclosure of classified information from his notebooks to his ghostwriter, risked serious damage to America's national security.

Hur Report at 200. Yet there will be no charges. *See id.* ("The Department's prior treatment of former presidents and vice presidents who kept national security materials also counsels against prosecution of Mr. Biden.").

---

[19] Kelly Hooper, *Additional Documents Marked Classified Found in Biden's Wilmington Garage*, POLITICO (Jan. 12, 2023, 10:39 AM), https://www.politico.com/news/2023/01/12/additional-documents-marked-classified-found-in-bidens-wilmington-garage-00077680; *Biden Says Classified Documents Were in Locked Garage With His Corvette*, YOUTUBE (Jan. 12, 2023), https://www.youtube.com/watch?v=J5qrb0NsF9U.

The same result for Vice President Pence, following an investigation by DOJ that concluded—coincidentally or not—just in time for Pence to declare his since-terminated candidacy in the 2024 election. Both President Biden and former Vice President Pence returned classified documents during an iterative process, but no one inferred obstructive intent from the multiple disclosures. Unlike President Trump, both men were offered an opportunity to consent to FBI searches rather than being forced to face the public spectacle of having their private homes raided by armed agents.

Despite prolonged mishandling of classified information and extensive deletion of evidence, no member of the Clinton family has been charged with a crime. Hillary Clinton led the State Department using a private email account, routed over servers at her private residence, to communicate regarding the type of foreign affairs matters the Special Counsel's Office and the Intelligence Community relegate to basement SCIFs in this case. The FBI identified 193 classified emails in the data that Clinton did not cause to be deleted, and we will never know the extent of the classified information in the data she caused to be destroyed using "BleachBit," at least "two instances" where an aid "destroyed Clinton's old mobile devices by breaking them in half or hitting them with a hammer,"[20] and other methods. But no charges followed. The decision was supported by the same George Toscas who did not "give a damn about the optics" of the Mar-a-Lago raid. Compel Mot. Ex. 35 at USA-00940276.

Former President Clinton possessed, and may still possess, tapes that obviously contain classified information. The tapes serve as conclusive evidence that he disclosed classified information to Branch. But no one in the government lifted a finger. Not even NARA. Years

[20] U.S. Dep't of Justice Fed. Bureau of Investigation, Clinton E-Mail Investigation (July 2016), *available at* https://vault.fbi.gov/hillary-r.-clinton/Hillary%20R.%20Clinton%20Part%2001/view.

later, however, Archivist Ferriero would run "out of patience" with President Trump within six months of the end of his term. Branch's book regarding Clinton's presidency, the *Clinton Tapes*, contains details that would almost certainly be deemed classified if they had been revealed by President Trump and were subject to a classification review by the biased Intelligence Community operatives supporting this prosecution.

James Comey disseminated classified information to private parties *regarding meetings with President Trump*. Like President Biden and the Clintons, he maintained classified records regarding those communications at his residence and faced no charges for that decision. It does not appear that Dr. Birx faced charges or even an investigation despite the fact that she (1) retained possession of "PRA materials" until at least September 2021, long after Ferriero was "out of patience" with President Trump, and (2) those materials contained at least one classified document. General Petraeus, Sandy Berger, and John Deutch all mishandled extremely sensitive classified information. *See* Hur Report at 251 n.958 (explaining that "there was stronger evidence of willfulness in Petraeus's case, in light of his lies and obfuscations," General Petraeus "was charged only with a misdemeanor"). Deutch, for example, "continuously processed classified information" on an unclassified computer. Each of these three was permitted to plead guilty to a misdemeanor.

Finally, the unproven obstruction allegations by the Special Counsel's Office cannot save this prosecution. Hillary Clinton and her colleagues deleted 31,830 emails and destroyed data on numerous electronic devices, including after a congressional preservation order. Comey hid from the FBI that he had used a private scanner and his personal email account to transmit at least two classified documents to his personal attorneys. Berger stole documents from NARA and cut three of them "into small pieces," which resulted in NARA having informal "'Sandy Berger' rules." Ex.

13. None of these individuals faced a charge under the Espionage Act or was prosecuted for obstruction.

Collectively, this history of non-prosecution and leniency for similarly situated individuals and others strongly supports President Trump's motion based on intolerable and unconstitutional selective and vindicative prosecution. Discovery and a hearing are necessary, and the Court should dismiss the Superseding Indictment.

CONCLUSION

For the foregoing reasons, President Trump respectfully submits that the Court should order necessary discovery and a hearing, and thereafter dismiss the Superseding Indictment.

Dated: February 22, 2024

Respectfully submitted,

/s/ Todd Blanche
Todd Blanche (PHV)
toddblanche@blanchelaw.com
Emil Bove (PHV)
emil.bove@blanchelaw.com
BLANCHE LAW PLLC
99 Wall Street, Suite 4460
New York, New York 10005
(212) 716-1250

/s/ Christopher M. Kise
Christopher M. Kise
Florida Bar No. 855545
ckise@continentalpllc.com
CONTINENTAL PLLC
255 Alhambra Circle, Suite 640
Coral Gables, Florida 33134
(305) 677-2707

Counsel for President Donald J. Trump

CERTIFICATE OF SERVICE

I, Christopher M. Kise, certify that on February 22, 2024, I filed the foregoing document and served it on the Special Counsel's Office via email, or CM/ECF to the extent possible, as required by the Court's February 20, 2024 Order. ECF No. 320.

/s/ Christopher M. Kise
Christopher M. Kise

EXHIBIT 1

Press Release Published: Apr 4, 2023

Chairman Comer's Statement on Transcribed Interview with Kathy Chung

WASHINGTON—House Committee on Oversight and Accountability Chairman James Comer (R-Ky.) issued the following statement on today's transcribed interview with Kathy Chung, who served as assistant to Joe Biden when he was Vice President:

"I thank Kathy Chung for her cooperation with the Oversight Committee's investigation into President Biden's mishandling of classified documents. She provided startling information that undermines the Biden White House's narrative on the matter.

"Today we learned that when Joe Biden left the vice presidency, boxes containing classified documents, vice presidential records, and other items were stored in three different locations around the Washington, D.C. area, including an office near the White House, an office in Chinatown, and eventually the Penn Biden Center. At some point, the boxes containing classified materials were transported by personal vehicles to an office location. The boxes were not in a 'locked closet' at the Penn Biden Center and remained accessible to Penn Biden employees as well as potentially others with access to the office space. We need to find out who had access to these documents.

"We also learned today that then-White House Counsel Dana Remus tasked Kathy Chung with retrieving these boxes from the Penn Biden Center as early as May 2022. This story does not begin in November 2022, as represented by President Biden's attorney.

"In the coming days, the Oversight Committee will follow up with persons of interest in this investigation."

Related

Press Release
Oversight and Judiciary Committees Release Tony Bobulinski Transcript
February 16, 2024

Press Release
Hearing Wrap Up: Americans Deserve Improved Vaccine Injury and Compensation Systems
February 16, 2024

Press Release
Hearing Wrap Up: Biden Administration's Catch and Release Operation Has Inflamed the Raging Crisis at the Southern Border
February 16, 2024

Press Release
Comer & Oversight Republicans Probing Biden Administration's Funding of UN Group with Ties to Hamas
February 16, 2024

EXHIBIT 2

JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED EIGHTEENTH CONGRESS

JAMIE RASKIN, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
https://oversight.house.gov

May 5, 2023

Dana Remus
Covington & Burling LLP
850 10th St. NW
Washington, D.C. 20268

Dear Ms. Remus:

The Committee on Oversight and Accountability is investigating President Biden's mishandling of highly classified documents.[1] The Committee has obtained information that contradicts important details from the White House's and President Biden's personal attorney's statements about the discovery of documents at the Penn Biden Center, including the location and security of the classified documents. The Committee has learned that you were a central figure in the early stages of coordinating the packing and moving of boxes that were later found to contain classified materials. Following a recent transcribed interview with Ms. Kathy Chung—the President's former assistant from when he was Vice President and subsequent employee of then former Vice President Biden's company, CelticCapri—the Committee has identified you as a witness with potentially unique knowledge about this matter and requests information from you.

The Committee's interview with Ms. Chung raised several questions to which the Committee believes you possess certain answers. Generally, these questions involve differences between Ms. Chung's account and the statements released separately by the White House and President Biden's personal attorney. Specifically, the Committee seeks clarification regarding the timeline of events prior to November 2, 2022 (the day, according to the White House and the President Biden's personal attorney, documents were discovered at Penn Biden Center), the security of the documents in the Penn Biden Center before and after Ms. Chung packed them, and President Biden's history of potentially mishandling classified material.

A. <u>The Committee seeks additional information about why in May 2022 you chose Ms. Chung—an employee at the Department of Defense who did not work for the Penn Biden Center—to do what she believed was a personal task for the President.</u>

The President's personal attorney, Mr. Bob Bauer, has released a statement that includes a timeline of events relevant to President Biden's mishandling of classified documents. That

[1] *See, e.g.*, Alexander Mallin, et al., *Key events in the Biden classified documents probe: Updated timeline*, ABCNews.com (Feb. 1, 2023).

timeline begins on November 2, 2022, with the "unexpected[] discover[y]" of classified materials at the Penn Biden Center.[2] Additionally, the White House has stated the "documents were discovered when the President's personal attorneys were packing files housed in a locked closet to prepare to vacate office space at the Penn Biden Center in Washington, D.C."[3]

The supposed timeline omitted nearly six months of communications between the White House and President Biden's personal attorney and Ms. Chung—an employee of the Department of Defense—to pack up and move documents located in the Penn Biden Center that began in May 2022. According to Ms. Chung and an email produced to the Committee, you contacted her on May 24, 2022, after not having spoken to Ms. Chung for approximately a year and a half, when she worked for the Biden presidential campaign.[4] Ms. Chung stated:

> Q It appears from the email that White House counsel Dana Remus called you prior to emailing you. Do you remember if she called you on your government phone or on your private phone?
>
> A My private phone.
>
> Q When she asked you if there was something -- or when she referenced here that she had something to run by you, at this point did you have any indication or did you have any knowledge of what it was that she wanted to talk about?
>
> A No.
>
> Q Prior to receiving the voicemail and this email, when was the last time you had spoken to Dana Remus?
>
> A A long time. Probably during the campaign.
>
> Q And, again, this is approximate, but approximately when do you think that was? You can give a year.
>
> A A year and a half.[5]

Ms. Chung previously worked for President Biden as his assistant when he was Vice President. During the final days of the Obama-Biden Administration, Ms. Chung packed up several moving boxes with materials from the West Wing, including files that she did not review and personal items. She stated:

---

[2] Statement from Bob Bauer, Personal Attorney for the President.
[3] Statement of Richard Sauber, Special Counsel to the President.
[4] Transcript of H. Comm. on Oversight & Accountability interview with Kathy Chung ("Transcript"), p. 15.
[5] *Id.*

Q Going back to initially when these documents were being packed up in the West Wing, can you explain that process for us as to how they were packed up and what the documents were that you can remember?

A We did it by -- we had -- he had a lot of stuff, primarily, you know, a lot of mementos, photos, framed photos, a lot of books.

We had to keep the office sort of functioning, so we just, you know -- so we packed those up. And then the documents or any files we just -- you know, we gathered and put in a box for moving.

[….]

Q Okay. And what type of activities did you undertake? So, for example, did you sort through files and pack boxes?

A No.

Q No[?]

A We did not sort through files.[6]

Ms. Chung worked as then Vice President Biden's assistant from July 2012 to the end of the Obama-Biden Administration:

Q What was your position with the Vice President?

A Assistant to the Vice President.

Q And as the Assistant to the Vice President, what were your job duties?

A Primarily is -- was going through his day-to-day calendar with him, schedule.

Q When did you begin that job?

A July of 2012.

Q And how did you come to interview for that position?

[6] Transcript, p. 20-21, 56-57.

A I was -- I was -- Hunter Biden called me and asked me if I was interested in the position.

Q And Hunter Biden is now-President Biden's son, correct?

A Yes.

Q And how long did you have that position with Vice President Biden at the time?

A I started there at July 2012, and I finished the administration with him.[7]

After the Obama-Biden Administration ended, Ms. Chung was employed by then former Vice President's corporate entity, CelticCapri. Employees of CelticCapri (including Ms. Chung) worked out of and had access to the Penn Biden Center:

Q What did you do after the Obama-Biden administration transitioned?

A After we left office, the Vice President had a- opened up a private entity, and I went with him.

Q Do you remember the name of that private entity?

A CelticCapri.

Q Where was that located?

A We ended up in Penn Biden Center.[8]

In May 2022, you contacted Ms. Chung about packing and moving materials in the President's office at the Penn Biden Center, but she was not aware—contrary to the explanation given by the White House in January 2023—of any plan to vacate the office. Ms. Chung explained:

Q Now, in May of 2022, when Ms. Remus first reached out to you about those documents, was it surprising to you that the White House was reaching out to make sure that those documents were properly packed up and -- I'm sorry. Let me restart that question.

[7] Transcript, p. 7-8.
[8] Transcript, p. 11.

> In May 2022, when Ms. Remus first reached out to you, was the vice -- were plans in progress to close down the Penn Biden Center now that the Vice President was in the White House?
>
> A No. Not that I'm aware of.[9]

Instead, according to Ms. Chung, you contacted her to pack up the Penn Biden Center documents because "they were his documents, [and] they wanted to take possession of them."[10] You contacted Ms. Chung on her personal email account from your White House email account—not her Department of Defense email account.[11] On June 28, 2022, Ms. Chung entered the Penn Biden Center and packed up 13 boxes that would later be found to have contained classified materials. She stated:

> Q So is it fair to say that you arrived on the morning of June 28th of 2022 to pack up the boxes at Penn Biden Center?
>
> A Yes, I believe so. Yep.
>
> Q And then if you go to exhibit 1, Bates number 98, did you write an email to Dana Remus, White House counsel, on that date?
>
> A The 98?
>
> Q Yes, so Exhibit 1.
>
> A From -- yes, I did.
>
> Q And what's the date of that email?
>
> A Tuesday, June 28, 2022.
>
> Q So this was the same day that you're packing up the boxes at Penn Biden Center?
>
> A Yes.
>
> Q And what time did you send this email?
>
> A 5:28.
>
> Q Did you send this email when you had completed packing up the boxes?

[9] Transcript, p. 119.
[10] Transcript, p. 18.
[11] Transcript, p. 14-15.

A It was later that day.

Q Sorry. What was later that day?

A Oh, when I wrote this email.

Q So how much later that day did you write this email from when you finished completing packing up the boxes?

A Hours later. Hours later.

Q And there you wrote how many boxes?

A Thirteen boxes.[12]

You left the White House in July 2022. On October 4, 2022, Ms. Chung was notified by a Penn Biden Center employee that no one had picked up the boxes that Ms. Chung had packed in June 2022:

Q Then if we can go to Bates number 115 on exhibit 1, and then if we could start from the second from the bottom, the October 4, 2022, email at 10:32 a.m. from [Penn Biden Center employee 1] to you. What does she write?

A "Hi, Kathy. Checking in to see if the below mentioned boxes will be picked up soon. Thanks, [Penn Biden Center employee 1]."

Q And what was your response?

A "Wait. Did they not pick up back in June?"

Q And as you discussed with my colleagues, you were surprised at this point that the items had not been picked up, correct?

A Correct.[13]

On October 13, 2022, Ms. Chung notified Mr. Bauer, the President's personal attorney, that boxes remained at the Penn Biden Center:

Q And in this text message dated October 13 of 2022, you send a text to Mr. Bob Bauer, correct?

[12] Transcript, p. 87-88.
[13] Transcript, p. 94.

A Yes.

Q And you've said this before, but you knew Mr. Bauer from previously working in the administration and other government jobs; right?

A Yes.

Q Can you please read your text to him?

A "Bob, one thing I forgot to ask you today. There are still boxes of materials at the Penn Biden Center. They are wondering if someone is going to pick up. Dana went there in June, but decided it was too much to take I was told."[14]

Mr. Bauer responded via text message the same day that "Pat has begun to sort through them and so we should get this organized in the near future."[15] According to Ms. Chung, "Pat" is a reference to Mr. Patrick Moore, a former personal attorney of President Biden.[16] The Penn Biden Center is located in Washington D.C. Mr. Moore's office is in Boston. The National Archives has acknowledged it retrieved boxes from Mr. Moore's Boston office.[17]

The Committee believes you have direct knowledge of certain events relevant to this investigation prior to your departure from the White House in July 2022. The Committee questions why you, as White House Counsel, would task Ms. Chung, an employee at the Department of Defense, to do what was then believed to be a personal errand of the President—packing personal items not subject to the Presidential Records Act. The Committee questions why—if there is a valid reason why White House Counsel would be the appropriate coordinator of this task—the President's personal attorneys assumed responsibility for the task after your departure in July 2022, instead of your successor as White House Counsel. The Committee questions why you contacted Ms. Chung on her personal telephone and email account.

B. <u>Ms. Chung's account complicates the White House's description of where and how classified documents were stored in the Penn Biden Center.</u>

During her interview with the Committee, Ms. Chung provided information that potentially conflicts with the White House's characterization of how and where documents were stored. According to the White House's statement, in November 2022 the President's personal attorneys discovered the documents in a "locked closet" at the Penn Biden Center while preparing to vacate the space.[18] As described above, the Committee's interview with Ms. Chung

[14] Transcript, p. 95.
[15] Transcript, p. 96.
[16] *Id.*
[17] Letter from Ms. Debra Steidel Wall, Acting Archivist, Nat'l Archives and Records Admin., to Sen. Ron Johnson & Sen. Charles E. Grassley (Mar. 7, 2023).
[18] *Supra*, fn. 3.

showed Ms. Chung—not President Biden's personal attorneys—packed boxes of documents in June 2022, not November 2022. The 13 boxes Ms. Chung packed, as well as additional boxes that were never unpacked from the Obama-Biden Administration, were not in a locked closet. She stated:

Q These boxes, when you went there on June 28th of 2022, and the items, were they in a locked closet?

A No.

Q Were any of the boxes in a locked closet at all?

A No.

Q Were any of the items that you boxed up and then put them in the 13 boxes so now you've boxed them up and packaged them up. Were those boxes placed in a locked closet?

A No.

Q Would you have even had the ability to lock them in a closet yourself without getting [Penn Biden employees] involved?

A No.[19]

Additionally, according to Ms. Chung, documents were in multiple places and were not secured:

Q When you first go into Penn Biden Center, I believe you said you need a fob to get in. Do I remember that correctly?

A Yes.

Q Do you need a fob to access any other part of Penn Biden Center once you go through the entrance?

A No.

Q So the fob is just to get you in the entranceway?

A Yes, to the suite.

[19] Transcript, p. 88.

Q Okay. In order to get into the storage room, was the storage room locked?

A I'm trying to think if [Penn Biden employe 2] or [Penn Biden employee 1] had to unlock -- no, I believe not.

Q It's fair to say since it wasn't locked, you didn't have a key for the storage room then?

A No.

Q Did you have any other keys or fobs or anything else related to Penn Biden Center to get in any other areas that could be locked in Penn Biden Center?

A I had a fob and a key. I had a key to his office, which was not locked. No.[20]

The Committee believes you may possess knowledge or information that would inform its investigation into how and where documents were stored at the Penn Biden Center after these items were packed by Ms. Chung at your direction on June 28, 2022, and your subsequent attempt to retrieve them on June 30, 2022. Additionally, the Committee believes you may possess information that would provide important insight regarding the discrepancies between Ms. Chung's explanation and the official account released by the White House after your departure from the White House in July 2022.

C. <u>The timing of your initial outreach to Ms. Chung regarding documents at the Penn Biden Center coincides with important dates in the federal government's subpoena for documents at former President Trump's residence at Mar-a-Lago.</u>

In January 2022, representatives from the National Archives and Records Administration (NARA) retrieved 15 boxes of presidential records from former President Trump's home at Mar-a-Lago, in Florida.[21] The boxes reportedly contained classified materials, and in February 2022, the FBI opened a criminal investigation of the matter.[22] On April 12, 2022, NARA informed former President Trump that it would provide the boxes to the FBI in furtherance of the FBI's investigation.[23] On April 29, 2022, and May 1, 2022, former President Trump requested an extension on NARA taking the documents to the FBI, citing the possibility of the applicability of executive privilege to the documents.[24]

---

[20] Transcript, p. 82-83.
[21] Jill Colvin & Lindsay Whitehurst, *A timeline of the investigation into Trump's Mar-a-Lago docs*, AP (Aug. 31, 2022).
[22] *Id.*
[23] *Id.*
[24] *Id.*

On May 10, 2022, Acting U.S. Archivist Debra Steidel Wall wrote to Mr. Evan Corcoran, a personal attorney for former President Donald Trump, regarding the claim of executive privilege.[25] In her letter, Ms. Wall noted that "Counsel to the President has informed me that, in light of the particular circumstances presented here, President Biden defers to my determination, in consultation with the Assistant Attorney General for the Office of Legal Counsel, regarding whether or not I should uphold the former President's purported 'protective assertion of executive privilege.''[26] Ms. Wall "decided not to honor the former President's 'protective' claim of privilege" and provided the FBI access to records in NARA's custody "as early as Thursday, May 12, 2022."[27] On May 11, 2022, a grand jury issued a subpoena "directed to the custodian of records for the Office of Donald J. Trump" requesting all documents bearing classification markings.[28] The subpoena return was dated for May 24, 2022—notably, the same day you first contacted Ms. Chung to begin coordinating the moving of President Biden's documents from Penn Biden Center.[29]

D. <u>The Committee is concerned about the President's history of not exercising proper care toward classified materials.</u>

Ms. Chung provided valuable insight into the President's past handling of classified material. The Committee is troubled to learn that the President's irresponsible handling of sensitive documents did not begin recently. As described above, the classified documents found at the Penn Biden Center on November 2, 2022, were packed originally in the West Wing in 2017 in part by Ms. Chung.[30] The Vice President's Office did have a secured storage area for classified materials, but then Vice President Biden did not use it. Ms. Chung explained:

Q And was there a safe in the Vice President's suite?

A Yes, there was. Uh-huh.

Q And could the safe have been used to store classified materials?

A Yes.

Q To your knowledge, was the safe used to store classified materials?

A No.

---

[25] Letter from Ms. Debra Steidel Wall, Acting Archivist, Nat'l Archives and Records Admin., to Mr. Evan Corcoran (May 10, 2022).
[26] *Id.*
[27] *Id.*
[28] *Supra*, fn. 21.
[29] United States' Response to Motion for Judicial Oversight and Additional Relief. *Trump v. United States*, Case No. 22-CV-81294-CANNON (S.D. FL), p. 8.
[30] Transcript: p. 22.

Q Okay. To your knowledge, is a safe an appropriate place to store classified materials?

A Yes, of course.[31]

Additionally, Ms. Chung stated that when the Obama-Biden Administration ended on January 20, 2017, the boxes she and two other employees of the Office of the Vice President had packed with then-undiscovered classified materials were transported to a General Services Administration (GSA) facility for approximately six months.[32] Then, those materials were transported to a temporary office space in Washington, D.C. by Ms. Chung and others:

Q Who moved the boxes from the first temporary office to the second temporary office?

A From the GSA office, we all put it in our cars and moved it.

Q Who's "we all"?

A Oh, Steve, myself, Sam and Melinda.

Q And I think you've said their last names already, but would you mind just repeating their last names?

A Oh, Steve Ricchetti, Melinda Medlin, Sam [Salk], Richard Ruffner and myself.[33]

These are disturbing revelations. The President's haphazard handling of classified materials raises many additional questions about the repercussions of these actions, including possible threats to national security. As you are aware, additional classified material has been discovered at the President's home in Wilmington, Delaware, including in his garage. The Committee believes you may possess information or knowledge that is crucial to understanding how those documents arrived in Delaware, as you played a primary role in the events precipitating the discovery of documents in the President's CelticCapri corporate headquarters at the Penn Biden Center in Washington, D.C.

To assist the Committee with this investigation, please provide the following information no later than May 19, 2023:

1. All communications between yourself and Ms. Chung or any employee of CelticCapri since May 24, 2022 regarding President Biden's documents and other items that were stored at Penn Biden Center;

[31] Transcript, p. 113.
[32] Transcript: p. 32.
[33] Transcript, p. 33.

2. All communications between yourself and any employee of the University of Pennsylvania or the Penn Biden Center from January 20, 2021 to when you departed the White House in July 2022; and

3. All documents and communications in your possession regarding President Biden's documents and other items that were stored at Penn Biden Center dated prior to your departure from the White House in July 2022.

The Committee has provided instructions regarding how these materials should be produced and defined certain terms in the accompanying attachment.[34]

Additionally, the Committee requests that you make yourself available for a transcribed interview with Committee staff. To arrange the transcribed interview, please contact either James Mandolfo or Jake Greenberg with the Committee at (202) 225-5074 by May 30, 2023.

The Committee on Oversight and Accountability is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

Thank you for your prompt attention to this important investigation.

Sincerely,

James Comer
Chairman
Committee on Oversight and Accountability

cc: The Honorable Jamie B. Raskin, Ranking Member
Committee on Oversight and Accountability

[34] Attachment A.

EXHIBIT 3

JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED EIGHTEENTH CONGRESS

JAMIE RASKIN, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
https://oversight.house.gov

January 10, 2023

Ms. Debra Steidel Wall
Acting Archivist of the United States
700 Pennsylvania Avenue, NW
Washington, DC 20408

Dear Ms. Steidel Wall:

The Committee on Oversight and Accountability is investigating whether there is a political bias at the National Archives and Records Administration (NARA). For months, NARA failed to disclose to Committee Republicans or the American public that President Biden—after serving as Vice President—stored highly classified documents in a closet at his personal office.[1] NARA learned about these documents days before the 2022 midterm elections and did not alert the public that President Biden was potentially violating the law. Meanwhile, NARA instigated a public and unprecedented FBI raid at Mar-a-Lago—former President Trump's home—to retrieve presidential records. NARA's inconsistent treatment of recovering classified records held by former President Trump and President Biden raises questions about political bias at the agency.

In the aftermath of the FBI's August 8, 2022, raid of Mar-a-Lago, NARA attempted to both minimize its role in the matter and explain that the Obama-Biden Administration's handling of documents was proper and complete. In an October 11, 2022, statement, NARA claimed it had assumed physical custody of all Obama-Biden Administration records when the President and Vice President left office.[2] NARA claimed, "[r]eports that indicate or imply that those Presidential records were in the possession of the former Presidents or their representatives, after they left office, or that the records were housed in substandard conditions, are false and misleading."[3] NARA's statement was apparently false and never corrected after learning that President Biden stored classified documents at Penn Biden Center.[4]

On November 2, 2022, a week before the midterm elections, President Biden's personal attorneys—whose level of security clearance remains unknown—"discovered" classified Obama-Biden Administration documents that were quietly handed off to the U.S. Department of

---

[1] Shawna Chen, *Classified docs from Biden's VP days found in private office*, AXIOS (Jan. 9, 2023).
[2] *Statement,* NATIONAL ARCHIVES (Oct. 11, 2022), *available at* https://www.archives.gov/press/press-releases/2022/nr22-001.
[3] *Id.*
[4] *Id.*

Justice without executing a residential search warrant.[5] The documents retrieved from President Biden's personal office included documents designated as "sensitive compartmented information . . . which is used for highly sensitive information obtained from intelligence sources."[6]

NARA's public enforcement of the Presidential Records Act against former President Trump while failing to disclose violations by President Biden to Committee Republicans and the American public raises concerns about inconsistent policy and procedures at the agency that creates the appearance of political bias. As such, please provide the following documents and information as soon as possible, but no later than January 24, 2023:

1. All documents and communications between NARA and the White House related to classified documents at the Penn Biden Center;

2. All documents and communications between and among NARA employees, including Gary Stern and John Hamilton related to classified documents at the Penn Biden Center;

3. All documents and communications between NARA and the Department of Justice related to classified documents at the Penn Biden Center; and

4. All documents and communications between NARA and any outside entity, including President Biden's attorneys, related to classified documents at the Penn Biden Center.

Additionally, we request that you make Gary Stern, NARA General Counsel, and John Hamilton, NARA Director of Congressional Affairs, available for transcribed interviews with Committee staff regarding this matter. Please schedule these interviews no later than January 17, 2023.

The Committee on Oversight and Accountability has specific jurisdiction over NARA under House Rule X. Additionally, the Committee on Oversight and Accountability is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X. If you have any questions about this request, please contact Committee on Oversight and Accountability staff at (202) 225-5074.

Thank you for your prompt attention to this important investigation.

---

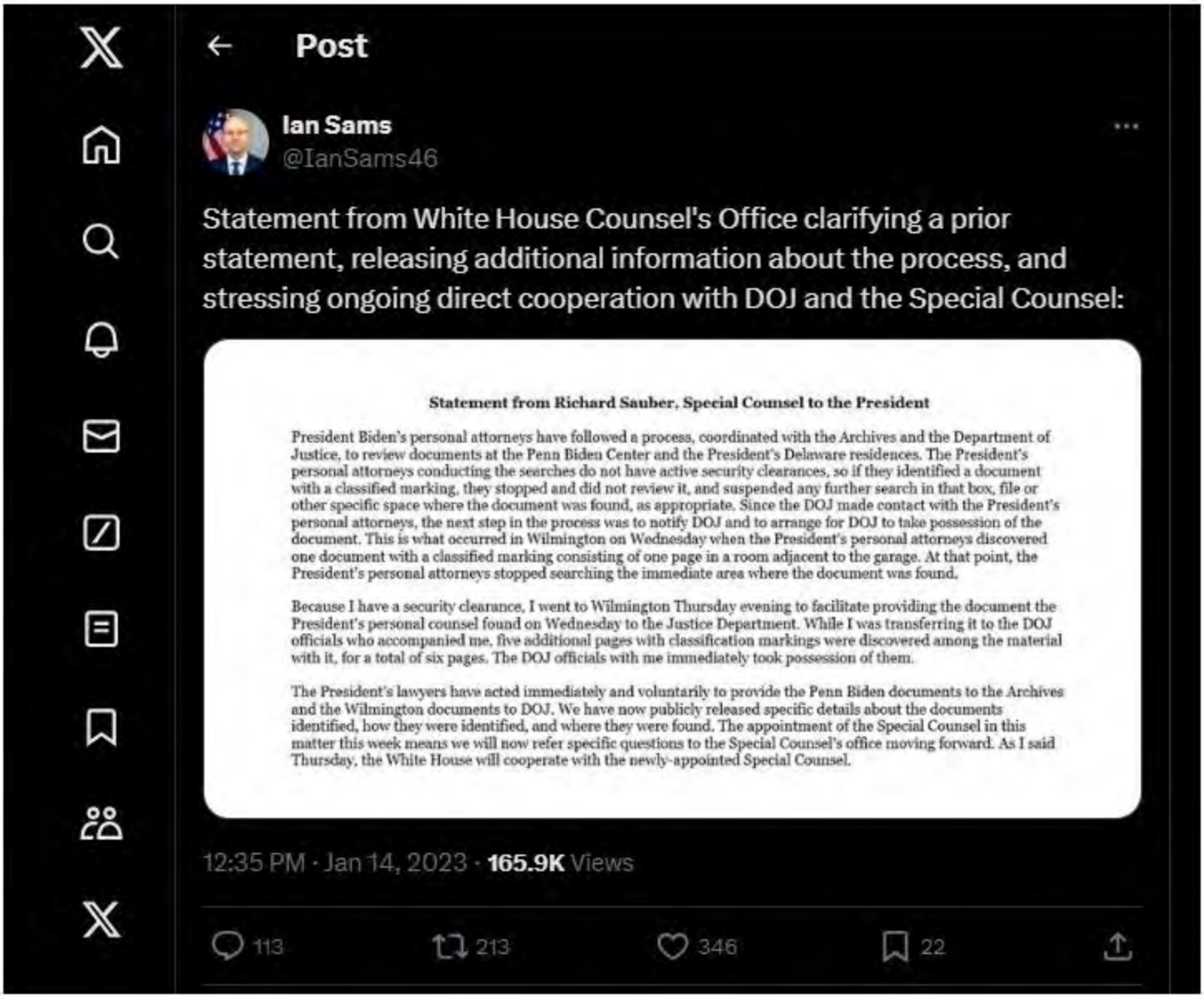
[5] Jamie Gangel, Marshall Cohen, Evan Perez & Phil Mattingly, *Classified documents from Biden's time as VP discovered in private office*, CNN.COM (Jan. 9, 2023).
[6] *Id.*

Sincerely,

James Comer
Chairman
Committee on Oversight and Accountability

cc: The Honorable Jamie B. Raskin, Ranking Member
Committee on Oversight and Accountability

EXHIBIT 4


Post
Ian Sams
@IanSams46
Statement from White House Counsel's Office clarifying a prior statement, releasing additional information about the process, and stressing ongoing direct cooperation with DOJ and the Special Counsel:
Statement from Richard Sauber, Special Counsel to the President
President Biden's personal attorneys have followed a process, coordinated with the Archives and the Department of Justice, to review documents at the Penn Biden Center and the President's Delaware residences. The President's personal attorneys conducting the searches do not have active security clearances, so if they identified a document with a classified marking, they stopped and did not review it, and suspended any further search in that box, file or other specific space where the document was found, as appropriate. Since the DOJ made contact with the President's personal attorneys, the next step in the process was to notify DOJ and to arrange for DOJ to take possession of the document. This is what occurred in Wilmington on Wednesday when the President's personal attorneys discovered one document with a classified marking consisting of one page in a room adjacent to the garage. At that point, the President's personal attorneys stopped searching the immediate area where the document was found.
Because I have a security clearance, I went to Wilmington Thursday evening to facilitate providing the document the President's personal counsel found on Wednesday to the Justice Department. While I was transferring it to the DOJ officials who accompanied me, five additional pages with classification markings were discovered among the material with it, for a total of six pages. The DOJ officials with me immediately took possession of them.
The President's lawyers have acted immediately and voluntarily to provide the Penn Biden documents to the Archives and the Wilmington documents to DOJ. We have now publicly released specific details about the documents identified, how they were identified, and where they were found. The appointment of the Special Counsel in this matter this week means we will now refer specific questions to the Special Counsel's office moving forward. As I said Thursday, the White House will cooperate with the newly-appointed Special Counsel.
12:35 PM · Jan 14, 2023 · 165.9K Views
113
213
346
22

Statement from Richard Sauber, Special Counsel to the President

President Biden's personal attorneys have followed a process, coordinated with the Archives and the Department of Justice, to review documents at the Penn Biden Center and the President's Delaware residences. The President's personal attorneys conducting the searches do not have active security clearances, so if they identified a document with a classified marking, they stopped and did not review it, and suspended any further search in that box, file or other specific space where the document was found, as appropriate. Since the DOJ made contact with the President's personal attorneys, the next step in the process was to notify DOJ and to arrange for DOJ to take possession of the document. This is what occurred in Wilmington on Wednesday when the President's personal attorneys discovered one document with a classified marking consisting of one page in a room adjacent to the garage. At that point, the President's personal attorneys stopped searching the immediate area where the document was found.

Because I have a security clearance, I went to Wilmington Thursday evening to facilitate providing the document the President's personal counsel found on Wednesday to the Justice Department. While I was transferring it to the DOJ officials who accompanied me, five additional pages with classification markings were discovered among the material with it, for a total of six pages. The DOJ officials with me immediately took possession of them.

The President's lawyers have acted immediately and voluntarily to provide the Penn Biden documents to the Archives and the Wilmington documents to DOJ. We have now publicly released specific details about the documents identified, how they were identified, and where they were found. The appointment of the Special Counsel in this matter this week means we will now refer specific questions to the Special Counsel's office moving forward. As I said Thursday, the White House will cooperate with the newly-appointed Special Counsel.

EXHIBIT 5

JAMES COMER, KENTUCKY
CHAIRMAN

ONE HUNDRED EIGHTEENTH CONGRESS

JAMIE RASKIN, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
https://oversight.house.gov

March 7, 2023

Mr. Jeff Zients
White House Chief of Staff
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. Zients,

The Committee on Oversight and Accountability continues to investigate President Biden's mishandling of highly classified documents. The Committee has previously written the White House regarding this matter on January 10, 2023; January 13, 2023; and January 15, 2023. However, the White House has produced no documents and neglected to provide a substantive response to the Committee's requests. Meanwhile, reports indicate the Federal Bureau of Investigation continues its search for more classified documents, most recently at the University of Delaware.[1] The Committee is concerned about President Biden's lack of transparency given the serious national security implications of his conduct.

On January 31, 2023, the Committee conducted a transcribed interview with National Archives and Records Administration's (NARA) general counsel, Gary Stern. The interview revealed information regarding President Biden's mishandling of classified documents and NARA's response. During questioning by Committee counsel, Mr. Stern acknowledged that on January 9, 2023, when CBS broke the news that President Biden stored classified materials at Penn Biden Center,[2] NARA drafted a public statement in response. Mr. Stern disclosed to the Committee that someone outside of NARA withheld its release. In complete contrast, on February 7, 2022, when the *Washington Post* broke the story that classified documents were found in President Trump's Mar-a-Lago home, NARA employees, including Gary Stern, drafted and *published* a statement on the agency's website that same day.[3] Mr. Stern stated:

[1] Paula Reid, *First on CNN: FBI searched University of Delaware for Biden documents, source says*, CNN (Feb. 15, 2023).
[2] Adriana Diaz, Amdres Triay, Arden Farhi, *U.S. attorney reviewing documents marked classified from Joe Biden's vice presidency found at Biden think tank*, CBS Evening News (updated Jan 10, 2023).
[3] Jacqueline Alemany, Josh Dawsey, Tom Hamburger, and Ashley Parker, *National Archives had to retrieve Trump White House records from Mar-a-Lago*, WASH. POST (Feb. 7, 2022).

Q. On January 9th of 2023, CBS broke the story that President Biden stored documents at Penn Biden Center that were subject to the Presidential Records Act and also contained classified material.

Did you draft a statement in response to that CBS report?

A. NARA did draft a statement.

Q. Did it go public?

A. No.

Q. Who prevented that statement from going public?

A. According to the DOJ guidance, I'm not supposed to talk about the, you know, content of our communications with other parties.

Q. So I just want to be clear. You published, being National Archives, a statement regarding President Trump's alleged possession of these materials at Mar-a-Lago the same day that the Washington Post story breaks, correct? Is that right?

A. We did, yes.

Q. You drafted it. You developed it.

A. I helped draft it, yes.

Q. But then, on January 9th of 2023, when the story breaks with CBS that President Biden has materials that are classified and subject to the Presidential Records Act, the National Archives actually drafted a press statement that has never made it to light?

A. Yes.

Congressman Jim Jordan asked Mr. Stern whether someone within NARA instructed that the statement not be released publicly. Mr. Stern asserted it was not a person at NARA who was responsible for blocking the statement:

Mr. Jordan. So I'm not talking about communications outside NARA. I'm talking about inside NARA. Did someone tell you not to put it out within the National Archives.

Mr. Stern. No.

In addition, Mr. Stern confirmed with Committee counsel that President Biden can publicly release his communications between his attorneys and NARA. Indeed, the Committee learned that President Biden is "free to release" all of his representatives' communications and be completely transparent with the American people, if he chooses. Mr. Stern stated:

> Q. Couldn't President Biden just release the emails from his attorneys and his representatives who contacted National Archives, himself, so that it would be public for everyone to view?
>
> A. Yeah, I can't speak for other parties. I mean, again, you've asked for our communications, you know, including internal communications and with all those parties, which are still under review. And, I mean, it is quite possible that I will be able to provide you that information; I'm just not able to do that right at this moment.
>
> Q. But there's nothing preventing the President of the United States from releasing the emails from his representatives and his attorneys to the National Archives for the public to view. In other words, the National Archives isn't preventing President Biden from releasing those documents, correct?
>
> A. That is correct. And that's the same with President Trump and his representatives. They are free to release, you know, the communications they receive from us. We treat them as – we treat them as confidential, but the recipients, you know, can act independently if they want to.

The Committee's transcribed interview with NARA General Counsel Gary Stern raises more questions regarding the Biden Administration's involvement in suppressing information related to President Biden's mishandling of classified documents. The Committee reiterates its previous requests to the White House for documents and information outlined in our January 10, 2023, January 13, 2023, and January 15, 2023, letters. Further, please provide the following answers, documents, and communications no later than March 21, 2023:

1) Did any White House staff member or representative of President Biden inform any employee of NARA to withhold any public statements regarding President Biden's mishandling of classified documents? If so, who?

2) All documents and communications regarding the withholding of NARA's statement it intended to issue on January 9, 2023, related to President Biden's mishandling and storage of classified documents at Penn Biden Center; and

3) Mr. Stern stated President Biden is "free to release" his emails between his attorneys/ representatives and NARA. Will President Biden release his attorneys' and representatives' communications with NARA for the public to view?[4]

The Committee has provided instructions regarding how these materials should be produced and defined certain terms in the accompanying attachment.[5] To make arrangements to deliver documents or ask any related follow-up questions, please contact Committee on Oversight and Accountability staff at (202) 225-5074.

The Committee on Oversight and Accountability is the principal oversight committee of the U.S. House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

Thank you for your prompt attention to this important investigation.

Sincerely,

James Comer
Chairman
Committee on Oversight and Accountability

cc: The Honorable Jamie B. Raskin, Ranking Member
Committee on Oversight and Accountability

[4] NARA has made only one production of materials related to this matter that cover communications between President Biden's personal attorneys and NARA from November 7, 2022 to November 10, 2022. *See* https://www.archives.gov/foia/biden-vp-records-covered-by-pra.
[5] *See* Attachment A.

EXHIBIT 6

O'Melveny & Myers LLP
1625 Eye Street, NW
Washington, DC 20006-4061

T: +1 202 383 5300
F: +1 202 383 5414
omm.com

File Number:

January 18, 2023

Greg Jacob
D: +1 202 383 5110
gjacob@omm.com

Kate Dillon McClure
Acting Director, White House Liaison Division
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

Dear Ms. McClure:

As Vice President Mike Pence's designated representative to the National Archives, I write to request your assistance with collecting and transferring to the custody of the National Archives an additional set of Vice Presidential records. The additional records appear to be a small number of documents bearing classified markings that were inadvertently boxed and transported to the personal home of the former Vice President at the end of the last Administration. Vice President Pence was unaware of the existence of sensitive or classified documents at his personal residence. Vice President Pence understands the high importance of protecting sensitive and classified information and stands ready and willing to cooperate fully with the National Archives and any appropriate inquiry.

Following press reports of classified documents at the personal home of President Biden, out of an abundance of caution, on Monday, January 16, Vice President Pence engaged outside counsel, with experience in handling classified documents, to review records stored in his personal home. Counsel identified a small number of documents that could potentially contain sensitive or classified information interspersed throughout the records. Vice President Pence's counsel, however, is unable to provide an exact description of the folders or briefing materials that may contain sensitive or classified information because counsel did not review the contents of the documents once an indicator of potential classification was identified. Vice President Pence immediately secured those documents in a locked safe pending further direction on proper handling from the National Archives.

Vice President Pence has directed his representatives to work with the National Archives to ensure their prompt and secure return. Vice President Pence appreciates the good work of the staff at the National Archives and trusts they will provide proper counsel in response to this letter.

Sincerely,

/s Greg Jacob
Gregory F. Jacob
Designated Representative
Pence Vice Presidential records

EXHIBIT 7

O'Melveny & Myers LLP
1625 Eye Street, NW
Washington, DC 20006-4061

T: +1 202 383 5300
F: +1 202 383 5414
omm.com

File Number:

January 22, 2023

Greg Jacob
D: +1 202 383 5110
gjacob@omm.com

William "Jay" Bosanko
Chief Operating Officer
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

Dear Mr. Bosanko:

Thank you for your prompt response to my letter dated January 18, 2023 concerning the collection of certain papers containing what appeared to be classified markings found at the residence of Vice President Pence on January 16. When we spoke at noon on January 19, you, together with National Archives General Counsel Gary Stern, explained to me the procedures by which the National Archives has historically taken custody of potential Presidential or Vice Presidential Records—including, most recently, those of President Biden and of former President Trump. You also explained to me the standard procedures by which the Department of Justice has thereafter requested and obtained access to such documents pursuant to the Presidential Record Act ("PRA").

As you are aware, on the evening of January 19, the Department of Justice bypassed the standard procedures and requested direct possession. Even though the Vice President was in Washington, D.C. to attend the March for Life, he still immediately agreed in the interest of ensuring an expeditious collection. FBI agents came to the Indiana residence of Vice President Pence at 9:30 p.m. to collect the documents that had been secured in his safe. The transfer was facilitated by the Vice President's personal attorney, who has experience in handling classified documents, and who conducted the prior review on January 16.

Prior to the Department of Justice's intervention, on our noon phone call on January 19, you suggested that Vice President Pence consider voluntarily providing to the Archives the two boxes in which the records had been found, as well as any other boxes containing copies of Administration papers. You stated this voluntary transfer of papers would permit the Archives to conduct a PRA review to ensure the boxes did not contain any original documents that could qualify as Presidential Records, that the Archives had not already obtained through the records transmission process at the end of the Administration. You assured me that all personal papers and effects of the Vice President would be returned once this review is complete, subject to any legal holds that might temporarily limit their return.

I promptly called you back on the afternoon of January 19 and advised you that the Vice President had agreed to allow the Archives to collect the boxes at the same time that it collected the papers appearing to bear classified markings that had been placed in the Vice President's

safe, so that the Archives could conduct the recommended review. I confirmed that four boxes contained copies of Administration papers: the two boxes in which a small number of papers appearing to bear classified markings had been found, and two separate boxes containing courtesy copies of Vice Presidential papers. The Vice President is, of course, permitted to obtain and retain copies of his own Vice Presidential records at any time. I expressed to you my expectation that the substantial majority of the documents in the four boxes would, upon examination, be found to be personal copies of other records that were previously transmitted to the Archives.

Following the Department of Justice's unexpected collection of the documents from the safe on the night of January 19, I contacted you again on January 20 to reiterate the offer the Vice President had made the day before to transfer the four boxes containing copies of Administration papers to the Archives for a PRA review. You indicated that the Archives did not have the capacity to arrange for the logistics of a near-term collection in Indiana, but that the Archives had determined it would be appropriate for the Vice President's agents to transport the four boxes to Washington, DC.

I will personally deliver the boxes to the Archives between 10:00 and 11:00 a.m. on Monday, January 23. The boxes were sealed at the Vice President's residence in Indiana, following a final review by the Vice President's personal attorney during which attorney-client privileged materials related to personal capacity attorneys, and Article I legislative branch materials, were placed in sealed and clearly labeled envelopes. All of the documents within the boxes, and within the sealed envelopes, remain in the exact place and order in which they were discovered on January 16. The Vice President is not waiving any privileges pertaining to the clearly labeled materials.

The Vice President has requested that I convey his thanks to you for your responsiveness and professionalism throughout your handling of this matter.

Sincerely,

/s Greg Jacob
Gregory F. Jacob
Designated Representative
Pence Vice Presidential records

EXHIBIT 8

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA	)	
	)	DOCKET NO. 3:15 CR 47
v.	)	
	)	**FACTUAL BASIS**
DAVID HOWELL PETRAEUS	)	
	)	

NOW COMES the United States of America, by and through Anne M. Tompkins, United States Attorney for the Western District of North Carolina, James P. Melendres, Trial Attorney, Jill Westmoreland Rose, Assistant United States Attorney, and Richard S. Scott, Trial Attorney, and hereby files this Factual Basis in support of the Plea Agreement filed simultaneously in this matter.

This Factual Basis does not attempt to set forth all of the facts known to the United States at this time. By their signatures below, the parties expressly agree that there is a factual basis for the guilty plea that the defendant will tender pursuant to the Plea Agreement. The parties also agree that this Factual Basis may, but need not, be used by the United States Probation Office and the Court in determining the applicable advisory guideline range under the United States Sentencing Guidelines or the appropriate sentence under 18 U.S.C. § 3553(a). The defendant agrees not to object to any fact set forth below being used by the Court or the United States Probation Office to determine the applicable advisory guideline range or the appropriate sentence under 18 U.S.C. § 3553(a). The parties' agreement does not preclude either party from hereafter presenting the Court with additional facts which do not contradict facts to which the parties have agreed not to object and which are relevant to the Court's guideline computations, to 18 U.S.C. § 3553 factors, or to the Court's overall sentencing decision.

The parties stipulate that the allegations in the Bill of Information and the following facts are true and correct, and that had the matter gone to trial, the United States would have proven them beyond a reasonable doubt with admissible and credible evidence. Specifically, the evidence would establish, at a minimum, the following facts:

At all relevant times,

The Defendant

1. Defendant DAVID HOWELL PETRAEUS, a citizen of the United States and resident of Arlington, Virginia, was a United States Army four-star general when he retired from the Army on or about August 31, 2011. From on or about July 4, 2010, to on or about July 18, 2011, defendant DAVID HOWELL PETRAEUS served as Commander of the International Security Assistance Force ("ISAF") in Afghanistan. From on or about September 6, 2011, to on or about November 9, 2012, defendant DAVID HOWELL PETRAEUS served as Director of the Central Intelligence Agency ("CIA").

Classified Information

2. Those persons with security clearances granting them access to classified information were required to properly store and secure classified information, by Title 18, United States Code, Sections 793 and 1924, and applicable rules, regulations, and orders.

3. Classified information was defined by Executive Order 13526 ("E.O. 13526") and relevant preceding Executive Orders, as information in any form that: (1) is owned by, produced by or for, or under the control of the United States government; (2) falls within one or more of the categories set forth in E.O. 13526; and (3) is classified by an original classification authority

who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security. Where such unauthorized disclosure reasonably could be expected to cause "damage" to the national security, the information is classified as "Confidential." Where such unauthorized disclosure reasonably could be expected to cause "serious damage" to the national security, the information is classified as "Secret." Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "Top Secret."

4. E.O. 13526 also provides that certain senior U.S. officials are authorized to establish "special access programs" upon a finding that "the vulnerability of, or threat to, specific information is exceptional" and "the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure." Within the U.S. Intelligence Community, the Director of National Intelligence is authorized to establish special access programs for intelligence sources, methods, and activities. Such intelligence programs are called "Sensitive Compartmented Information Programs" or SCI Programs. A term commonly used to describe certain materials in such programs is "code word."

5. Pursuant to E.O. 13526, a person may gain access to classified information only if a favorable determination of eligibility for access has been made by an agency head or an agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a "need-to-know" the information.

6. "Need-to-know" means a determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function.

7. The classified information being accessed may not be removed from the controlling agency's premises without permission. Moreover, even when SCI is maintained on the controlling agency's premises, it must be stored in a Sensitive Compartmented Information Facility ("SCIF"), which is an accredited area, room, group of rooms, building, or installation designed to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons.

The Department of Defense

8. The Department of Defense ("DOD") was a United States government military agency. The DOD's headquarters were at Arlington, Virginia. The DOD was responsible for providing the military forces needed to deter war and protect the security of the United States. Moreover, through its subordinate national intelligence services, including the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office, the DOD was responsible for, among other things, collecting information that revealed the military plans, intentions, and capabilities of the United States' adversaries and the bases for their decisions and actions, as well as conducting clandestine actions, at the direction of the President and his authorized designee, designed to preempt threats and achieve the United States' policy objectives.

9. The responsibilities of certain DOD employees required that their association with the DOD be kept secret; as a result, the fact that these individuals were employed by the DOD

was classified. The responsibilities of other DOD employees required that, while their employment by the DOD was itself not secret, their association with certain DOD programs and their particular activities on behalf of the DOD were kept secret; accordingly, such information was classified. Disclosure of the fact that such individuals were employed by the DOD, associated with certain DOD programs, or engaged in particular activities on behalf of the DOD, had the potential to damage national security in ways that ranged from preventing the future use of individuals in a covert or clandestine capacity, to compromising clandestine actions and intelligence-gathering methods and operations, to endangering the safety of DOD employees and those who interacted with them.

The Central Intelligence Agency

10. The CIA was a United States government intelligence agency. The CIA's headquarters were at Langley, Virginia. The CIA was responsible for, among other things, collecting information that revealed the plans, intentions, and capabilities of the United States' adversaries and the bases for their decisions and actions, as well as conducting clandestine actions, at the direction of the President and his authorized designees, designed to preempt threats and achieve the United States' policy objectives.

11. The responsibilities of certain CIA employees required that their association with the CIA be kept secret; as a result, the fact that these individuals were employed by the CIA was classified. The responsibilities of other CIA employees required that, while their employment by the CIA was itself not necessarily secret, their association with certain CIA programs and their particular activities on behalf of the CIA be kept secret; accordingly, such information was classified. Disclosure of the fact that such individuals were employed by the CIA, associated

with certain CIA programs, or engaged in particular activities on behalf of the CIA, had the potential to damage national security in ways that ranged from preventing the future use of individuals in a covert or clandestine capacity, to compromising clandestine actions and intelligence-gathering methods and operations, to endangering the safety of CIA employees and those who dealt with them.

Criminal Conduct

12. Throughout his employment by the DOD, defendant DAVID HOWELL PETRAEUS entered into various agreements with the United States regarding the protection and proper handling of classified information. Examples of these agreements include:

a. On March 15, 2006, as a condition of being granted access to certain SCI, DAVID HOWELL PETRAEUS entered into a Non-Disclosure Agreement ("NDA") with the DOD in which he agreed, in pertinent part, as follows:

> I have been advised that unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency . . . that last authorized my access to SCI.
>
> I hereby agree to submit for security review by the [agency] that last authorized my access to such information or material, any writing or other preparation in any form . . . that contains or purports to contain any SCI . . . that I contemplate disclosing to any person not authorized to have access to SCI . . .
>
> In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute a violation or violations of United States criminal laws, including the provisions of . . . Section[ ] 793 . . . [of] Title 18, United States Code . . .
>
> I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity

> providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code . . .

Defendant DAVID HOWELL PETRAEUS entered into at least 13 additional NDAs in the course of his DOD employment. In each instance, DAVID HOWELL PETRAEUS promised never to disclose SCI to anyone not authorized to receive it without prior written authorization from the United States government, and he acknowledged that unauthorized retention and/or disclosure of classified information could cause irreparable injury to the United States and be used to advantage by a foreign nation. The scope of these NDAs encompassed classified information referenced in this Statement of Facts.

b. As a condition of being granted access to classified information, defendant DAVID HOWELL PETRAEUS entered into a Secrecy Agreement with the DOD, in which he agreed, in pertinent part, as follows:

> I accept the responsibilities associated with being granted access to classified national security information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and official need to know. I further understand that, in being granted access to classified information, a special confidence and trust has been placed in me by the United States Government.

Defendant DAVID HOWELL PETRAEUS entered into at least 13 additional Secrecy Agreements in the course of his DOD employment. In each instance, defendant DAVID HOWELL PETRAEUS agreed to protect classified national security information through proper safeguarding and limiting access to individuals with proper security clearance and official need-to-know.

13. On or about August 31, 2011, defendant DAVID HOWELL PETRAEUS retired from the DOD, after which time he retained his continuing lifelong obligation to the United

States to protect the classified information to which he had been granted access while employed by the DOD.

14. As a condition of his employment by the CIA, defendant DAVID HOWELL PETRAEUS entered into various agreements with the United States, including, for example, the following:

a. On June 16, 2011, as a condition of being granted access to certain SCI, defendant DAVID HOWELL PETRAEUS entered into a NDA with the CIA which was materially identical to the March 2006 NDA he signed while employed by the DOD.

b. On November 26, 2012, following his resignation from the CIA, defendant DAVID HOWELL PETRAEUS entered into a Secrecy Agreement with the CIA in which he agreed, in pertinent part, as follows:

> I understand that in the course of my employment . . . I may be given access to information or material that is classified or is in the process of a classification determination . . . that, if disclosed in an unauthorized manner would jeopardize intelligence activities of the United States Government. I accept that by being granted access to such information or material I will be placed in a position of special confidence and trust and become obligated to protect the information and/or material from unauthorized disclosure.
>
> As a further condition of the special confidence and trust reposed in me by the Central Intelligence Agency, I hereby agree to submit for review by the Central Intelligence Agency any writing or other preparation in any form . . . which contains any mention of intelligence data or activities, or contains any other information or material that might be based on [classified information] . . .
>
> I understand that . . . the disclosure of information that I agreed herein not to disclose can, in some circumstances, constitute a criminal offense . . .

15. On or about November 9, 2012, defendant DAVID HOWELL PETRAEUS resigned from the CIA, after which time he retained his continuing lifelong obligation to the

United States to protect the classified information to which he had been granted access while employed by the CIA.

16. During his tenure at the DOD and the CIA, defendant DAVID HOWELL PETRAEUS held a United States government security clearance allowing him access to classified United States government information. As a result, defendant DAVID HOWELL PETRAEUS had regular access to classified and national defense information relating to DOD and CIA programs, operations, methods, sources, and personnel.

17. During his tenure as Commander of ISAF in Afghanistan, defendant DAVID HOWELL PETRAEUS maintained bound, five-by-eight-inch notebooks that contained his daily schedule and classified and unclassified notes he took during official meetings, conferences, and briefings. The notebooks had black covers and, for identification purposes, defendant DAVID HOWELL PETRAEUS taped his business card on the front exterior of each notebook. A total of eight such books (hereinafter the "Black Books") encompassed the period of defendant DAVID HOWELL PETRAEUS's ISAF Command and collectively contained classified information regarding the identities of covert officers, war strategy, intelligence capabilities and mechanisms, diplomatic discussions, quotes and deliberative discussions from high-level National Security Council meetings, and defendant DAVID HOWELL PETRAEUS's discussions with the President of the United States of America.

18. The Black Books contained national defense information, including Top Secret//SCI and code word information.

19. The National Defense University ("NDU") was an institution of higher education funded by the DOD, intended to facilitate high-level training and education, as well as the

development of national security strategy. It was located on the grounds of Fort Lesley McNair, in Washington, D.C. NDU was a repository for the DOD's classified collections.

20. From in or about July 2009 to in or about July 2012, defendant DAVID HOWELL PETRAEUS's DOD historian gathered and organized the classified materials that defendant DAVID HOWELL PETRAEUS collected during his DOD tenure. Defendant DAVID HOWELL PETRAEUS never provided the Black Books to his DOD historian. Instead, defendant DAVID HOWELL PETRAEUS personally retained the Black Books.

21. In or about September 2012, defendant DAVID HOWELL PETRAEUS's DOD historian transferred defendant DAVID HOWELL PETRAEUS's classified collection to NDU for storage and archiving. Because defendant DAVID HOWELL PETRAEUS personally retained the Black Books, they were never transferred to NDU.

22. On or about August 4, 2011, after defendant DAVID HOWELL PETRAEUS returned permanently to the United States from Afghanistan, during a conversation, recorded by his biographer, defendant DAVID HOWELL PETRAEUS stated that the Black Books were "highly classified" and contained "code word" information:

Biographer:	By the way, where are your black books? We never went through. . .
PETRAEUS:	They're in a rucksack up there somewhere.
Biographer:	Okay . . . You avoiding that? You gonna look through 'em first?
PETRAEUS:	Umm, well, they're really – I mean they are highly classified, some of them. They don't have it on it, but I mean there's code word stuff in there.

23. On or about August 27, 2011, defendant DAVID HOWELL PETRAEUS sent an e-mail to his biographer in which he agreed to provide the Black Books to his biographer.

24. On or about August 28, 2011, defendant DAVID HOWELL PETRAEUS delivered the Black Books to a private residence in Washington, D.C. (the "DC Private Residence"), where his biographer was staying during a week-long trip to Washington, D.C. The DC Private Residence was not approved for the storage of classified information.

25. Thereafter, from on or about August 28, 2011, to on or about September 1, 2011, defendant DAVID HOWELL PETRAEUS left the Black Books at the DC Private Residence in order to facilitate his biographer's access to the Black Books and the information contained therein to be used as source material for his biography, titled *All In: The Education of General David Petraeus*, released by Penguin Press in 2012. No classified information from the Black Books appeared in the aforementioned biography.

26. On or about September 1, 2011, defendant DAVID HOWELL PETRAEUS retrieved the Black Books from the DC Private Residence and returned them to his own Arlington, Virginia home (the "PETRAEUS Residence").

27. On or about November 9, 2012, defendant DAVID HOWELL PETRAEUS resigned from the CIA. Approximately two weeks after his November 9, 2012 resignation, defendant DAVID HOWELL PETRAEUS was debriefed and read-out of the SCI compartments and Special Access Programs to which he previously had been granted access. Specifically, on or about November 26, 2012, defendant DAVID HOWELL PETRAEUS executed two SCI NDAs which contained debriefing acknowledgments, a Secrecy Agreement, and a Security Exit Form. The Security Exit Form included seven provisions regarding his continuing duty to

protect classified information from disclosure. Among other things, by signing the Security Exit Form, defendant DAVID HOWELL PETRAEUS adopted the following provision: "I give my assurance that there is no classified material in my possession, custody, or control at this time." At the time he provided this assurance, the Black Books were still in the PETRAEUS Residence.

28. On or about January 3, 2013, a SCIF, which had been installed at the PETRAEUS Residence by the CIA during defendant DAVID HOWELL PETRAEUS's tenure as CIA Director, was closed and de-accredited. The SCIF was subsequently removed on or about February 13, 2013.

29. On or about April 5, 2013, the FBI executed a court-authorized search warrant at the PETRAEUS Residence and seized the Black Books from an unlocked desk drawer in the first-floor study of the PETRAEUS Residence.

30. Between in or about August 2011, and on or about April 5, 2013, defendant DAVID HOWELL PETRAEUS, being an employee of the United States, and by virtue of his employment, became possessed of documents and materials containing classified information of the United States, and did unlawfully and knowingly remove such documents and materials without authority and thereafter intentionally retained such documents and materials at the DC Private Residence and the PETRAEUS Residence, aware that these locations were unauthorized for the storage and retention of such classified documents and materials.

31. On or about June 12, 2012, in two separate interviews conducted by special agents of the Federal Bureau of Investigation ("FBI") regarding investigations unrelated to the instant offense, defendant DAVID HOWELL PETRAEUS acknowledged that he understood that making false statements to the FBI in the course of a criminal investigation was a crime.

Specifically, on June 12, 2012, defendant DAVID HOWELL PETRAEUS was interviewed in his office at CIA Headquarters in Langley, Virginia, in connection with two media leak investigations. During both interviews, defendant DAVID HOWELL PETRAEUS affirmed in writing, "I understand that providing false statements to the Federal Bureau of Investigation is a violation of law."

32. On or about October 26, 2012, defendant DAVID HOWELL PETRAEUS was interviewed by two FBI special agents in his office at CIA Headquarters in Langley, Virginia. Defendant DAVID HOWELL PETRAEUS was advised that the special agents were conducting a criminal investigation. During that interview, the special agents questioned DAVID HOWELL PETRAEUS about the mishandling of classified information. In response to those questions, defendant DAVID HOWELL PETRAEUS stated that (a) he had never provided any classified information to his biographer, and (b) he had never facilitated the provision of classified information to his biographer. These statements were false. Defendant DAVID HOWELL PETRAEUS then and there knew that he previously shared the Black Books with his biographer.

33. The acts taken by defendant DAVID HOWELL PETRAEUS were in all respects knowing and deliberate, and were not committed by mistake, accident, or other innocent reason.

34. This Statement of Facts includes those facts necessary to support the Plea Agreement between the defendant and the government. It does not include each and every fact known to the defendant or to the government, and it is not intended to be a full enumeration of all the facts surrounding defendant DAVID HOWELL PETRAEUS's case.

//

//

United States Sentencing Guidelines

35. Further, in accordance with Fed. R. Crim. P. 11(c)(1)(B) of the Federal Rules of Criminal Procedure, the United States and the defendant will recommend to the Court that the following provisions of the United States Sentencing Guidelines apply:

Base Offense Level:	6	[U.S.S.G. § 2X5.2]
Abuse of Position of Trust:	+2	[U.S.S.G. § 3B1.3]
Obstruction of Justice	+2	[U.S.S.G. § 3C1.1]
Acceptance of Responsibility	–2	[U.S.S.G. § 3E1.1(a)]
Total Adjusted Offense Level	**8**	

ANNE M. TOMPKINS
UNITED STATES ATTORNEY

2/23/2015

JAMES P. MELENDRES
TRIAL ATTORNEY

Feb. 23, 2015

JILL WESTMORELAND ROSE
ASSISTANT UNITED STATES ATTORNEY

2/23/2015

RICHARD S. SCOTT
TRIAL ATTORNEY

//

//

//

//

//

Defendant's Signature: After consulting with my attorney, and pursuant to the Plea Agreement entered into this day between myself and the United States, I hereby stipulate that the above Factual Basis is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 22 February 2015

David Howell Petraeus
Defendant

Defense Counsel Signature: I am counsel for the defendant in this case. I carefully reviewed the above Factual Basis with the defendant. To my knowledge, the defendant's decision to stipulate to these facts is an informed and voluntary one.

Date: Feb 23, 2015

David E. Kendall
Williams & Connolly LLP
Counsel for the Defendant

Defense Counsel Signature: I am counsel for the defendant in this case. I carefully reviewed the above Factual Basis with the defendant. To my knowledge, the defendant's decision to stipulate to these facts is an informed and voluntary one.

Date: Feb. 23, 2015

Simon A. Latcovich
Williams & Connolly LLP
Counsel for the Defendant

EXHIBIT 9

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	**Criminal Number:**
	:	
	:	**VIOLATION:**
v.	:	
	:	**Count One:**
	:	**18 U.S.C. § 1924**
SAMUEL R. BERGER	:	**Unauthorized Removal and**
Defendant	:	**Retention of Classified Documents**

FACTUAL BASIS FOR PLEA

The United States of America, through its undersigned attorneys, and the defendant, SAMUEL R. BERGER, personally and through his undersigned counsel, hereby stipulate to the following facts pursuant to United States Sentencing Commission Guidelines § 6A1.1 and Rule 32(c)(1) of the Federal Rules of Criminal Procedure:

1. In or about April 2002, the defendant was designated to review Clinton Administration presidential records that were stored by the National Archives and Records Administration ("NARA"). In this capacity, the defendant served as a consultant of the United States. At that time and thereafter, the defendant possessed a United States government security clearance and was aware of the laws and rules regarding the handling and storage of classified information.

2. In 2003, the defendant visited NARA's Washington, D.C. office to review presidential records for production to The National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission). In each of the visits, which occurred on July 18, September 2, and October 2, the defendant reviewed classified documents.

3. On September 2, 2003, after his document review, the defendant concealed and removed a copy of a classified document from its proper place of storage at the National Archives. The defendant was aware that he had no authority to remove the document. The defendant ultimately stored the document at his office in the District of Columbia, knowing that his office was a location not authorized for the storage of classified documents.

4. On October 2, 2003, after another document review, the defendant concealed and removed four copies of classified documents from their proper place of storage at the National Archives. The defendant was aware that he had no authority to remove the documents. The defendant ultimately stored the documents at his office, which he knew was a location that was not authorized for the storage of classified documents. After reviewing the documents that night, the defendant cut three of the documents into small pieces and discarded them.

5. Each of the five documents that the defendant removed on September 2 and October 2 bore markings that identified them as classified United States government documents, and the defendant was aware that they were classified United States government documents. The five documents were copies of versions of the same document.

6. On October 4, 2003, NARA staff called the defendant and advised him that copies of documents were missing from his October 2 review. Initially, the defendant did not tell NARA that he had taken the documents. Later that night, the defendant told NARA that he had accidentally misfiled documents and had found two. On October 5, NARA staff members went to the defendant's office, and the defendant personally handed the staff members two documents, one of which was the document that he removed on September 2, and the other was one of the documents that he removed on October 2.

7. The National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission) received copies of each document in the normal course of document production.

8. During the defendant's July 18, September 2 and October 2 visits to NARA, the defendant made handwritten notes of classified material that he had reviewed. The defendant concealed and removed the notes from NARA. The defendant was aware that he was not authorized to remove his notes.

9. All of the defendant's handwritten notes were returned to the United States.

Dated: 4/1/05

FOR THE DEFENDANT

Samuel R. Berger
SAMUEL R. BERGER
Defendant

LANNY A. BREUER
Counsel for Defendant

FOR THE UNITED STATES

JOHN J. DION
Chief, Counterespionage Section

NOEL L. HILLMAN
Chief, Public Integrity Section

THOMAS REILLY
Trial Attorney
U.S. Department of Justice
Criminal Division
Counterespionage Section

HOWARD SKLAMBERG
Trial Attorney
U.S. Department of Justice
Criminal Division
Public Integrity Section

EXHIBIT 10

Central Intelligence Agency
Inspector General

REPORT OF INVESTIGATION

IMPROPER HANDLING OF CLASSIFIED INFORMATION BY JOHN M. DEUTCH (1998-0028-IG)

February 18, 2000

L. Britt Snider
Inspector General

Daniel S. Seikaly
Assistant Inspector General for Investigations

TABLE OF CONTENTS

OFFICE OF INSPECTOR GENERAL
INVESTIGATIONS STAFF

REPORT OF INVESTIGATION

IMPROPER HANDLING OF CLASSIFIED INFORMATION BY JOHN M. DEUTCH
(1998-0028-IG)

February 18, 2000

This unclassified report has been prepared from the July 13, 1999 version of the classified Report of Investigation at the request of the Senate Select Committee on Intelligence. Information in this version is current as of the date of the original report. All classified information contained in the original Report of Investigation has been deleted.

INTRODUCTION

1. John M. Deutch held the position of Director of Central Intelligence (DCI) from May 10, 1995 until December 14, 1996. Several days after Deutch's official departure as DCI, classified material was discovered on Deutch's government-owned computer, located at his Bethesda, Maryland residence.

2. The computer had been designated for unclassified use only and was connected to a modem. This computer had been used to access **[an Internet Service Provider (ISP)]**, the Internet, **[Deutch's bank]**, and the Department of Defense (DoD). This report of investigation examines Deutch's improper handling of classified information during his tenure as DCI and how CIA addressed this matter.

3. Currently, Deutch is a professor at the Massachusetts Institute of Technology. He also has two, no-fee contracts with the CIA. The first is to provide consulting services to the current DCI and his senior managers; this contract went into effect on December 16, 1996, has been renewed twice, and will expire in December 1999. The second contract is for Deutch's appointment to serve on the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (Proliferation Commission). Under the terms of the second contract, this appointment will continue until the termination of the Commission.

SUMMARY

4. The discovery of classified information on Deutch's unclassified computer on December 17, 1996 was immediately brought to the attention of senior Agency managers. In January 1997, the Office of Personnel Security (OPS), Special Investigations Branch (SIB), was asked to conduct a security investigation of this matter.[1] A technical exploitation team, consisting of personnel expert in data recovery, retrieved the data from Deutch's unclassified magnetic media and computers. The results of the inquiry were presented to CIA senior management in the spring and summer of 1997.

5. The Office of General Counsel (OGC) had been informed immediately of the discovery of classified information on Deutch's computer. Although such a discovery could be expected to generate a crimes report to the Department of Justice (DoJ), OGC determined such a report was not necessary in this case. No other

[1]OPS was established in 1994 and was subsumed as part of the new Center for CIA Security in 1998. The mission of OPS was to collect and analyze data on individuals employed by or affiliated with the Agency, for the purpose of determining initial and continued reliability and suitability for access to national security information. SIB conducts investigations primarily related to suitability and internal security concerns of the Agency. SIB often works with the OIG, handling initial investigations, and refers cases to the OIG and/or the proper law enforcement authority once criminal conduct is detected.

actions, including notification of the Intelligence Oversight Committees of the Congress[2] or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board, were taken until the Office of Inspector General (OIG) opened a formal investigation in March 1998. On March 19, 1998, OIG referred the matter to DoJ. On April 14, 1999, the Attorney General declined prosecution and suggested a review to determine Deutch's suitability for continued access to classified information.

6. Deutch continuously processed classified information on government-owned desktop computers configured for unclassified use during his tenure as DCI. These unclassified computers were located in Deutch's Bethesda, Maryland and Belmont, Massachusetts residences,[3] his offices in the Old Executive Office Building (OEOB), and at CIA Headquarters. Deutch also used an Agency-issued unclassified laptop computer to process classified information. All were connected to or contained modems that allowed external connectivity to computer networks such as the Internet. Such computers are vulnerable to attacks by unauthorized persons. CIA personnel retrieved **[classified]** information from Deutch's unclassified computers and magnetic media related to covert action, Top Secret communications intelligence and the National Reconnaissance Program budget.

7. The OIG investigation has established that Deutch was aware of prohibitions relating to the use of unclassified computers for processing classified information. He was further aware of specific vulnerabilities related to the use of unclassified computers that were connected to the Internet. Despite this knowledge, Deutch processed a large volume of highly classified information on these unclassified computers, taking no steps to restrict

[2]Congressional oversight is provided by the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). The two appropriations committees—the Senate Appropriations Committee, Subcommittee on Defense (SAC) and the House Appropriations Committee, National Security Subcommittee (HAC)—also bear oversight responsibilities.

[3]Hereafter, the residences will be referred to as Maryland and Belmont.

unauthorized access to the information and thereby placing national security information at risk.

8. Furthermore, the OIG investigation noted anomalies in the way senior CIA officials responded to this matter. These anomalies include the failure to allow a formal interview of Deutch, and the absence of an appropriate process to review Deutch's suitability for continued access to classified information.

BACKGROUND

9. In 1998, during the course of an unrelated investigation, OIG became aware of additional circumstances surrounding an earlier allegation that in 1996 Deutch had mishandled classified information. According to the 1996 allegation, classified information was found on a computer configured for unclassified use at Deutch's Maryland residence. This computer had been used to connect to the Internet. Additionally, unsecured classified magnetic media was found in Deutch's study at the residence. Further investigation uncovered additional classified information on other Agency-owned unclassified computers issued to Deutch. In 1998, OIG learned that senior Agency officials were apprised of the results of the OPS investigation but did not take action to properly resolve this matter. The Inspector General initiated an independent investigation of Deutch's alleged mishandling of classified information and whether the matter was appropriately dealt with by senior Agency officials.

PROCEDURES AND RESOURCES

10. OIG assigned a Supervisory Investigator, five Special Investigators, a Research Assistant, and a Secretary to this investigation. The team of investigators interviewed more than 45 persons thought to possess knowledge pertinent to the investigation, including Deutch, DCI George Tenet, former CIA

Executive Director Nora Slatkin, former CIA General Counsel Michael O'Neil, and **[the]** former FBI General Counsel. The team reviewed security files, memoranda for the record written contemporaneously with the events under investigation, data recovered from Deutch's unclassified magnetic media, Congressional testimony, and material related to cases involving other individuals who mishandled classified information. Pertinent information was also sought from the National Security Agency (NSA), the DoD, and an Internet service provider (ISP). In addition, the team reviewed applicable criminal statutes, Director of Central Intelligence Directives, and Agency rules and regulations.

QUESTIONS PRESENTED

11. This Report of Investigation addresses the following questions:

- Why was Deutch issued government computers configured for unclassified use and were his computer systems appropriately marked as unclassified?
- Why was Deutch permitted to retain government computers after resigning as DCI?
- What information was found on Deutch's magnetic media?
  - How was the classified material discovered?
  - What steps were taken to gather the material?
  - What steps were taken to recover information residing on Deutch's magnetic media?

- What are some examples of the classified material that was found?

- What vulnerabilities may have allowed the hostile exploitation of Deutch's unprotected computer media?
  - What was the electronic vulnerability of Deutch's magnetic media?
  - What was the physical vulnerability of Deutch's magnetic media?
- Could it be determined if classified information on Deutch's unclassified computer was compromised?
- What knowledge did Deutch have concerning vulnerabilities associated with computers?
  - What is Deutch's recollection?
  - What did Deutch learn at **[an]** operational briefing?
  - What was Deutch's Congressional testimony?
  - What are the personal recollections of DCI staff members?
- Had Deutch previously been found to have mishandled classified information?
- What laws, regulations, agreements, and policies have potential application?
- How was a similar case handled?

- What actions did senior Agency officials take in handling the Deutch case?
    - What actions were taken by senior Agency officials after learning of this matter?
    - How were the Maryland Personal Computer Memory Card International Association (PCMCIA) cards handled?
    - What was the course of the Special Investigations Branch's investigation of Deutch?
- Should a crimes report initially have been filed on Deutch in this case?
- Should application of the Independent Counsel statute have been considered?
- Were senior Agency officials obligated to notify the Congressional oversight committees or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board? Were these entities notified?
- Why was no administrative sanction imposed on Deutch?
- What was OIG's involvement in this case?
    - When did OIG first learn of this incident?
    - Why did OIG wait until March 1998 to open an investigation?
    - What steps were taken by OIG after opening its investigation?

- What is Deutch's current status with the CIA?

- What was the disposition of OIG's crimes report to the Department of Justice?

CHRONOLOGY OF SIGNIFICANT EVENTS

1995	
January 1	John Deutch establishes Internet access via an **[ISP provider]**.
May 10	Deutch sworn in as DCI.
June 15	Earliest classified document later recovered by technical exploitation team.
August 1	Deutch receives **[a]** briefing on computer attacks.
1996	
December 5	Deutch requests that he be able to retain computers after he leaves office.
December 13	Deutch signs a no-fee consulting contract permitting him to retain government computers.
December 14	Deutch's last day as DCI.
December 17	Classified information found on Deutch's computer in Bethesda, Maryland. Slatkin and O'Neil notified. Slatkin notifies Tenet within a day. O'Neil informs Deutch of discovery.
December 23	Four PCMCIA cards retrieved from Deutch and given to O'Neil.
December 27	Hard drive from Deutch's Maryland computer retrieved.
December 28	Chief/DCI Administration informs IG Hitz of discovery at Deutch's residence.
December 30	Hard drives from residences given to O'Neil.
1997	
January 6	OPS/SIB initiates investigation on Deutch. PDGC and the OPS Legal Advisor discuss issue of a crimes report.
January 9	O'Neil releases to DDA Calder and C/SIB the hard drives from the residences and two of six PCMCIA cards. O'Neil retains four PCMCIA cards from the Maryland residence.
January 9	Memo from ADCI to D/OPS directing Deutch to keep clearances through December 1997.
January 13	Technical exploitation team begins the recovery process.
January 22	Technical exploitation team documents that two hard drives contain classified information and had Internet exposure after classified material placed on drives.

January 30	O'Neil speaks with FBI General Counsel and was reportedly told that FBI was not inclined to investigate.
February 3	O'Neil releases four remaining PCMCIA cards that are subsequently exploited.
February 21	C/SIB meets with OIG officials to discuss jurisdictional issues.
February 27	D/OPS tasked to review all material on hard drives and PCMCIA cards.
March 11	D/OPS completes review of 17,000 pages of recovered items.
July 8	D/OPS's report to ADCI prepared for distribution. Included on distribution are Slatkin, O'Neil, and Richard Calder.
July 21	Slatkin is replaced as Executive Director.
July 30	PDGC reaffirms with OGC attorney that original disks and hard drives need to be destroyed to ensure protection of Deutch's privacy.
August 11	PDGC appointed Acting General Counsel and O'Neil goes on extended annual leave.
August 12	Technical exploitation team confirms selected magnetic media were destroyed per instruction of D/OPS.
September 8	Slatkin leaves CIA.
October 1	O'Neil retires from CIA.
November 24	DCI approves Deutch and other members of the Proliferation Commission for temporary staff-like access to CIA information and facilities without polygraph.
1998	
February 6	OIG is made aware of additional details of the SIB investigation and subsequently opens a formal investigation.
March 19	IG forwards crimes report to DoJ.
May 8	IG letter to IOB concerning Deutch investigation.
June 2	DCI notifies oversight committees of investigation.
1999	
April 14	Attorney General Reno declines prosecution and suggests a review of Deutch's security clearances.

FINDINGS

WHY WAS DEUTCH ISSUED GOVERNMENT COMPUTERS CONFIGURED FOR UNCLASSIFIED USE AND WERE HIS COMPUTER SYSTEMS APPROPRIATELY MARKED AS UNCLASSIFIED?

12. The then-Chief of the Information Services Management Staff (C/ISMS) for the DCI Area, recalled that prior to Deutch's confirmation as DCI, she was contacted by **[Deutch's Executive Assistant]** regarding computer requirements for Deutch. C/ISMS, who would subsequently interface with **[the Executive Assistant]** on a routine basis, learned that Deutch worked exclusively on Macintosh computers. An Information Security (Infosec) Officer assigned to ISMS recalled C/ISMS stating that **[the Executive Assistant]** instructed **[her]** to provide Internet service at the 7th floor Headquarters suite, OEOB, and Deutch's Maryland residence.

13. According to C/ISMS, Deutch's requirements, as imparted by **[his Executive Assistant]**, were for Deutch to have not only access to the Internet, including electronic messaging, but access to CIA's classified computer network from Deutch's offices in CIA Headquarters, OEOB, and his Maryland residence. In addition, Deutch was to be issued an unclassified laptop with Internet capability for use when traveling.

14. A computer specialist, who had provided computer support to Deutch at the Office of the Secretary of Defense, confirmed that, at Deutch's request, he had been hired by CIA to establish the same level of computer support Deutch had received at the Pentagon. At CIA, the computer specialist provided regular and close computer support to Deutch on an average of once a week. The computer specialist recalled **[that Deutch's Executive Assistant]** relayed that he and Deutch had discussed the issue of installing the

classified computer at Deutch's Maryland residence, and Deutch either did not believe he needed or was not comfortable having the classified computer in his home.

15. **[Deutch's Executive Assistant]** also remembered discussions about locating a classified computer at Deutch's Maryland residence. **[The Executive Assistant]**, however, could not recall with any certainty if the computer had in fact been installed. **[The Executive Assistant]** said that a classified system had been installed at his own residence. However, after using it once, he found its operation to be difficult and time consuming, and he had it removed from his residence. **[The Executive Assistant's]** experience with the deployed classified system may have influenced Deutch to decide he did not want one located at his Maryland residence. If so, **[the Executive Assistant]** would have informed the ISMS representative of Deutch's decision.

16. C/ISMS recalled **[the Executive Assistant]** telling her he was not sure Deutch required a classified computer system at Deutch's Maryland residence.

17. A Local Area Network (LAN) technician installed classified and unclassified Macintosh computers in Deutch's 7th floor Headquarters office and in Deutch's OEOB office. The technician also installed a computer configured for unclassified use at Deutch's Maryland residence. The technician stated that Deutch was also provided with an unclassified laptop that had an internal hard drive with modem and Internet access. The computer specialist installed an unclassified computer at Deutch's Belmont residence several months after Deutch was appointed DCI.

18. Personal Computer Memory Card International Association (PCMCIA) cards are magnetic media capable of storing large amounts of data. According to the computer specialist, Deutch's unclassified computers were equipped with PCMCIA card readers. The computer specialist said this configuration afforded Deutch the opportunity to write to the cards and back up

information. One PCMCIA card would reside at all times in a reader that was attached to the unclassified computer, and the other PCMCIA card would be in Deutch's possession. The computer specialist stated that Deutch valued the ability to access, at several locations, data on which he was working. C/ISMS stated that all the unclassified computers and PCMCIA cards provided for Deutch's use contained a green label indicating the equipment was for unclassified purposes. The LAN technician also stated that a concern was to label all of Deutch's automated data processing equipment and magnetic media, including monitors and PCMCIA cards, as either "unclassified" (green label) or "Top Secret" (purple label). The technician stated that his purpose was to make it perfectly clear to Deutch and anyone else using these systems, what was for classified and unclassified use.

19. The OIG has in its possession eight PCMCIA cards that had been used by Deutch. Seven of the eight cards were labeled unclassified; the eighth was not labeled. Four of the cards were from the Maryland residence. Three of the cards were from CIA Headquarters and one was from the OEOB. In addition, OIG received four Macintosh computers and one Macintosh laptop that were used by Deutch. The laptop and two of the computers were marked with green unclassified labels; the other two computers were marked with purple classified labels. One of the classified computers was determined to have come from Deutch's 7th floor Headquarters office; the other from his OEOB office.

WHY WAS DEUTCH PERMITTED TO RETAIN GOVERNMENT COMPUTERS AFTER RESIGNING AS DCI?

20. In a Memorandum for the Record (MFR) dated December 30, 1996, **[the]** then Chief DCI Administration (C/DCI Administration), noted that Deutch announced on December 5, 1996 that he would resign as DCI. That same day, according to C/DCI Administration's MFR, Deutch summoned **[him]** to his office.

Deutch told **[him]** "to look at a way in which he could keep his government computers."

21. The C/DCI Administration's MFR indicated that on December 6, 1996, he spoke with **[the then]** Chief of the Administrative Law Division[4] (C/ALD) in OGC, to ask if Deutch could retain his Agency-issued, unclassified computer after leaving CIA. C/ALD reportedly said that he had concerns with government-owned property that was to be utilized for personal use. He advised that he would discuss the matter with the Principal Deputy General Counsel (PDGC).

22. On December 9, 1996, C/DCI Administration asked ISMS personnel to identify a system configuration which was identical to Deutch's. **[He]** hoped that Deutch would purchase a computer instead of retaining a government-owned computer.

23. According to a December 19, 1996 MFR signed by C/ALD and the PDGC, **[C/ALD]** discussed with **[her]** the request to loan computers to Deutch.[5] **[She]** mentioned the request to General Counsel Michael O'Neil, and stated:

> The only legal way to loan the computers to the DCI would be if a contract was signed setting forth that John Deutch was a consultant to the CIA, and that the computers were being loaned to Mr. Deutch to be used solely for U.S. Government business.

24. Despite her reservations, the PDGC was told by O'Neil to work with C/DCI Administration to formulate a contract for Deutch to be an unpaid consultant. The contract would authorize

---

[4]This division has since been renamed the Administrative Law and Ethics Division.

[5]According to his July 14, 1998 OIG interview, C/ALD prepared the MFR and it was co-signed by the PDGC and **[him]**. **[He]** stated that he took the only copy of it, sealed it in an envelope, and retained it. He sensed that it was likely there would eventually be an Inspector General investigation of the computer loan. **[He]** stated that this was the only time in his career that he has resorted to preparing such an MFR. He stated that he did not tell O'Neil about the MFR nor provide a copy to O'Neil since he judged that to be "unwise." He did not provide a copy of it to the OGC Registry. He said that he has kept it in his "hold box" since he wrote it.

the provision of a laptop computer for three months and a desktop computer for up to a year.

25. According to the MFR:

> On or about 11 December, [the PDGC] was informed by [C/DCI Administration] that the DCI wanted the computers loaned to him because they had the DCI's personal financial data on them and he wanted access to that data. [C/DCI Administration] learned this information in conversation with the DCI. [The PDGC] informed [C/ALD] of this development, and they both agreed that it was improper to loan the computers to the DCI if the true purpose of the loan was to allow the DCI to have continued access to his personal information. [The PDGC] and [C/ALD] also expressed concern that the computers should not have been used by the DCI to store personal financial records since this would constitute improper use of a government computer. [C/ALD] held further conversations with [C/DCI Administration] at which time [C/ALD] suggested that the DCI's personal financial data be transferred to the DCI's personal computer rather than loaning Agency computers to the DCI. [C/DCI Administration] stated that this proposal would not work because the DCI did not own any personal computers. It was then suggested that the DCI be encouraged to purchase a personal computer and that the DCI personal financial records be transferred to the computer.

26. On December 10, 1996, a no-fee contract was prepared between John Deutch, Independent Contractor, and the CIA. Deutch was to provide consulting services to the DCI and senior managers, was to retain an Agency-issued laptop computer for three months, and would retain an Agency-issued desktop computer for official use for one year.

27. C/DCI Administration's MFR notes that on December 13, 1996, he spoke with O'Neil on the telephone. O'Neil directed that the contract being prepared for Deutch be modified to authorize Deutch two computers for a period of one year. The contract was revised on December 13, 1996; the reference to the laptop was

deleted but Deutch was to retain two Agency-issued desktop computers and two STU-III secure telephones for one year.

28. According to the C/DCI Administration's MFR, on December 12, 1996, **[he]** again met with Deutch to discuss matters relating to Deutch's departure. The computer issue was again discussed:

> I mentioned again that I had "strong reservations" about Mr. Deutch maintaining the Government-owned computers and restated that we would be happy to assist moving Mr. Deutch to a personally-owned platform. Mr. Deutch slammed shut his pen drawer on his desk and said thanks for everything without addressing the issue.

29. According to the C/ALD and PDGC MFR, they met with O'Neil on December 13, 1996 to discuss the loan of the computers to Deutch. **[They]** expressed concern that the loan of the computers would be improper if Deutch intended to use the computers for personal purposes. O'Neil stated that he had discussed the matter with Deutch, and Deutch knew he could not use the computers for personal purposes. O'Neil also stated, according to the MFR, that Deutch had his own personal computers and that Deutch would transfer any personal data from the CIA computers to his own. O'Neil said that the contract, which only called for the loan of two computers, had to be re-drafted so that it would cover the loan of a third computer. O'Neil advised that Deutch would not agree to an arrangement in which he would simply use his own computers for official work in place of a loaned CIA computer.[6]

30. The PDGC recalls standing in the receiving line at a farewell function for Deutch and being told by Deutch's wife, "I can't believe you expect us to go out and buy another computer."

31. The MFR indicates that **[the two OGC attorneys]** dropped their objections to the loan of the computers, based on

[6]The OIG investigation has not located any contract that includes a third computer.

assurances from O'Neil that Deutch understood the computers would only be used for official purposes, and he would transfer his personal financial data to his own computer.

32. The contract was signed on December 13, 1996 by O'Neil and Deutch. The effective date for the contract was December 16, 1996. The contract states that Deutch "shall retain, for Government use only, two (2) Agency-issued desktop computers and two (2) STU-III's for the period of one year." Instead, Deutch was issued three PCMCIA cards and two PCMCIA card readers and all government-owned computers were returned to the Agency. On June 23, 1997, he purchased the cards and readers from CIA for $1,476.

WHAT INFORMATION WAS FOUND ON DEUTCH'S MAGNETIC MEDIA?

- **How was the classified material discovered?**

33. Each of the two, unclassified, Agency-owned computers that were to be loaned to Deutch under the provisions of the December 13, 1996 contract were already located at Deutch's Maryland and Belmont residences. To effect the loan of the computers, C/DCI Administration, after consulting with Deutch and his personal assistant, requested that an Infosec Officer perform an inventory of the two government-owned Macintosh computers and peripherals at the Deutch residences. In addition, the Infosec Officer was to do a review to ensure no classified material had been accidentally stored on these computers. While at the Deutch residences, a contract engineer was to document the software applications residing on the computers and, at Deutch's request, install several software applications. This software included FileMaker Pro (e.g., a database) that was to be used with a calendar function and Lotus Notes that would be used with an address book. Deutch has no recollection of authorizing an inventory or a personal visit to his residences and questions the appropriateness of such a visit.

34. On December 17, 1996, the contract network engineer and the Infosec Officer, escorted by a member of the DCI security protective staff, entered Deutch's Maryland residence to conduct the review of the unclassified Macintosh computer and its peripherals. The Infosec Officer reviewed selected data on the computer and two PCMCIA cards, labeled unclassified, located in each of two PCMCIA card drives. Two other PCMCIA cards, one labeled unclassified and the other not labeled, were located on Deutch's desk.

35. The Infosec Officer's initial review located six files containing what appeared to be sensitive or classified information. Although the Infosec Officer believed that numerous other classified or sensitive files were residing on the computer, he concluded the system was now classified and halted his review. The contract network engineer agreed the system should be considered classified based on the information residing on the computer.

36. In addition to these six files, the contract network engineer and the Infosec Officer noted applications that allowed the Macintosh computer external connectivity via a FAX modem. The computer also had accessed the Internet via **[an ISP]**, a DoD unclassified e-mail system, and **[Deutch's bank]** via its proprietary dial-up software.

¨ **What steps were taken to gather the material?**

37. The Infosec Officer telephoned C/DCI Administration and informed him of the discovery of classified material. Although normal information security practice would have been to immediately confiscate the classified material and equipment, C/DCI Administration advised the Infosec Officer to await further instruction. **[He]** proceeded to contact then-CIA Executive Director Nora Slatkin. She referred him to O'Neil for guidance. **[He]** stated that he consulted with O'Neil, who "requested that we print off

copies of the documents for his review." **[He]** contacted the Infosec Officer and instructed him to copy the six classified/sensitive files to a separate disk and return to Headquarters. The Infosec Officer copied five of the six files.[7]

38. After returning to Headquarters, the contract network engineer recalled being contacted by O'Neil. O'Neil advised that he had spoken with Deutch, and Deutch could not understand how classified information came to be found on the computer's hard drive. O'Neil wanted to know if any extraordinary measures were used to retrieve the classified documents and was told the documents were simply opened using Microsoft Word. O'Neil asked the contract network engineer to wait while Deutch was again contacted.

39. Shortly thereafter, the contract engineer stated that Deutch telephoned him and said he could not understand how classified information could have been found on the computer's hard drive as he had stored such information on the PCMCIA cards. The contract engineer told Deutch that the classified information had been found on the PCMCIA cards. The contract engineer recalled suggesting that Deutch might want a new hard drive and replacement PCMCIA cards to store unclassified files that could be securely copied from Deutch's existing PCMCIA cards. According to the contract engineer, Deutch agreed but wanted to review the PCMCIA card files first because they contained personal information.

40. On December 23, 1996, Deutch provided the four PCMCIA cards from his Maryland residence to the DCI Security Staff. These four cards were delivered to O'Neil the same day.

41. On December 27, 1996, the contract network engineer advised C/DCI Administration that two PCMCIA cards previously used by Deutch had been located in an office at Headquarters. One

[7]The Infosec Officer did not copy the sixth document, a letter to DCI nominee Anthony Lake that contained Deutch's personal sentiments about senior Agency officials.

of the cards had an unclassified sticker and was labeled as "Deutch's Personal Disk." The other did not have either a classification sticker or a label. The files on the card with the unclassified sticker had been erased; however, the contract network engineer was able to recover data by the use of a commercially available software utility. Although labeled "unclassified," the contract network engineer noted that the files contained words such as "Secret," "Top Secret Codeword," "CIA," and the name of an Office of Development and Engineering facility. This discovery caused C/DCI Administration, on the advice of **[the]** Associate Deputy Director for Administration (ADDA),[8] to contact O'Neil for assistance in expeditiously retrieving Deutch's Macintosh computers from the Maryland and Belmont residences.

42. On the evening of December 27, 1996, the contract network engineer visited Deutch's Maryland residence, removed Deutch's hard drive, and delivered it to C/DCI Administration. On December 30, 1996, DCI Security Staff delivered to C/DCI Administration the hard drive from Deutch's Belmont residence. Both hard drives were then delivered to O'Neil.

43. On January 6, 1997, OPS/SIB, upon the approval of Slatkin, initiated an internal investigation to determine the security implications of the mishandling of classified information by Deutch.

44. According to Slatkin, she, O'Neil, and Richard Calder, Deputy Director for Administration had several discussions about how to proceed with the investigation. She also discussed with Acting DCI Tenet the issue of how to proceed. As a result, a select group was created to address this matter. Its purpose was to (1) take custody of the magnetic media that had been used by Deutch, (2) review Deutch's unclassified magnetic media for classified data, (3) investigate whether and to what extent Deutch mishandled classified information, and (4) determine whether classified

[8]The former ADDA retired in October 1997.

information on Deutch's computers that had Internet connectivity was compromised.

45. By January 13, 1997, all hardware and files that had been used by Deutch, except four PCMCIA cards retrieved from Deutch's Maryland residence on December 23, 1996, were in SIB's possession. On February 3, 1997, O'Neil released the four PCMCIA cards to Calder, who transferred them to the group on February 4, 1997. Then-Director of Personnel Security (D/OPS) headed the group. Calder was the senior focal point for the group. In addition, a technical exploitation team was formed to exploit the magnetic media.

- **What steps were taken to recover information residing on Deutch's magnetic media?**

46. Five government-issued MacIntosh computer hard drives and eight PCMCIA cards, used by Deutch and designated for unclassified purposes, were examined by a technical exploitation team within the group. Because each of the computers had modems, the PCMCIA cards were considered equally vulnerable when inserted into the card readers attached to the computers. The group had concerns that the processing of classified information on Deutch's five computers that were designated for unclassified information were vulnerable to hostile exploitation because of the modems. The group sought to determine what data resided on the magnetic media and whether CIA information had been compromised.

47. The examination of Deutch's magnetic media was conducted during the period January 10 through March 11, 1997. The technical exploitation team consisted of a Senior Scientist and two Technical Staff Officers, whose regular employment responsibilities concerned **[data recovery]**. The Infosec Officer who participated in the December 17, 1996 security inspection at Deutch's Maryland residence also assisted in the exploitation effort.

48. This team performed the technical exploitation of Deutch's magnetic media, recovered full and partial documents containing classified information, and printed the material for subsequent review. Technical exploitation began with scanning for viruses and making an exact copy of each piece of media used by Deutch. Further exploitation was performed on the copies. The original hard drives and PCMCIA cards were secured in safes. The copies were restored, in a read-only mode, on computers used by the team. Commercially available utility software was used to locate, restore, and print recoverable text files that had been erased. In an attempt to be exhaustive, the Senior Scientist wrote a software program to organize text fragments that appeared to have been part of word processing documents.

49. To accommodate concerns for Deutch's privacy, D/OPS was selected to singularly review all recovered data. He reviewed in excess of 17,000 pages of recovered text to determine which documents should be retained for possible future use in matters relating to the unauthorized disclosure of classified information.

50. Three of the PCMCIA cards surrendered by Deutch subsequent to the security inspection of December 17, 1996, were found to have characteristics that affected exploitation efforts. Specifically, the card labeled "John Backup" could not be fully exploited as 67 percent of the data was unrecognizable due to "reading" errors. The card labeled "Deutch's Disk" was found to have 1,083 "items" that were erased. The last folder activity for this card occurred on "December 20, 1996 at 5:51 [p.m.]." The third card, labeled "Deutch's Backup Disk" and containing files observed during the security inspection, was found to have been reformatted.[9] The card was last modified on "December 20, 1996, [at] 5:19 p.m."

51. Subsequent investigation by OIG revealed that Deutch had paged the contract network engineer at 1000 hours on

[9]Formatting prepares magnetic media for the storing and retrieval of information. Reformatting erases the tables that keep track of file locations but not the data itself, which may be recoverable.

Saturday, December 21, 1996. In an e-mail to C/DCI Administration the following day, the contract network engineer wrote:

> . . . he [Deutch] was experiencing a problem deleting files from one or [sic] his 170MB PCMCIA disks. As near as I [Contractor] can tell the disk has become corrupted and while it appears to allow him [Deutch] to copy files it did not allow him to delete them. We tried several techniques to get around the problem but none were successful. He [Deutch] indicated that he [Deutch] would continue to copy files and not worry about deleting any additional files. He [Deutch] asked what we were going to do with the disks he returned and I told him that we would in all probability degauss them and then physically destroy them . . . .

52. The exploitation efforts resulted in eight pieces of magnetic media yielding classified information. Of the eight pieces, four computers and three PCMCIA cards had prominent markings indicating that the equipment was for unclassified use.[10] Forty-two complete documents **[were classified up to Top Secret and a non-CIA controlled compartmented program]** and 32 text or document fragments classified up to **[Top Secret and a non-CIA controlled compartmented program]** were recovered. Fourteen of the recovered classified documents contained actual printed classification markings (i.e., "SECRET," "Top Secret/**[a non-CIA controlled compartmented program]**") as part of the document. These documents were located on hard drives and/or PCMCIA cards linked to Deutch's residences, 7th floor CIA office, and laptop.

53. Indications of Internet, **[an ISP]**,[11] an unclassified Pentagon computer e-mail,[12] and online banking usage were found

[10] OIG was unable to determine how the Belmont computer was marked because the chassis was disposed of prior to the OIG investigation.

[11] In response to an authorization for disclosure signed by Deutch, **[the ISP]** provided business records to OIG. These records reflect that Deutch, using the screen name **[that was a variation of his name,]** maintained an account with **[the ISP]** since January 1, 1995.

on several of the storage devices. A virus was found to have corrupted a file on the computer formerly located in Deutch's 7th floor CIA office. This computer was labeled "DCI's Internet Station Unclassified," but yielded classified information during the exploitation effort.

54. Recovered computer-generated activity logs reflect, in certain instances, classified documents were created by "John Deutch" during the period of June 1, 1995 and November 14, 1996. Many of the same documents, in varying degrees of completion, were found on different pieces of magnetic media. Additionally, the team recovered journals (26 volumes) of daily activities maintained by Deutch while he served at the DoD and CIA.

55. The following text box provides a summary of Deutch's magnetic media that resulted in the recovery of classified information.

[12]The Department of Defense recovered and produced in excess of 80 unclassified electronic message exchanges involving Deutch from May 1995 through January 1996. These messages reflect Deutch's electronic mail address as **[variations of his name].**

MEDIA/LOCATION	MARKINGS	CONNECTED TO	INFORMATION RECOVERED
Quantum ProDrive Hard Drive/Deutch's Maryland Residence	"Unclassified" on MacIntosh Power PC	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet, **[ISP]**, **[Deutch's bank]**, and DoD electronic mail usage. Indicators of visits to high risk Internet sites[13]
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Disk," "Unclassified," GS001414	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	Three complete classified documents and text fragments including TS/Codeword.[14] **[Bank]** online usage. Card apparently reformatted on 12/20/96 at 5:51 p.m.
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Backup Disk," "Unclassified," GS001490	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	31 complete classified documents and text fragments, five observed during security inspection. **[Bank]** Online Usage. Card apparently reformatted on 12/20/96 at 5:19 p.m.
Quantum ProDrive Hard Drive/Deutch's Belmont Residence	"JMD" on Drive Shell	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet usage. Indicators of visits to high risk Internet sites
MacIntosh Power PC with Hard Drive/Deutch's 7th Floor Office, Original Headquarters Building	"Unclassified," "Property of O/DCI…." "DCI's Internet Station Unclassified"	U.S. Robotics Fax Modem Two PCMCIA Card Readers	One complete classified document and text fragments including TS/Codeword. Word macro concept virus. Internet, DoD electronic mail usage.
MacIntosh Power PC with Hard Drive/Deutch's OEOB Office	"Unclassified," "Property of DCI…"	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Text fragments including TS/Codeword. DoD electronic mail usage.
MacIntosh Powerbook Laptop	"Dr. Deutch Primary," "Unclassified,"	Global Village Internal Modem	Two complete classified documents and text fragments including TS/Codeword.

[13]Certain material viewed by the exploitation team was described as leaving the user's computer particularly vulnerable to exploitation. The exploitation team did not recover this material and it was never viewed by OIG.

[14]Journals containing classified material classified up to TS/SCI encompassing Deutch's DoD and CIA activities were recovered from multiple PCMCIA cards. Deutch stated that he believed his journals to be unclassified.

MEDIA/LOCATION	MARKINGS	CONNECTED TO	INFORMATION RECOVERED
	"Property of /DCI…."		
Microtech PCMCIA Card/ISMS Office	"Deutch's Personal Disk," "Unclassified,"	N/A	Text fragments including TS/Codeword.

- **What are some examples of the classified material that was found?**

56. An October 7, 1996 memorandum from Deutch to the President and the Vice President, found on the hard drive of the Maryland residence computer, **[contained information at the Top Secret/Codeword level]**. The last paragraph of the memorandum notes **[that the information is most sensitive and must not be compromised]**:

> Accordingly, with [National Security Advisor] Tony's [Lake] advice, I have restricted distribution of this information to Chris [Secretary of State Warren Christopher], Bill [Secretary of Defense William Perry], Tony [Lake], Sandy [Deputy National Security Advisor Sandy Berger], Leon Fuerth [the VP's National Security Advisor], and Louie Freeh with whom I remain in close touch.

57. **[The]** former Chief of Staff to the DCI and Slatkin both identified the memorandum as one Deutch composed on the computer at his Maryland residence in their presence on October 5, 1996.

58. In a memorandum to the President that was found on a PCMCIA card from the Maryland residence, Deutch described an official trip. **[The memorandum discussed information classified at the Top Secret level.]**

59. In a memorandum to the President, which was found on a PCMCIA card from the Maryland residence, concerning a trip Deutch **[discusses information classified at the Top Secret/Codeword level]**.

60. Deutch's memorandum to the President found on a PCMCIA card from the Maryland residence also **[discusses a non-CIA controlled compartmented program]**.

61. An undated memorandum from Deutch to the President that was found on a PCMCIA card from the Maryland residence discusses a trip. **[The memorandum discusses information classified at the Secret level.]**

62. Another Deutch memorandum to the President that was found on a PCMCIA card from the Maryland residence **[discusses information classified at the Secret/Codeword level]**.

63. In a memorandum to the President that was found on a PCMCIA card from the Maryland residence, Deutch **[discusses information classified at the Top Secret/Codeword level]**.

64. **[In]** a memorandum with no addressee or originator listed, noted as revised on May 9, 1996 that was found on a PCMCIA card from the Maryland residence, **[Deutch discusses information at the Secret level]**.

65. A document with no heading or date concerning a Deutch trip was found on the hard drive of Deutch's laptop computer which was marked for unclassified use, describes **[information classified at the Secret/Codeword level]**.

66. A document without headings or dates, which was found on the hard drive of the unclassified computer in Deutch's 7th floor office, **[discusses information classified at the Secret/Codeword level]**.

67. Deutch's journal, which was found on a PCMCIA card from the Maryland residence, also covered this topic but in more detail.

68. A spread sheet document **[contains]** financial **[data]** from fiscal year 1995 (FY95) through FY01 **[which is classified at the Secret/compartmented program level]**. It was found on a PCMCIA card from the Maryland residence.

WHAT VULNERABILITIES MAY HAVE ALLOWED THE HOSTILE EXPLOITATION OF DEUTCH'S UNPROTECTED COMPUTER MEDIA?

69. The June 1994 *User's Guide for PC Security*, prepared by CIA's Infosec Officer Services Division, defines unclassified media as media that has never contained classified data. To maintain this status, all media and supplies related to an unclassified computer must be maintained separately from classified computer hardware, media, and supplies. Classified media is defined as media that contains or has contained classified data. It must be appropriately safeguarded from unauthorized physical (i.e., actually handling the computer) and electronic access (i.e., electronic insertion of exploitation software) that would facilitate exploitation. Computer media must be treated according to the highest classification of data ever contained on the media.

70. The *Guide* addresses vulnerabilities relating to computers. Word processors, other software applications, and underlying operating systems create temporary files on internal and external hard drives or their equivalents (i.e., PCMCIA cards). These temporary files are automatically created to gain additional memory for an application. When no longer needed for memory purposes, the location of the files and the data saved on the media is no longer tracked by the computer. However, the data continues to exist and is available for future recovery or unwitting transfer to other media.

71. Additionally, data contained in documents or files that are deleted by the user in a standard fashion continue to reside on magnetic media until appropriately overwritten. These deleted

files and documents can be recovered with commercially available software utilities. Furthermore, computers reuse memory buffers, disk cache, and other memory and media locations (i.e., slack and free space) on storage devices without clearing all previously stored information. This results in residual data being saved in storage space allocated to new documents and files. Although this data cannot be viewed with standard software applications, it remains in memory and can be recovered.

72. As a result of these vulnerabilities, security guidelines mandate procedures to prevent unauthorized physical and electronic access to classified information. An elementary practice is to separately process classified and unclassified information. Hard drives, floppy disks, or their equivalents used in the processing of classified information must be secured in approved safes and areas approved for secure storage when not in use. Individuals having access to media that has processed classified information must possess the appropriate security clearance. Computers that process classified information and are connected to a dial-up telephone line must be protected with a cryptographic device (e.g., STU-III) approved by NSA.

- **What was the electronic vulnerability of Deutch's magnetic media**?

73. Deutch used five government-owned Macintosh computers, configured for unclassified purposes, to process classified information. At least four of these computers were connected to modems that were lacking cryptographic devices and linked to the Internet, **[an ISP]**, a DoD electronic mail server, and/or **[bank]** computers. As a result, classified information residing on Deutch's computers was vulnerable to possible electronic access and exploitation.

74. Deutch did receive e-mail on unclassified computers. One such message from France, dated July 11, 1995, was

apparently from a former academic colleague who claimed to be a Russian.

75. Deutch's online identities used during his tenure as DCI may have increased the risk of electronic attack. As a private subscriber **[to an ISP]**, Deutch used a variant of his name for online identification purposes. He was also listed by true name in **[the ISP's]** publicly available online membership directory. This directory reflected Deutch as a user of Macintosh computers, a scientist, and as living in Bethesda, Maryland. Similarly, Deutch's online identity associated with CIA was:

> johnd@odci[Office of DCI].gov[Government]

and with DoD, as:

> deutch.johnd@odsdpo[Office of Deputy Secretary of Defense Post Office].secdef[Secretary of Defense].osd.mil[Military].

After his confirmation as DCI, Deutch's DoD user identity was unobtainable from their global address database.

76. The technical exploitation team determined that high risk Internet sites had placed "cookies"[15] on the hard drives of the computers from Deutch's residences. According to DDA Calder, SIB's investigation demonstrated that the high risk material was accessed when Deutch was not present. These web sites were considered "risky" because of additional security concerns related to possible technical penetration.

- **What was the physical vulnerability of Deutch's magnetic media?**

77. Deutch's government-issued computer at his primary residence in Maryland contained an internal hard drive and was

[15] A "cookie" is a method by which commercial web sites develop a profile of potential consumers by inserting data on the user's hard drive.

lacking password protection. The drive was not configured for removal and secure storage when unattended even though classified information resided on the drive. Additionally, at the time of the December 17, 1996 security inspection, three of the four unsecured PCMCIA cards yielded classified information: two in PCMCIA readers and one on the desk in Deutch's study. An empty safe was also found with its drawer open.

78. Unlike his predecessors, Deutch declined a 24-hour security presence in his residence, citing concerns for personal privacy. Past practice for security staff, if present in a DCI's residence, was to assume responsibility for securing classified information and magnetic media. To compensate for the lack of an in-house presence, CIA security personnel and local police drove by Deutch's residence on a periodic basis. The two security chiefs responsible for Deutch's protective detail stated that Deutch was responsible for securing classified information in his residence. Deutch said that he thought his residence was secure. In hindsight, he said that belief was not well founded. He said he relied, perhaps excessively, on the CIA staff and security officials to help him avoid mistakes that could result in the unauthorized disclosure of classified information.

79. On May 16, 1995, Deutch approved the installation of a residential alarm system to include an alarm on the study closet. A one-drawer safe was placed in the alarmed closet. These upgrades were completed by early June 1995.

80. According to the first Security Chief assigned to Deutch, the alarm deactivation **[was provided]** code to a resident alien who performed domestic work at the Maryland residence. The alien **[was permitted]** independent access to the residence while the Deutch's were away. CIA security database records do not reflect any security clearances being issued to the alien. The resident alien obtained U.S. citizenship during 1998.

COULD IT BE DETERMINED IF CLASSIFIED INFORMATION ON DEUTCH'S UNCLASSIFIED COMPUTER WAS COMPROMISED?

81. According to the Senior Scientist who led the technical exploitation team, there was "no clear evidence" that a compromise had occurred to information residing on storage devices used by Deutch. In a February 14, 1997 MFR, the Senior Scientist concluded:

> A complete, definitive analysis, should one be warranted, would likely take many months or longer and still not surface evidence of a data compromise.

82. On May 2, 1997, the Chief, SIB wrote in a memorandum to the Director of OPS:

> In consultation with technical experts, OPS investigators determined the likelihood of compromise was actually greater via a hostile entry operation into one of Mr. Deutch's two homes (Bethesda, Maryland and Boston, Massachusetts) to "image" the contents of the affected hard drives . . . . Due to the paucity of physical security, it is stipulated that such an entry operation would not have posed a particularly difficult challenge had a sophisticated operation been launched by opposition forces . . . . The Agency computer experts advised that, given physical access to the computers, a complete "image" of the hard drives could be made in **[a short amount of time]**.

WHAT KNOWLEDGE DID DEUTCH HAVE CONCERNING VULNERABILITIES ASSOCIATED WITH COMPUTERS?

- **What is Deutch's recollection?**

83. During an interview with OIG, Deutch advised that, to the best of his recollection, no CIA officials had discussed with him

the proper or improper use of classified and unclassified computers. Around December 1997, approximately one year after he resigned as DCI, he first became aware that computers were vulnerable to electronic attack. Not until that time, Deutch commented, had he appreciated the security risks associated with the use of a modem or the Internet in facilitating an electronic attack.[16]

84. Although stating that he had not received any CIA security briefings relating to the processing of information on computers, Deutch acknowledged that classified information must be properly secured when unattended. Specifically, he stated, "I am completely conscious of the need to protect classified information."

85. In response to being advised that classified information had been recovered from government computers configured for his unclassified work, Deutch stated that he "fell into the habit of using the [CIA] unclassified system [computers] in an inappropriate fashion." He specifically indicated his regret for improperly processing classified information on the government-issued Macintosh computers that were connected to modems. Deutch acknowledged that he used these government-issued computers to access **[the ISP]**, **[his bank]**, the Internet, and a DoD electronic mail server.

86. Deutch indicated he had become accustomed to exclusively using an unclassified Macintosh computer while serving at DoD. He acknowledged that prior to becoming DCI, he was aware of the security principle requiring the physical separation of classified and unclassified computers and their respective information. However, he said he believed that when a file or document was deleted (i.e., dragged to the desktop trash folder), the information no longer resided on the magnetic media nor was it recoverable. Deutch maintained that it was his usual

[16]After reading the draft ROI, Deutch's refreshed recollection is that it was in December 1996, not December 1997, that he first became aware that his computer priorities resulted in vulnerability to electronic attack.

practice to create a document on his desktop computers, copy the document to an external storage device (e.g., floppy disk), and drag the initial document to the trash folder.

87. During his tenure as DCI, Deutch said that he intentionally created the most sensitive of documents on computers configured for unclassified use. Deutch stated that if these documents were created on the classified CIA computer network, CIA officials might access the system at night and inappropriately review the information. Deutch said that he had not spent a significant amount of time thinking about computer security issues.

88. Deutch advised that other individuals had used the government computer located in the study of his Maryland residence. Deutch's wife used this computer to prepare reports relating to official travel with her husband. Additionally, **[another family member]** used this computer to access **[a university]** library. Regarding the resident alien employed at the Maryland residence, Deutch indicated that, to his knowledge, this individual never went into the study. He further believed that the resident alien normally worked while Mrs. Deutch was in the residence.

- **What did Deutch learn at [an] operational briefing?**

89. On August 1, 1995, Deutch and several senior CIA officials receive**[d]** various operational briefings.

90. **[During these briefings,]** Deutch was specifically told that data residing on a **[commercial ISP network was vulnerable to a computer attack.]**

91. Deutch did not have a specific recollection relating to the August 1, 1995 briefing. He could not recall making specific comments to briefers concerning his use of **[his ISP]** and the need to switch to another ISP.

♦ **What was Deutch's Congressional testimony?**

92. On February 22, 1996, DCI Deutch testified before the Senate Select Committee on Intelligence on the subject of worldwide security threats to the United States during the post-Cold War era. During his appearance, Deutch stated:

> Mr. Chairman, I conclude with the growing challenge of the security of our information systems. There are new threats that come from changing technologies. One that is of particular concern to me is the growing ease of penetration of our interlocked computer and telecommunications systems, and the intelligence community must be in the future alert to these needs- -alert to these threats.

93. On June 25, 1996, DCI Deutch testified in front of the Permanent Investigations Subcommittee of the Senate Governmental Affairs Committee. The Committee was investigating the vulnerability of government information systems to computer attacks. Deutch's testimony focused on information warfare, which he defined as unauthorized foreign penetrations and/or manipulation of telecommunications and computer network systems.

94. In his prepared statement submitted to the Committee, Deutch indicated:

> . . . like many others in this room, [I] am concerned that this connectivity and dependency [on information systems] make us vulnerable to a variety of information warfare attacks . . . . These information attacks, in whatever form, could . . . seriously jeopardize our national or economic security . . . . I believe steps need to be taken to address information system vulnerabilities and efforts to exploit them. We must think carefully about the kinds of attackers that might use information warfare techniques, their targets, objectives, and methods . . . . Hacker tools are readily available on the Internet, and hackers themselves are a source of expertise for any nation

> or foreign terrorist organization that is interested in developing an information warfare capability . . . . We have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks.

- **What are the personal recollections of DCI staff members?**

95. Deutch's **[Executive]** Assistant served in that position from February 1995 through July 1996 at DoD and CIA. **[He]** considered Deutch to be an "expert" computer user. **[The Executive Assistant]** was responsible for coordinating the preparation of computers for Deutch's use upon his confirmation as DCI. During the transition, **[the Executive Assistant]** informed Deutch that the processing of classified and unclassified information required the use of separate computers to prevent the improper transfer of data. **[The Executive Assistant]** stated that the computer support staff at CIA went to great lengths to appropriately label Deutch's computers as either classified or unclassified in order to prevent improper use.

96. **[The Executive Assistant]** advised that he never informed Deutch that it was permissible to process classified information on a computer configured for unclassified use. **[The Executive Assistant]** stated that he was not aware that Deutch processed classified information on computers configured for unclassified use. When advised that classified material had been recovered from multiple computers used by Deutch that had been configured for unclassified purposes, **[the Executive Assistant]** responded that he was at a loss to explain why this had occurred.

97. **[The Executive Assistant]** remembered the August 1, 1995 briefing. **[The Executive Assistant]** said that Deutch was very concerned about information warfare and, specifically, computer systems being attacked. **[The Executive Assistant]** recalled that during his CIA tenure, Deutch and he became aware of efforts by **[others]** to attack computer systems.

98. The computer specialist who provided regular information support to Deutch while he served at DoD, was hired at Deutch's request in June 1995 to provide computer support to the DCI Area. After arriving at CIA, the computer specialist provided direct computer support to Deutch about once per week. At times, Deutch, himself, would directly contact the computer specialist for assistance.

99. The computer specialist described Deutch as a "fairly advanced" computer user who sought and used software that was considered to be above average in complexity. Deutch was further described as having "more than a passing interest in technology" and asking complex computer-related questions. The computer specialist found that Deutch "kept you on your toes" with questions that required research **[for]** the answers. Deutch was also described as having a heightened interest in the subject of encryption for computers. The computer specialist recalled that all computer equipment issued to Deutch was appropriately labeled for classified or unclassified work.

100. The computer specialist remembered a conversation with Deutch on the subject of computer operating systems creating temporary documents and files. This conversation occurred while the computer specialist restored information on Deutch's computer after it had failed (i.e., crashed). Deutch watched as documents were recovered and asked how the data could be restored. Deutch was also curious about the utility software that was used to recover the documents. The computer specialist explained to Deutch that data was regularly stored in temporary files and could be recovered. Deutch appeared to be "impressed" with the recovery process.

101. During another discussion, the computer specialist recalled telling Deutch that classified information could not be moved to or processed on an unclassified computer for security reasons.

102. The computer specialist considered Deutch to be a knowledgeable Internet user who had initially utilized this medium while a member of the scientific community at the Massachusetts Institute of Technology. During September 1996 and while Deutch was still serving as DCI, the unclassified CIA Internet web page was altered by a group of Swedish hackers. During discussions with the computer specialist concerning this incident, Deutch acknowledged that the Internet afforded the opportunity for the compromise of information.

103. C/ ISMS, who supervised computer support provided to Deutch from the time of his arrival at CIA through October 1996, considered Deutch to be a computer "super user." Deutch only sought assistance when computer equipment was in need of repair or he desired additional software. The computer support supervisor stated that all unclassified computers and PCMCIA cards that were provided for Deutch's use had green labels indicating they were for unclassified purposes.

104. The LAN technician, who initially configured Deutch's computers at CIA, stated that he labeled all equipment to reflect whether it was designated for classified or unclassified purposes. The technician's stated purpose was to make it clear to Deutch what information could be processed on a particular computer given the requirement that Deutch have access to both classified and unclassified computers.

HAD DEUTCH PREVIOUSLY BEEN FOUND TO HAVE MISHANDLED CLASSIFIED INFORMATION?

105. Beginning in 1977, when he was the Director of Energy Research at the Department of Energy (DoE), Deutch had a series of positions with U.S. Government agencies that required proper handling and safeguarding of classified information to include sensitive compartmented information and DoE restricted data.

106. From 1982 to 1988, Deutch was a paid consultant to the CIA's National Intelligence Council. In 1984, he was also under contract to the CIA's Directorate of Intelligence, Office of Scientific Weapons and Research, serving as a member of the DCI's Nuclear Intelligence Panel.

107. **[CIA records reflect Deutch had problems before becoming Director with regard to the handling of classified information. Other specific information on security processing and practices has been deleted due to its level of classification.]** Deutch served as DoD's Undersecretary for Acquisitions and Technology and Deputy Secretary of Defense prior to his appointment as DCI.

108. On November 21, 1995, DCI Deutch signed a CIA classified information non-disclosure agreement concerning a sensitive operation. Several provisions pertain to the proper handling of classified information and appear to be relevant to Deutch's practices:

> I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, ...
>
> I have been advised that . . . negligent handling of classified information by me could cause damage or irreparable injury to the United States. . . .
>
> I have been advised that any breach of this agreement may result in the termination of any security clearances I hold; removal from any position or special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. . . .

> I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access . . . upon the conclusion of my employment . . . .
>
> I have read this Agreement carefully and my questions, if any, have been answered.

OIG also obtained similar, non-disclosure agreements signed by Deutch during his employment at DoD.

WHAT LAWS, REGULATIONS, AGREEMENTS, AND POLICIES HAVE POTENTIAL APPLICATION?

109. Title 18 United States Code (U.S.C.) §793, "Gathering, transmitting or losing defense information" specifies in paragraph (f):

> Whoever, being entrusted with or having lawful possession or control of any document, writing, . . . or information, relating to national defense . . . through gross negligence permits the same to be removed from its proper place of custody . . . shall be fined under this title or imprisoned not more than ten years, or both.

110. Title 18 U.S.C. §798, "Disclosure of classified information" specifies in part:

> Whoever, knowingly and willfully . . . uses in any manner prejudicial to the safety or interest of the United States . . . any classified information . . . obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes . . . shall be fined under this title or imprisoned not more than ten years, or both.

111. Title 18 U.S.C. §1924, "Unauthorized removal and retention of classified documents or material" specifies:

> Whoever, being an officer, employee, contractor or consultant of the United States, and, by virtue of his office, employment, position or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than $1,000, or imprisoned for not more than one year, or both.

112. The National Security Act of 1947, CIA Act of 1949, and Executive Order (E.O.) 12333 establish the legal duty and responsibility of the DCI, as head of the United States intelligence community and primary advisor to the President and the National Security Council on national foreign intelligence, to protect intelligence sources and methods from unauthorized disclosure.

113. Director of Central Intelligence Directive (DCID) 1/16, effective July 19, 1988, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," reiterates the statutory authority and responsibilities assigned to the DCI for the protection of intelligence sources and methods in Section 102 of the National Security Act of 1947, E.O.s 12333 and 12356, and National Security Decision Directive 145 and cites these authorities as the basis for the security of classified intelligence, communicated or stored in automated information systems and networks.

114. DCID 1/21, effective July 29, 1994, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," specifies in paragraph 2:

> All [Sensitive Compartmented Information] must be stored within accredited SCIFs. Accreditation is the formal affirmation that the proposed facility meets physical security standards imposed by the DCI in the physical security standards manual that supplements this directive.

115. Headquarters Regulation (HR) 10-23, Storage of Classified Information or Materials. Section C (1) specifies:

> Individual employees are responsible for securing classified information or material in their possession in designated equipment and areas when not being maintained under immediate personal control in approved work areas.

116. HR 10-24, "Accountability and Handling of Collateral Classified Material," prescribes the policies, procedures, and responsibilities associated with the accountability and handling of collateral classified material. The section concerning individual employee responsibilities states:

> Agency personnel are responsible for ensuring that all classified material is handled in a secure manner and that unauthorized persons are not afforded access to such material.

117. HR 10-25, "Accountability and Handling of Classified Material Requiring Special Control," sets forth policy, responsibilities, and procedures that govern the transmission, control, and storage of Restricted Data, treaty organization information, cryptographic materials, and Sensitive Compartmented Information. The section states:

> Individuals authorized access to special control materials are responsible for observing the security requirements that govern the transmission, control, and storage of said materials. Further, they are responsible for ensuring that only persons having appropriate clearances or access approvals are permitted access to such materials or to the equipment and facilities in which they are stored.

HOW WAS A SIMILAR CASE HANDLED?

118. In November 1996, a senior CIA official was determined to have routinely authored CIA unique, classified documents on his personal home computer and CIA-issued laptop computer configured for unclassified use. Some of the documents were at the Secret and Top Secret/Codeword level. In addition, the senior

Agency official had used both computers to visit Internet sites. In addition, the senior official's family members had access to both computers. However, there was no way to determine if the computer hard drives had been compromised.

119. On December 12, 1996, **[the]** OPS Legal Advisor, referred a crimes report to the Associate General Counsel (AGC) in the CIA Office of General Counsel. On December 13, 1996, the AGC forwarded to DoJ a crimes report on this incident. In June 1997, a Personnel Evaluation Board (PEB) decided to downgrade the official from an SIS-06 to SIS-05, issue a two-year letter of reprimand including caveats against monetary and non-monetary awards and promotions, and suspend the official for 30 workdays without pay. In addition, the PEB directed the Office of Congressional Affairs to brief the appropriate Congressional intelligence committees about this senior official's breach of security. On September 11, 1997, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were briefed on this incident by Executive Director David Carey.

WHAT ACTIONS DID SENIOR AGENCY OFFICIALS TAKE IN HANDLING THE DEUTCH CASE?

- **What actions were taken by senior Agency officials after learning of this matter?**

120. After learning from O'Neil on December 17, 1996 that classified information had been discovered at Deutch's Maryland residence, Slatkin brought the issue to the attention of Acting DCI George Tenet within one day. She asserted there were multiple discussions with Tenet over time and "everything" had his concurrence. Slatkin explained that the issue was too sensitive for her and Tenet had the responsibility for making the decisions relating to the Deutch incident. Slatkin stated she was also concerned that others may have perceived that she and O'Neil, due

to their close association with Deutch, should recuse themselves from the matter. Slatkin said that Tenet gave her the responsibility for coordinating this matter. She relied on O'Neil for legal advice and Calder for a technical review.

121. Calder recalled one or possibly two "late night discussions" with Tenet concerning the Deutch incident. One meeting was to provide Tenet "the lay of the land." At the second meeting, Tenet gave instructions for the investigation to proceed unimpeded.

122. Tenet stated he first learned of the discovery of classified information on the Maryland computer in December 1996 or January 1997 from either the Chief, DCI Security Staff or from the C/DCI Administration. Tenet recalled that Slatkin and O'Neil got involved in deciding how to handle the issue. Tenet did not hear about any disagreements concerning the handling of this matter and believed that Slatkin and O'Neil did not want to place Tenet in the position of adjudicating a matter involving Deutch.

123. O'Neil stated that he is uncertain how he first learned of the discovery of classified information on Deutch's Maryland computer. However, according to C/DCI Administration, a meeting was held on the afternoon of December 17, 1996 with O'Neil. At that meeting, O'Neil stated Deutch was concerned about retaining his personal information before returning the four PCMCIA cards to CIA. C/DCI Administration offered a solution by offering to provide Deutch with replacement PCMCIA cards on which Deutch could transfer his personal information. O'Neil passed this suggestion to Deutch, and Deutch agreed. Afterward, the contract network engineer also talked to Deutch about copying his personal information to the new PCMCIA cards. The contract network engineer recalled Deutch wanting to review the files on the original PCMCIA cards because they contained personal information.[17]

[17] In his interview with OIG, Deutch confirmed he reviewed the original PCMCIA cards to delete personal information.

124. **[The]** PDGC learned of the matter on the day of its discovery. Between that date, December 17, 1996, and the date SIB began its investigation, the PDGC recalled there was an ongoing dialogue involving O'Neil, Slatkin, and Calder. The PDGC stated that O'Neil kept her abreast of developments.

125. The former ADDA believes that C/DCI Administration initially apprised her of the discovery on December 26, 1996. Her first concern related to properly securing the classified information at the Deutch residence, which the C/DCI Administration said he would handle. Several days later, **[she]** learned that the magnetic media at the Maryland residence had been secured, although not as expeditiously as she desired. **[She]** stated that the PCMCIA cards that had been in Deutch's possession were given to O'Neil.

126. The former ADDA stated that Calder, Slatkin, and O'Neil held a series of meetings to discuss how to handle the incident. She recalled other issues surfacing, such as the resident alien employed as a maid at the Deutch residence; Deutch's personal financial records being maintained on government-owned computers; "disks" Deutch carried in his shirt pocket; and other government-issued unclassified computers at Deutch's Belmont residence, the OEOB, and Headquarters that may contain classified information.

127. D/OPS was first briefed on the case by Calder, who became **[his]** senior focal point with the former ADDA serving as a back-up. D/OPS never discussed the case directly with either Slatkin or O'Neil. He remembered that the specific permission of Slatkin or O'Neil was needed to involve others in the case. According to D/OPS, the former ADDA believed that Slatkin and O'Neil had as their main concern the fear that sensitive and personal information contained in Deutch's journals would leak. Slatkin stated it was standard operating procedure, when dealing with sensitive investigations or operations, to review requests to involve additional individuals. She claimed it was common

practice for her to review such requests with the DCI. She does not recall denying any request to involve others in this case.

128. According to C/SIB, D/OPS asked him to conduct a security investigation to determine: (1) if classified information found on Deutch's government-issued unclassified computer had been compromised, and (2) what conditions would allow a compromise to occur. C/SIB said he was to determine the "who, what, where, when, and why." C/SIB expected "noteworthy" information would be compared to the appropriate DCID security standards and adjudication would be based on SIB's findings. He recalled advising the D/OPS that classified information on unclassified media could involve a potential violation of federal law.

129. The OPS Legal Advisor wrote in a January 7, 1997 MFR that he attended a meeting the previous day with Calder, D/OPS, C/SIB, and an SIB investigator to discuss the discovery of the classified information on the computer at Deutch's Maryland residence. Among the issues discussed were:

> Acknowledgment that because this case involves former DCI Deutch, whatever actions are taken by OPS and other parties will be scrutinized very closely. Therefore, it was stressed by everyone at the meeting that the security investigation of this case must follow the same pattern established in other cases where employees have placed classified information on a computer and possibly exposed that information to access by unauthorized individuals.

130. Calder stated that the OPS Legal Advisor was strident in his concern that Deutch be treated the same as any other Agency employee and senior officials should scrupulously avoid showing special treatment to Deutch. Calder agreed that the investigation should resemble those conducted for similar violations by other Agency personnel. He stated he was concerned that he insulate the OPS/SIB personnel and the C/DCI Administration to ensure that they did not "get ground up."

131. Calder stated that he initially assumed this matter would arise again in the future, possibly with a Congressional committee. Therefore, he insisted that the case be conducted in the same manner as for any CIA employee.

♦ **How were the Maryland PCMCIA cards handled?**

132. SIB sought to obtain and secure all the government-issued computer equipment and magnetic media that had been provided to Deutch, such as the computers and peripherals that were at both Deutch residences. By early January 1997, all government-issued computer equipment and magnetic media used by Deutch had been turned over to SIB with the exception of the four PCMCIA cards that had been observed by the inspection team on December 17, 1996.

133. O'Neil recalled that a DCI Security officer brought him the four PCMCIA cards from the Maryland residence. O'Neil stated he put the PCMCIA cards in his safe and never opened the envelope that contained them. He said he gave the PCMCIA cards to Calder without argument when asked.

134. Calder recalled that O'Neil told him that Deutch wanted the PCMCIA cards destroyed. Calder advocated the position that the cards should not be tampered with and must be maintained in the event of a future leak investigation. According to Calder, O'Neil and Deutch came to realize the PCMCIA cards could not be summarily destroyed. Calder stated that he went to O'Neil on three or four occasions in an attempt to obtain the four PCMCIA cards, and it took two to three weeks to reach a satisfactory arrangement for O'Neil to surrender them.

135. The PDGC also recalled, "We had to hammer O'Neil to give the [PCMCIA] cards to Security." The PDGC believes Slatkin, whose "loyalty to Deutch was incredible," and Deutch pressured O'Neil not to allow others to have access to the personal information on the cards. The PDGC stated that she, Calder, the OPS Legal Advisor, and C/SIB "pushed the other way" and advocated that O'Neil turn the cards over to Security. C/SIB confirmed the difficulty obtaining the four PCMCIA cards in O'Neil's possession.

136. The former ADDA recalled advising Slatkin that the investigation was dragging on, and that unidentified individuals believed that this was being done purposely in order to "cover up" the event. The former ADDA told Slatkin that O'Neil's withholding of the four cards supported the "cover up" perception.

137. According to Slatkin, after the former ADDA told Slatkin about the problem with the four remaining disks, she requested a meeting with Tenet, O'Neil, and Calder. Tenet reportedly told O'Neil to surrender the PCMCIA cards to Calder. Calder stated that O'Neil claimed that, although Calder had discussed his need for the cards, Calder had never specifically asked O'Neil to turn them over. C/SIB states that Calder, in his presence, "specifically ask[ed]" O'Neil to release the PCMCIA cards. Slatkin said she would have reacted earlier if she had known of Calder's concern.

138. According to O'Neil, he, Tenet, Slatkin, and Calder had conversations over a period of several weeks on the exploitation of the PCMCIA cards and protecting Deutch's privacy. After Tenet decided on the process for handling the cards, they were delivered to Calder. O'Neil said he never refused to turn over the cards for exploitation.

139. O'Neil surrendered the four PCMCIA cards to Calder on February 3, 1997. Calder provided the cards to C/SIB on February 4, 1997.

- **What was the course of the Special Investigations Branch's investigation of Deutch?**

140. Calder stated that, in his view, Slatkin and O'Neil did not want Deutch's name "to be besmirched" and O'Neil assumed the role of an "interlocutor." He also said that Slatkin and O'Neil were particularly sensitive that a possible vendetta would be orchestrated by security personnel as a response to interference by O'Neil and Slatkin in a previous, unrelated, joint investigation

involving the DoD.[18] Calder characterized his encounters with Slatkin regarding the Deutch investigation as "always difficult discussions" and that it was continually necessary to "push forward" and achieve "a negotiated peace." Slatkin, however, stated that she had no involvement in the DoD-CIA investigation except to determine why the Acting Director and she had not been informed of the notification to DoD.

141. The OPS Legal Advisor believes Slatkin "constrained the investigative apparatus." He cited, as an example, Slatkin advocating allowing Deutch to go into the files to determine if the information was personal or belonged to the CIA. The OPS Legal Advisor stated that the policy has always been that an individual who places personal information on a government computer loses the expectation of privacy and the material reverts to the control of the government authorities. The OPS Legal Advisor stated that Calder, D/OPS, and the former ADDA tried to keep the investigation on track. Slatkin denied interfering with the investigation. She stated that she did not make any unilateral decisions about the course of the investigation. All requests made by Deutch were relayed to O'Neil, Calder, and Tenet.

142. In the early stages of SIB's investigation, Calder recalled telling Tenet there was no indication of a compromise and the investigation was proceeding. Calder said that the investigators showed him some of the classified material. It included Top Secret/**[Codeword]** information; collection methods and imagery; and possibly information identifying CIA operations officers.

[18]Based on a series of intelligence leaks in the *Washington Times*, CIA's Special Investigations Branch determined the leaks were related to the distribution of intelligence reports at the Pentagon. In a routine procedure, CIA sent a letter to DoD and the Defense Intelligence Agency (DIA) to coordinate an investigation. According to Calder, the DIA nominee for Director of that organization contacted Slatkin and demanded an explanation of the CIA's actions. Subsequently, O'Neil requested that DDA Calder rescind the CIA letter. Calder states that O'Neil commented the actions of CIA security officials appeared to be "vindictive and malicious."

143. Calder stated that after a complete package of Deutch's material was recovered from the magnetic media, the question arose as to the proper person to review the material. Because the material contained personal information, Calder recalled that Deutch wanted to review the material himself or have O'Neil do the review. Ultimately, Slatkin selected D/OPS for the task.

144. As part of the SIB investigation, C/SIB interviewed staff from DCI Security and the DCI Information Services Management Staff; he also planned to interview **[Deutch's Executive Assistant]** and Deutch.[19] On March 24, 1997, Calder informed C/SIB that C/SIB would not be the one to interview Deutch. (Calder later explained to OIG investigators that a concern existed to have somebody who was politically sensitive question Deutch, should such an interview prove necessary.) At Calder's request, SIB composed questions to ask Deutch and, on May 15, 1997, forwarded them to D/OPS for review. However, C/SIB also informed Calder that SIB would not continue their efforts because certain interviewees (i.e., Deutch) were not accessible to SIB. Calder agreed.

145. The OPS Legal Advisor stated that, normally, a case similar to Deutch's would not only be referred to SIB for investigation, but a contemporaneous damage assessment would also be conducted. If the subject was a former employee, typically the subject would be banned from holding a security clearance and future CIA employment.

146. After D/OPS reviewed the 17,000 pages of recovered documents, he prepared a report of his findings and attached a copy of C/SIB's separate, signed report. He recalled receiving a "panicky" call from the former ADDA relaying that Slatkin wanted the report immediately.

[19] C/SIB noted that he did not review Deutch's official security file. OIG reviewed the file.

147. Calder was familiar with D/OPS's report and stated that it was the lone document that he retained following the conclusion of the investigation. He recalled sending the report to Slatkin and receiving it back with marginal comments, possibly asking if the PCMCIA cards had been destroyed. Slatkin recalled that the draft report was hand-carried to her by Calder. After she read the report, she made written editorial comments requesting clarification and returned the draft report to either Calder or D/OPS. She received the final report, reviewed it, and personally handed it to Tenet. Tenet does not remember ever seeing D/OPS's report, nor does he recall any of the details of the report. He said it is possible that someone told him about the report or showed it to him.

148. A signed copy of the D/OPS report dated July 8, 1997, was recovered from the DDA's Registry. It did not have any notes on the text or attached to the document. No copy was ever recovered from the DCI's Executive Registry, the Executive Director's Office, Calder's personal safe, or anywhere in OGC.

149. There was considerable discussion of what should be done with the magnetic media after its material was catalogued. O'Neil said that Tenet's decision was to retain permanently the PCMCIA cards and a copy of all the classified documents. Calder, however, said there was some disagreement among the parties and the ultimate decision was to destroy the material, including the magnetic media. At the end of the investigation, Calder remembered asking D/OPS what happened to the PCMCIA cards and being told the disks were about to be destroyed or had been destroyed. Nevertheless, Calder said he was not certain the cards were destroyed.

150. After D/OPS sent his report to Calder, the OPS Legal Advisor received an e-mail from the C/ALD stating that the PDGC had spoken to Calder about the SIB investigation of Deutch. Calder reportedly said Deutch would be given a code of conduct briefing in conjunction with Deutch's security briefing as a member of the

Proliferation Commission.[20] On August 3, 1997, the OPS Legal Advisor sent the C/ALD an e-mail response expressing concern that no one at DoD or the White House had, so far, been notified about a possible compromise of information. He also raised the issue of Deutch retaining his security clearance. The OPS Legal Advisor wrote:

> I remain unpersuaded, however, that the CIA has done everything it can in this case to protect CIA and DOD equities. The investigation has been one in name only . . . . I'm certainly not persuaded that giving this man a security clearance is in the best interest of the U.S. Government or the President . . . . I mean, geez, when was the last time a subject of an investigation was not interviewed because he objected to talking to security officers and the EXDIR, a personal friend, used her position to short circuit an investigation? Let's be honest with each other, this so-called investigation has been handled in a manner that was more designed not to upset friendships than to protect the interests of the U.S.G.

151. C/SIB had also relayed his concerns about the possible exposure of DoD classified material of ongoing military operations. In his chronology, C/SIB wrote that on March 14, 1997, Calder decided appropriate senior level DoD officials should be briefed on a potential compromise. Calder planned to brief Slatkin of this decision. C/SIB indicated he again reminded Calder of the need for DoD notification on March 24, 1997. The OIG investigation did not locate any information that such notification occurred until OIG notified DoD on June 17, 1998.

152. As of May 1998, when OIG began its investigation, there was no information in Deutch's official Agency security file concerning the SIB investigation or its findings nor was there any evidence of a security adjudication.

---

[20]There is no record of Deutch receiving a code of conduct briefing. The Center for CIA Security provided an SCI briefing to the Commission members on two occasions. Deutch was present for the second one-hour presentation on November 17, 1998.

SHOULD A CRIMES REPORT INITIALLY HAVE BEEN FILED ON DEUTCH IN THIS CASE?

153. Title 28 U.S.C. §535, "Investigation of crimes involving Government officers and employees," requires that

> any information, allegation or complaint received in a department or agency of the executive branch of the government relating to violations of Title 18 [U.S. Code] involving Government officers and employees shall be expeditiously reported to the Attorney General.

154. Section 1.7(a) of E.O. 12333, United States Intelligence Activities, requires senior officials of the intelligence community to "report to the Attorney General possible violations of federal criminal laws by employees and [violations] of specified criminal laws by any other person . . . ." This responsibility is to be carried out "as provided in procedures agreed upon by the Attorney General and the head of the department or agency concerned . . . ."

155. Pursuant to Part 1.7(a) of E.O. 12333, the DCI and the Attorney General agreed on crimes reporting procedures for CIA on March 2, 1982. These procedures, which are included as Annex D to HR 7-1, were in effect from that time until August 2, 1995, when they were superseded by new procedures.[21] The new procedures are contained in a document, "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," signed by DCI Deutch.

156. According to the Memorandum of Understanding (MOU),

> [w]hen the General Counsel has received allegations, complaints, or information (hereinafter allegations) that an

[21] Although HR 7-1 Annex D was superseded by the MOU on August 2, 1995, the current version of HR 7-1 Annex D is dated December 23, 1987 and does not reflect the changes caused by the subsequent MOU.

> employee[22] of the Agency may have violated, may be violating, or may violate a federal criminal statute, that General Counsel should within a reasonable period of time determine whether there is a reasonable basis[23] to believe that a federal crime has been, is being, or will be committed and that it is a crime which, under this memorandum, must be reported.[24]

157. In **[the]** MFR of the OPS Legal Advisor of January 7, 1997, he wrote that another issue discussed was:

> The need to determine whether a crimes report will be required after an assessment of the information stored on the drives and the PCMCIA cards. [18 U.S.C. §§1924 and 793(f) were briefly discussed.] The General Counsel will make any determination in that regard.

158. The OPS Legal Advisor stated that he understood that Deutch had placed classified information on unclassified CIA computers that were connected to the Internet, and the classified information only "came out of Deutch's head" when he composed documents on the computer. The OPS Legal Advisor said he did not know or have any information that Deutch had removed documents from controlled areas containing classified information.[25]

159. The OPS Legal Advisor remembered discussing the issue of the possible criminality of Deutch's actions with the PDGC. His position was more conservative than the PDGC's. She raised the point that, as DCI, Deutch had the legal authority to declassify material under his control. This led to her contention that Deutch

---

[22]According to paragraph II B. 1. of the MOU, an "employee" is defined as "a staff employee, contract employee, asset, or other person or entity providing service to or acting on behalf of any agency within the intelligence community."

[23]According to paragraph II E. of the MOU, "'Reasonable basis' exists when there are facts and circumstances, either personally known or of which knowledge is acquired from a source believed to be reasonably trustworthy, that would cause a person of reasonable caution to believe that a crime has been, is being, or will be committed."

[24]Records of the Office of General Counsel indicate there were an average of 200 written crimes reports submitted to DoJ each year for the period 1995-1998.

[25]Title 18 U.S.C. §§793(f) and 1924 both prohibit the improper removal of "documents."

could not be prosecuted for a security violation. She reportedly cited an instance when then-DCI William Casey inadvertently divulged classified information in an interview with the media.

160. The OPS Legal Advisor provided handwritten notes from January 6, 1997 about a discussion of a possible crimes report with the PDGC:

> Talked to [the PDGC]. She already knew about the Deutch leak. Discussed the 793(f) issue. She concluded years ago that the DCI who has authority to declassify cannot realistically be punished under the statute. I expressed my disbelief in that analysis. Hypo - does that put the DCI beyond espionage statutes? No she says that would be a natl. security call . . . . Returned briefly to information in play. Discussed how there may have been **[non-CIA controlled compartmented program material]** on the computer. Doesn't this push 793(f) back into play?

161. In his OIG interview, the OPS Legal Advisor said that DoD material and Top Secret/**[the non-CIA controlled compartmented program]** material would not qualify for information a DCI had the authority to declassify. He realized that a referral to the FBI would "technically not" be the same as making a crimes report to DoJ. He stated there was a tendency to discuss some cases with the FBI in order to get their procedural advice.

162. The OPS Legal Advisor had a discussion with an FBI agent then assigned to the Counterespionage Group, Counterintelligence Center (CIC), regarding the possible applicability of Title 18 U.S.C. §§793(f) and 1924 in the matter regarding Deutch. The OPS Legal Advisor recalled this FBI Agent believing that there had to be a physical removal of documents to constitute a violation of the statutes.

163. A two-page handwritten note of January 24, 1997, composed by the OPS Legal Advisor, reported his discussion

with the FBI Agent regarding the case. The note indicated that the FBI Agent at CIC suggested that it was better to have O'Neil call the then-FBI General Counsel to discuss the case.

164. The OPS Legal Advisor provided an MFR reporting a January 28, 1997 meeting with the PDGC and O'Neil to discuss the Deutch case. At that time, O'Neil indicated he anticipated calling the FBI General Counsel to tell him CIA intended to conduct an investigation of this matter unless the FBI General Counsel wanted the FBI to assert investigative authority.

165. According to O'Neil, neither he nor anyone else suggested a crimes report be filed on the Deutch matter. O'Neil said a crimes report can be made at several points during an investigation. He pointed out that, in a number of cases, CIA conducts its own investigation. Matters could also be referred to DoJ to conduct an investigation.

166. O'Neil is not certain whether he talked to the FBI agent at CIC about the Deutch matter. O'Neil has a vague recollection he called the FBI General Counsel and asked him how CIA should proceed. O'Neil described the case to the FBI General Counsel, who said that the CIA should continue its own process of looking at the matter. O'Neil believes he wrote an MFR documenting his conversation and may have given the MFR to his secretary to keep in a personal folder used for sensitive matters.[26]

167. The FBI Agent at CIC recalled that he was told Deutch had classified information on a computer disk at his home in Maryland shortly after the matter was discovered. The FBI Agent was asked if the matter was an "811" violation.[27] The FBI Agent concluded there was no reason to believe that the information had been compromised to a foreign power and, therefore, the FBI did

[26]A check of O'Neil's "sensitive personal file" was conducted by his secretary's successor in OGC. There was no evidence of any document regarding contact between O'Neil and the FBI General Counsel concerning a possible crimes report on Deutch.

[27]"811" is Section 811 of the Counterintelligence and Security Enhancement Act of 1994.

not need to get involved. The FBI Agent recalled telling someone at CIA, whose identity he does not remember, that since Deutch was involved, O'Neil may want to contact the FBI General Counsel, O'Neil's counterpart at FBI. The FBI Agent said that he established early on in his tenure at CIA that merely telling him something did not constitute official notification of the FBI much less DoJ. He was aware that OGC had crimes reporting responsibilities, and he expected them to fulfill those responsibilities.

168. The FBI General Counsel recalled a single telephone call from O'Neil after Deutch left CIA, between February and April 1997. At that time, O'Neil told the FBI General Counsel an issue had arisen about classified information existing on some computer disks at Deutch's home. The FBI General Counsel recalled they discussed CIA reporting requirements to the FBI under "811." **[He]** believes he would have told O'Neil that not enough was known about the matter at the time. If an "811" problem surfaced after CIA had looked into the matter, CIA should refer the problem to the FBI through official CIA channels.

169. The FBI General Counsel stated that he did not consider O'Neil's call as a submission of a crimes report because, from what he remembers being told, there was no evidence of a crime. He said that he and O'Neil spoke on the telephone several times a week, but O'Neil never made a crimes report to him. **[He]** said that if he thought O'Neil was giving him a crimes report, he would have told him to do it through the proper channel.

170. Calder said that if a referral should have been made to DoJ and was not, he believes the omission was not intentional. However, Calder stated the responsibility for a crimes report was O'Neil's. Calder added that "I have never issued a crimes report and would always raise such an issue with OGC for their action." Calder said the FBI General Counsel had informed O'Neil that DoJ would not pursue a Deutch investigation regarding misuse of the computer.

171. The PDGC had supervisory responsibility of the Litigation Division which had the crimes reporting account in OGC at that time.[28] The PDGC stated she did not have a lot of hands-on experience with the mechanics of coordinating crimes reports and had never authored a crimes report. She first learned of the discovery of classified information, including Top Secret / **[a non-CIA controlled compartmented program]** material, on a computer in Deutch's Maryland residence on the day of its discovery in December 1996. She remembered hearing about information regarding a covert action with **[two countries]** but does not recall hearing there was **[codeword]** or **[a different codeword]** information on the computer. She did not learn that the computer at his Belmont residence also contained classified information.

172. The PDGC was not aware that Deutch was deleting files from the Maryland computer in the days immediately following the discovery of the classified information. She remembered speaking with Calder about the necessity of protecting the magnetic media. Her reason for wanting to retain the magnetic media was not for evidence of a crime but to have a record should there be a need to conduct a leak investigation in the future.

173. When considering the need for a crimes report, the PDGC said she did not examine the "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes." She did not consult with any attorneys from the Internal Security Section of DoJ or with the United States Attorneys Office. She does not remember reviewing Title 18 U.S.C. §793(f), "Gathering, transmitting or losing defense information." She spoke with O'Neil's Executive Assistant[29] regarding the provisions

---

[28]The PDGC has served in the CIA since 1982. **[She]** was appointed PDGC, the second highest position in the Office of General Counsel, in the summer of 1995 and served in that capacity until March 1, 1999. While serving as PDGC, **[she]** also served as Acting General Counsel from the August 11, 1997 until November 10, 1997.

[29]The then-Executive Assistant to the GC states he was aware of the inquiry regarding the classified information found on Deutch's computer and that it was being worked by others in OGC.

of Title 18 and with the OPS Legal Advisor. She did not agree with the OPS Legal Advisor's assertion that, because the classified information "was [only] in his [Deutch's] head," Deutch did not remove classified information from the Agency. The PDGC was aware that, on occasion, Deutch carried the PCMCIA cards "back and forth" with him. She did not know if the cards contained classified information. The PDGC saw no distinction between classified information on a document as opposed to being on magnetic media. She explained that she was more concerned at this time with protecting and recovering the magnetic media than considering a crimes report.

174. The PDGC reviewed the statutes she thought would be relevant and did not see all the elements present for a violation. She believed that Deutch, as DCI, was the authority for the rules concerning the handling of classified information. Because Deutch issued DCIDs on classified material, she believed he could waive the rules for himself. The PDGC recognized that the DCI cannot declassify Top Secret/**[the non-CIA controlled compartmented program]** material, but said such material may be handled under the DCID rules. The PDGC stated that given the fact that this matter involved a former DCI, if she had believed a crimes report was necessary, she would have shown the draft to O'Neil and he would have had the final say as to whether a crimes report was warranted.

175. The PDGC focused on Title 18 U.S.C. §1924, "Unauthorized Removal and Retention of Classified Documents or Material." She understood that Deutch was authorized to remove classified information and take it home since he had a safe at his residence. She stated that she did not see "intent"[30] by Deutch. She reasoned that "intent" was a necessary element, "otherwise everyone [inadvertently] carrying classified information out of a

---

The Executive Assistant does not remember assisting the PDGC in this matter, but concludes that, if the PDGC states that he assisted her, he has no reason to doubt her recollection.

[30]The statute contains the pertinent phrase "and with the intent to retain such documents or materials at an unauthorized location."

CIA building would be the subject of a crimes report." According to the PDGC, Deutch had permission to take the classified material home, and Deutch's use of the PCMCIA cards was permissible within his residence. In the PDGC's view, the security violation occurred when he "did not do it right" by connecting the Internet to his computer and "leaving the card in the slot." She did not distinguish between Deutch as DCI and his actual status as an Independent Contractor when the classified information was discovered. However, she would have looked at the issue differently if she understood that the only acceptable means of safeguarding the computer would have been to remove and secure the computer's hard drive.

176. The PDGC did not remember when she made the legal decision that a crimes report was not required. She remembered speaking with C/SIB in March 1997 about his concern that a crimes report should be filed.

177. The PDGC said that D/OPS's report was not made available to her. Although someone in OGC would usually read OPS reports, the PDGC speculated that the D/OPS would not have shown the report to her without receiving authorization. She never thought to request a copy of the D/OPS's report to determine if his findings were consistent with her decision not to file a crimes report. Later, after she became Acting General Counsel, the issue of her reviewing the report never arose, and she would have expected OPS to raise the report with her only if the facts had changed significantly from what she learned initially.

178. In comparing the Deutch case to a similar case involving a senior Agency official, the PDGC asserted that the other official did not have a safe in his residence and was not authorized to take home classified information. She viewed this dissimilarity as a major distinction. Nor did he have the authority to waive the rules on the handling of classified information. The PDGC did not

remember if OGC made a crimes report on that case of mishandling classified information.[31]

179. George Tenet, who was Acting DCI at the time of the OPS/SIB investigation, said no one ever raised the issue of reporting this incident to DoJ, and it did not occur to him to do so. Tenet said no one ever came forward with a legal judgment that what had occurred was a crime. In Tenet's opinion, based upon what he knew at that time, there was no intent on Deutch's part to compromise classified information. Therefore, Tenet did not believe a crime was committed. Tenet was aware of the incident involving **[another]** senior Agency official but was not aware a crimes report had been filed on it.

SHOULD APPLICATION OF THE INDEPENDENT COUNSEL STATUTE HAVE BEEN CONSIDERED?

180. The fundamental purpose of the Independent Counsel statute is to ensure that serious allegations of unlawful conduct by certain federal executive officials are subject to review by counsel independent of any incumbent administration.

181. Title 28 U.S.C. §592, "Preliminary investigation and application for appointment of an independent counsel" cites Title 28 U.S.C. §591, "Applicability of provisions of this chapter," as the basis for those positions who are "covered persons" under the Independent Counsel statute.

182. Title 28 U.S.C. §591 (a), "Preliminary investigation with respect to certain covered persons" specifies:

> The Attorney General shall conduct a preliminary investigation in accordance with Section 592 whenever the Attorney General receives information sufficient to constitute grounds to

[31] A crimes report was made by letter to DoJ on December 13, 1996. It is signed by the AGC in the Litigation Division, who was the OGC focal point for crimes reports at that time.

> investigate whether any person described in subsection (b) may have violated any Federal criminal law other than a violation classified as a Class B or C misdemeanor or an infraction.[32]

183. Title 28 U.S.C. §591 (b), "Persons to whom subsection (a) applies" lists:

> . . . the Director of Central Intelligence [and] the Deputy Director of Central Intelligence . . . . [33]

184. Title 28 U.S.C. §591 (d) (1), "Examination of information to determine need for preliminary investigation," "factors to be considered" specifies:

> In determining . . . whether grounds to investigate exist, the Attorney General shall consider only—(A) the specificity of the information received; and (B) the credibility of the source of the information.

185. The Deputy Chief, Public Integrity Section, Criminal Division, DoJ, is responsible for the preliminary review of matters referred to DoJ under the provisions of the Independent Counsel statute. **[She]** explained that the provisions of the Independent Counsel statute require DoJ to review an allegation regarding a "covered person" to determine the need for preliminary investigation based only on the two factors listed above.

186. The Deputy Chief of the Public Integrity Section explained that after the CIA IG referral in March 1998, the Public Integrity Section reviewed the matter and described it in a memorandum to the Attorney General. The memorandum stated that the allegations of illegal behavior regarding former DCI Deutch were received more than one year after Deutch left office.

---

[32]Title 18 U.S.C. §793(f) and Title 18 U.S.C. §798 are felonies; Title 18 U.S.C. §1924 is a Class A misdemeanor.

[33]Title 28 U.S.C §591(b)(7) limits applicability of the statute to the term of office of the "covered person" and the one-year period after the individual leaves the office or position. This means that Deutch's potential exposure to the provisions of the Independent Counsel statute expired following the one-year anniversary of his resignation, December 14, 1997.

Accordingly, under the provisions of the Independent Counsel statute, Deutch was no longer a "covered person." The Deputy Chief of the Public Integrity Section added that the allegation should have been promptly referred to DoJ by CIA personnel.

187. The OPS Legal Advisor stated that he never considered the need to refer this matter to an Independent Counsel based on Deutch's status as a "covered person." Nor was he aware of any other discussions on this matter.

188. The PDGC stated that the issue of Deutch being a "covered person" under the Independent Counsel legislation did not arise. She said that "she never gave a thought" to the applicability of the Independent Counsel statute, and she does not know what positions within the Agency are specified as "covered persons."

189. O'Neil stated that there was no recommendation to refer the Deutch matter to DoJ under the provisions of the Independent Counsel statute.

WERE SENIOR AGENCY OFFICIALS OBLIGATED TO NOTIFY THE CONGRESSIONAL OVERSIGHT COMMITTEES OR THE INTELLIGENCE OVERSIGHT BOARD OF THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD? WERE THESE ENTITIES NOTIFIED?

190. Pursuant to the National Security Act of 1947, as amended, the President and the DCI bear statutory responsibility for keeping the two Congressional intelligence committees *fully and currently* informed of all intelligence activities.

191. Agency Regulation (AR) 7-2, "Reporting of Intelligence Activities to Congress," provides interpretation of the statutes so the Agency, with the assistance of the Office of Congressional Affairs and the Office of General Counsel, can assist the DCI in meeting the obligation to keep the intelligence committees fully and

currently informed. Under the section, "Obligation to Keep Congressional Intelligence Committees Fully and Currently Informed," one of the three categories requiring reporting are:

> Particular intelligence activities or categories of activities as to which either of the Congressional intelligence committees has expressed a continuing interest (for example, potentially serious violations of U.S. criminal law by Agency employees, sources, or contacts);

192. E.O. 12863, issued September 13, 1993, President's Foreign Intelligence Advisory Board, specifies:

> The heads of departments and agencies of the Intelligence Community, to the extent permitted by law, shall provide the Intelligence Oversight Board (IOB)[34] with all information that the IOB deems necessary to carry out its responsibilities. Inspectors General and General Counsel of the Intelligence Community, to the extent permitted by law, shall report to the IOB, at least on a quarterly basis and from time to time as necessary or appropriate, concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

193. According to the Director of the CIA's Office of Congressional Affairs (OCA), OCA is responsible for notifications to Congress and should be informed of any formal Agency investigations. OCA receives notifications from a variety of Agency components. During Slatkin's tenure, all formal written Congressional notifications were to be routed through her office. The Director of OCA was unaware of SIB's investigation into the discovery of classified information on Deutch's government-issued unclassified computer.

194. At the January 6, 1997 meeting to discuss the planned investigation of the finding of classified information on Deutch's

[34]The Intelligence Oversight Board is a standing committee of the President's Foreign Intelligence Advisory Board.

unclassified CIA computer, the OPS Legal Advisor stated that the Congressional oversight committees may eventually inquire about this matter. He recalled that Calder wanted the investigation performed "by the book" in case there would be a need to account for SIB actions.

195. Calder assumed this matter would again arise in the future, possibly through a leak, with a Congressional committee. He recalled a discussion about doing briefings and was left with the impression that there was a briefing of the "Group of Four" Congressional oversight committees.[35]

196. C/SIB maintained a chronology of the investigation consistent with Calder's instructions. He also advised Calder, the former ADDA, the PDGC, and the D/OPS on at least two occasions that Congress, along with DoD, should be informed about the material found on Deutch's unclassified computer. After receiving a copy of the D/OPS's report on the investigation, C/SIB realized the report did not contain a recommendation that Congress be notified.

197. The PDGC stated she did not remember any discussion concerning notifying the Congressional oversight committees or the IOB. O'Neil said that "the question of informing the IOB or the Congressional oversight committees did not come up."

198. Slatkin stated she could not recall any discussion or recommendation regarding the need to notify the Congressional committees about the Deutch matter. In her interview with OIG, she stated that, "surely, yes, the Committees should have been notified—but at what point?"

[35]The Group of Four refers to the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, and the two appropriations committees—the Senate Appropriations Committee, Subcommittee on Defense and the House Appropriations Committee, National Security Subcommittee.

199. The IOB was officially notified of OIG's investigation on May 8, 1998. After being informed of the OIG investigation, the Director of Congressional Affairs prepared talking points, which DCI Tenet presented to the SSCI and HPSCI in early June 1998.

WHY WAS NO ADMINISTRATIVE SANCTION IMPOSED ON DEUTCH?

200. Deutch was aware that an inquiry was conducted after classified information was discovered on his government-issued computers configured for unclassified use. He said that he never tried to influence the outcome of the investigation. Nor was he told the outcome, although he had requested that someone apprise him of the results.

201. Calder said that, despite the pressure that accompanied the investigation of a DCI, he and OPS did "the right thing." Calder said that since Deutch was no longer a CIA employee, there was no punishment that could be administered to him. The issue was what position the Agency should take if Deutch needed access to classified information in the future. Calder was aware that Deutch's computers had been replaced with totally unclassified magnetic media. Calder said that while Deutch was on several governmental committees, he did not believe that Deutch had a need for classified information in those positions. Calder said the remedy was to counsel Deutch in a discrete manner that would not offend his ego so he would understand the gravity of what had happened. Calder was aware that Slatkin had spoken with Deutch about the issue, and, from those conversations, Deutch would have recognized that his actions were wrong. Calder stated it was his responsibility to counsel Deutch and he planned to do so when Deutch received a briefing regarding future access. However, Calder said he never had the opportunity to meet with Deutch under the conditions he desired.

202. The former ADDA stated that she was "worn down" by Slatkin and O'Neil, and perceived that the D/OPS and Calder were

similarly affected. Additionally, Calder was "frustrated" because Slatkin would not resolve issues presented to her but, instead, provided more tasking. The former ADDA said that she, the D/OPS, and Calder had reached a point where they could not go any further in that there was no additional merit in further evaluating the collected data. Slatkin had "emotional attachments" and O'Neil was not considered to be objective. According to the former ADDA, Slatkin's and O'Neil's oversight of the investigation was colored by a distrust of OPS and an interest to protect Deutch's privacy. The former ADDA said that she and SIB investigators perceived Slatkin's and O'Neil's behavior as "stonewalling." The former ADDA and SIB investigators also viewed Slatkin's requests for repeated clarifications, while typical of her management style, as a form of "pressure" to wear down the others until they were ultimately in agreement with her and O'Neil.

203. The PDGC said that there was not a "crisp end" to the case; "it ran out of steam" when many of the principals left the Agency. The PDGC thought a decision was made that the Director of the Center for CIA Security or the D/OPS would brief either Deutch or the whole Proliferation Commission regarding safeguarding classified information, but she does not know if this action was taken. O'Neil stated that after the process for producing the review was approved by the ADCI, who had been kept informed all long, he had little to do with the investigation. O'Neil also stated, he did not interfere with the OPS investigation, he left the Agency in July 1997,[36] and he does not know how the investigation was concluded. Slatkin said that she gave the information to Tenet and assumed that the investigation would have proceeded after she departed the Agency. The D/OPS said that, as far as he knows, no decision was ever made on what to do concerning Deutch's actions.

204. Tenet did not recall how the matter was resolved. He believes Calder, the D/OPS, Slatkin, and O'Neil had detailed

[36]Although O'Neil states he left the Agency in July 1997, he was present for duty until August 11, 1997 when he was replaced by the PDGC as Acting General Counsel.

discussions on the matter. Tenet was aware of concerns for Deutch's privacy. According to Tenet no one ever raised the issue of reporting the incident to the Department of Justice, or whether Deutch's clearance should be affected.

WHAT WAS OIG'S INVOLVEMENT IN THIS CASE?

- **When did OIG first learn of this incident?**

205. The former C/DCI Administration spoke with then-IG Frederick Hitz on December 18, 1996[37] regarding what was found at Deutch's residence. The former C/DCI Administration described conversations he had with O'Neil and Slatkin about the matter, and O'Neil's assertion that the former C/DCI Administration was responsible for allowing Deutch to improperly process classified information. Hitz instructed the former C/DCI Administration to provide the IG with copies of any documentation,[38] encouraged the former C/DCI Administration to brief Tenet as soon as possible, and suggested that the former C/DCI Administration stay in contact with the IG.

206. According to the former C/DCI Administration's MFR of December 30, 1996, the IG Counsel contacted him on December 19, 1996. Reportedly, the IG Counsel urged the former C/DCI Administration to prepare an MFR and provide related documentation to the IG.

207. On December 20, 1996, Hitz called the former C/DCI Administration to inform him that he had met with Tenet, who was reportedly not aware of the Deutch matter. Hitz indicated that he and Tenet both supported the process that was being pursued on the acquisition of relevant information and the classified magnetic media. Hitz encouraged the former C/DCI Administration to ensure that his documentation was forwarded to Hitz's staff for the former C/DCI Administration's protection.

---

[37] Hitz served as CIA IG from October 12, 1990 until April 30, 1998, when he retired.

[38] The former C/DCI Administration provided a copy of his MFR to Hitz, Calder, and C/SIB.

208. Hitz remembers that in mid-December 1996, the former C/DCI Administration met with him regarding classified information discovered on one or two Agency-owned computers at Deutch's residences in Maryland and Belmont. Hitz recalled the former C/DCI Administration seeking advice on what action to take. Hitz's impression was that C/DCI Administration was concerned that the former C/DCI Administration's supervisors would not act appropriately. Hitz understood that the classified information found on Deutch's computer included sensitive trip reports. The computer was connected to the Internet, and there was **[a]** threat of the information being vulnerable to electronic compromise.

209. Hitz believes that he discussed the former C/DCI Administration's information with IG Counsel and the then-Deputy IG for Investigations and obtained their advice. This advice included instructing the former C/DCI Administration to secure the hard drive and other classified information that was recovered from Deutch's computers. Hitz remembered passing that instruction to the former C/DCI Administration. Hitz recalled that after meeting with IG Counsel and then-Deputy IG for Investigations, "we knew we were going to get into it and be helpful with it."

210. Hitz stated that he cannot remember what follow-up instruction he may have provided to IG Counsel and then-Deputy IG for Investigations. Hitz thinks he ultimately read the former C/DCI Administration's MFR and "did not like the smell of it" [the nature of the allegation] and "if half of what the former C/DCI Administration said was true - we would get in it." Hitz emphasized that the determination of whether to get involved would be made in concert with IG Counsel and the then-Deputy IG for Investigations. Hitz stated he never discussed the SIB investigation with Deutch, Slatkin, O'Neil, Calder, the PDGC, or D/OPS.

211. IG Counsel said that he does not remember any discussions that Hitz may have had with him and the then-Deputy IG for Investigations stemming from information received from the former C/DCI Administration. The IG Counsel stated that he does not remember calling the former C/DCI Administration or having any discussion of an allegation regarding Deutch, nor does he remember seeing an MFR by the former C/DCI Administration.[39]

212. The then-Deputy IG for Investigations said there were contacts between the former C/DCI Administration and Hitz over this issue, and Hitz would tell the then-Deputy IG for Investigations about the conversations afterwards. The then-Deputy IG for Investigations stated he "may have detected an inference from Hitz that classified information was on the computer." However, the then-Deputy IG for Investigations did not remember any discussion with Hitz regarding the need to protect the computer's hard drive. The then-Deputy IG for Investigations was not in contact with the former C/DCI Administration.

- **Why did OIG wait until March 1998 to open an investigation?**

213. Hitz observed that the investigation had started with the former C/DCI Administration's "security people" finding the data, and the investigation stayed in a security channel. Hitz believed that it was appropriate for that to continue as long as OPS would be allowed to do their job.

214. C/SIB's chronology noted a call from the then-Deputy IG for Investigations on January 7, 1997 asking that SIB look at a particular issue, normally the purview of the OIG (improper personal use of a government computer) to put some preliminary perspective to the issue and keep him apprised.

---

[39] A review of Hitz's files, which he left when he retired, failed to locate **[the]** MFR of the former C/DCI Administration or any notes or correspondence connected with this investigation.

215. The then-Deputy IG for Investigations stated that he must have learned from Hitz that C/SIB was involved with an investigation related to Deutch and that knowledge prompted the then-Deputy IG for Investigations to call C/SIB on January 7, 1997. The then-Deputy IG for Investigations said that, if he had been informed that the matter under investigation by C/SIB was a "serious issue," he would remember it. The then-Deputy IG for Investigations categorized the issue under investigation by SIB as one of "propriety and property management." He does not recall knowing that the computers involved were intended for unclassified use.

216. The OPS Legal Advisor stated he learned from Calder that on January 5, 1997, Hitz was briefed on the incident involving Deutch. Reportedly, Calder stated that Hitz believed that the incident was a security issue and not one for the IG. After learning of Deutch's possible appointment to the Office of Science and Technology Policy, on May 16, 1997, [the OPS Legal Advisor] wrote in an MFR that he met briefly with Hitz to discuss Deutch's possible appointment and

> Fred [Hitz] said he would speak to the DCI about this matter, and sensitize him to the problems associated with [Deutch's] needing a clearance at another U.S.G. agency. Fred asked to be kept informed.[40]

217. According to C/SIB, he contacted OIG to define OIG interests before the D/OPS began his review of the recovered documents. C/SIB met with the then-Deputy IG for Investigations, the IG Counsel, and the then-Deputy Associate IG for Investigations. C/SIB advised them that any difficulties he encountered to date were within his ability to resolve. In his chronology, C/SIB writes:

> C/SIB met with [the then-Deputy IG for Investigations, the Deputy Associate IG for Investigations and the IG Counsel] re

[40] Hitz corroborates the OPS Legal Advisor's account of this meeting.

> "reporting threshold" to OIG for USG Computer Misuse, both in this case in particular, and in other cases, in general. This meeting was imperative in order for C/SIB to know before the "security" review [being conducted by **[the]** D/OPS] what would vice would not be OIG reportable. Upon discussion, it was determined that the OIG would avail great latitude to SIB re such reporting, noting that only in instances wherein the use of the computer was obviously criminal in nature, a conflict of interests [*sic*] existed, an outside business was being conducted, or a private billing reimbursement for "personal entertainment" was in evidence, would the OIG require a report be submitted by SIB. (C/SIB so advised D/OPS). No particulars[41] were discussed relative to SIB's ongoing investigation, nor were any requested.

218. The then-Deputy IG for Investigations remembers the February 21, 1997 meeting with C/SIB in the presence of the Deputy Associate IG for Investigations, and possibly the IG Counsel. Up to that point, OIG had lost track of the allegation against Deutch. The then-Deputy IG for Investigations stated he told C/SIB about OIG's jurisdictional interests in terms of the computer. The then-Deputy IG for Investigations said it is possible that C/SIB made some comment about encountering some difficulty in the investigation but was working through the problem and appeared self-confident about his capability to investigate the matter. The then-Deputy IG for Investigations sensed that C/SIB was being "squeezed by unspecified OPS officials."

219. The then-Deputy IG for Investigations remembered C/SIB agreeing that he should re-contact OIG if he encountered any matter of IG interest, such as evidence of misuse of an official computer, during his investigation. According to the then-Deputy IG for Investigations, "there was no zest" on the part of OIG to take it over while OPS was working the issue. The then-Deputy IG for

[41] C/SIB later explains his use of the word "particulars" meant that he did not disclose what evidence had been discovered in his investigation. He states that it does not necessarily mean that Deutch's name and/or title was not discussed.

Investigations does not recall knowing at the time that the OPS/SIB investigation involved classified information.

220. On February 6, 1998, the Deputy Associate IG for Investigations met with C/SIB on an unrelated investigation. C/SIB incorrectly assumed the Deputy Associate IG for Investigations was investigating Deutch's mishandling of classified information on a computer at his residence. According to the Deputy Associate IG for Investigations, C/SIB disclosed that he was unable to fully pursue his investigation because of a problem with Slatkin and O'Neil. C/SIB was frustrated because there had been no interview of Deutch, a customary part of an SIB investigation.

221. During this meeting, the Deputy Associate IG for Investigations reviewed a number of documents that included an unsigned report prepared by the D/OPS. This report detailed the D/OPS review of data discovered on the Deutch's magnetic media. The Deputy Associate IG for Investigations, subsequently met with the then-Deputy IG for Investigations, and told him what he had learned from C/SIB.

222. In his OIG interview, the then-Deputy IG for Investigations explained that OIG opened an investigation because SIB's investigation was impeded or "shutdown," and a crimes report was never sent to DoJ.

223. Hitz explained that a security violation of this nature would not normally be a matter investigated by OIG.[42] He stated that as the IG, he would have been inclined to assert investigative authority only when he believed that the normal management response was inappropriate or not helpful. He recognized that

[42]On February 5, 1997, Hitz sent a memorandum to the Director of Personnel Security, Subject: "Crimes Reporting and Other Referrals by Office of Personnel Security to the Office of Inspector General." The memorandum eliminated the requirement for OPS to routinely notify OIG of certain specific investigative matters in which it is engaged. Included as one of the nine categories of investigative issues identified in the memorandum was the following: "Mishandling of classified information that is or could be a possible violation of 18 U.S.C. 1924, 'Unauthorized removal and retention of classified documents or material.'"

Deutch appointees Slatkin and O'Neil were involved in the review process. Hitz stated that it was the responsibility of OIG "to support the institution."

- **What steps were taken by OIG after opening its investigation?**

224. IG Counsel remembered advising the Deputy Associate IG for Investigations that the allegation had to be referred to DoJ as a possible crimes report. The IG Counsel also remembers a discussion about the relevance of the Independent Counsel statute since Deutch was a "covered person."

225. On March 19, 1998, OIG referred the allegations to DoJ. The crimes report letter noted that at the time of the alleged violations, Deutch was a "covered person" under the Independent Counsel statute. DoJ advised they would review the allegations for applicability to the Independent Counsel statute and further OIG investigation was not authorized until completion of DoJ's review. In May 1998, DoJ informed OIG that the Independent Counsel statute would not apply because DoJ was not notified of the alleged violations until more than one year after Deutch left his position. As such, Deutch's status as a "covered person" had expired.

226. On May 8, 1998, OIG informed the Chairman of the Intelligence Oversight Board by letter of the criminal investigation of Deutch pursuant to E.O. 12863.

227. On June 2 and 3, 1998, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were notified by DCI Tenet that the OIG was conducting an investigation of former DCI Deutch and the manner in which the matter was originally handled by CIA officials.

WHAT IS DEUTCH'S CURRENT STATUS WITH THE CIA?

228. Deutch's no-fee, December 1996 consulting contract was renewed in January 1998 and December 1998. The latest renewal covers the period December 16, 1998 until December 15, 1999. This contract provides Deutch with staff-like access to the Agency, its computer system, and a Top Secret clearance. Deutch's contract for the Proliferation Commission will expire when the commission finishes its work. That contract does not contain any information regarding access to classified information.

WHAT WAS THE DISPOSITION OF OIG'S CRIMES REPORT TO THE DEPARTMENT OF JUSTICE?

229. On April 14, 1999, Attorney General Janet Reno sent a letter to DCI Tenet **[declining prosecution.] [The letter stated in part:]**

> The results of that [OIG] investigation have been reviewed for prosecutive merit and that prosecution has been declined. As I understand that Mr. Deutch currently holds a Top Secret security clearance, I suggest that the appropriate security officials at the Central Intelligence Agency review the results of this investigation to determine Mr. Deutch's continued suitability for access to national security information.

CONCLUSIONS

230. Former DCI John Deutch was specifically informed that he was not authorized to process classified information on government computers configured for unclassified use.

231. Throughout his tenure as DCI, Deutch intentionally processed on those computers large volumes of highly classified information to include Top Secret Codeword material.

232. Because Deutch's computers configured for unclassified use had connections to the Internet, all classified information on

those computers was at risk of compromise. Whether any of the information was stolen or compromised remains unknown.

233. On August 1, 1995, Deutch was made aware that computers with Internet connectivity were vulnerable to attack. Despite this knowledge, Deutch continued his practice of processing highly classified material on unclassified computers connected to the Internet.

234. Information developed during this investigation supports the conclusion that Deutch knew classified information remained on the hard drives of his computers even after he saved text to external storage devices and deleted the information.

235. Deutch misused U.S. Government computers by making extensive personal use of them. Further, he took no steps to restrict unauthorized persons from using government computers located at his residences.

236. The normal process for determining Deutch's continued suitability for access to classified information, to include placing the results of the SIB investigation in Deutch's security file, was not followed in this case, and no alternative process was utilized. The standards that the Agency applies to other employees' and contractors' ability to access classified information were not applied in this case.

237. Because there was a reasonable basis to believe that Deutch's mishandling of classified information violated the standards prescribed by the applicable crimes reporting statute, Executive Order and Memorandum of Understanding, OGC officials Michael O'Neil and the PDGC should have submitted a crimes report to the Department of Justice.

238. The actions of former Executive Director Nora Slatkin and former General Counsel Michael O'Neil had the effect of delaying a prompt and thorough investigation of this matter.

239. DDA Richard Calder should have ensured the completion of a more thorough investigation, in particular, by arranging for an interview of Deutch and a subsequent documentation of that interview in accordance with established Agency procedures. Calder should also have ensured that the matter was brought to a conclusion rather than permitting it to languish unresolved.

240. Former Inspector General Frederick Hitz should have involved himself more forcefully to ascertain whether the Deutch matter raised issues for the Office of the Inspector General as well as to ensure the timely and definitive resolution of the matter.

241. DCI George Tenet should have involved himself more forcefully to ensure a proper resolution of this matter.

242. The application of the Independent Counsel statute was not adequately considered by CIA officials and, given the failure to report to DoJ on a timely basis, this in effect avoided the potential application of the statute.

243. The Congressional oversight committees and the Intelligence Oversight Board should have been promptly notified of Deutch's improper handling of classified information.

Daniel S. Seikaly

RECOMMENDATIONS

1. John Deutch's continued suitability for access to classified information should be reviewed immediately.

2. The accountability of current and former Agency officials, including Deutch, for their actions and performance in connection with this matter should be determined by an appropriate panel.

3. All appropriate Agency and Intelligence Community components should be informed in writing of the sensitive information Deutch stored in his unclassified computers so that responsible authorities can take any actions that would minimize damage from possible compromise of those materials.

CONCUR:

L. Britt Snider — Date
Inspector General

EXHIBIT 11

DEPARTMENT OF DEFENSE
OFFICE OF THE INSPECTOR GENERAL

REPORT OF INVESTIGATION

AUG 28 2000

ALLEGATIONS OF BREACHES OF SECURITY: DR. JOHN M. DEUTCH, FORMER DEPUTY SECRETARY OF DEFENSE AND FORMER UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND TECHNOLOGY

ALLEGATIONS OF BREACHES OF SECURITY BY DR. JOHN M. DEUTCH, FORMER DEPUTY SECRETARY OF DEFENSE AND FORMER UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND TECHNOLOGY

I. INTRODUCTION

On February 9, 2000, the Secretary of Defense requested the Deputy Inspector General and the Acting General Counsel, Department of Defense (DoD), conduct a review of material obtained by the Office of Inspector General, Central Intelligence Agency (OIG, CIA), during its investigation into allegations of breaches of security by Dr. John M. Deutch. Specifically, the Secretary of Defense requested that we review a journal that Dr. Deutch maintained on a computer while he served as the Under Secretary of Defense (Acquisition and Technology) (USD(A&T)), the Deputy Secretary of Defense (DEPSECDEF) and the Director, Central Intelligence (DCI). The Secretary of Defense also requested that we obtain from the CIA any other information or documents relating to potential matters of concern to the DoD.

Subsequently, the former DEPSECDEF, Dr. John Hamre directed the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)) to conduct a damage assessment of Dr. Deutch's journal as well as of any other potentially classified material maintained by Dr. Deutch on unclassified computers or computer media during his tenure with the DoD. A complete analysis of that information and final damage assessment will be reported by the ASD(C3I).[1]

[1] During the course of our inquiry, the President's Foreign Intelligence and Advisory Board (PFIAB) and the Department of Justice (DOJ) also initiated separate inquiries into the actions of Dr. Deutch. Upon request, the Deputy Inspector General, DoD, briefed the PFIAB on two occasions concerning the scope of our inquiry and provided preliminary findings. In May 2000, the PFIAB completed their work and provided their report to the President. The review by the DOJ is not yet complete.

With the concurrence of the Acting General Counsel, DoD, the scope of the OIG, DoD, review was to:

- determine the disposition of computers used by Dr. Deutch during his tenure as the USD(A&T) and as the DEPSECDEF;
- determine what information Dr. Deutch stored on computers while he served as the USD(A&T) and the DEPSECDEF; and,
- recover all information and documents relating to potential matters of concern to the DoD.

As initially reported by the CIA IG, during the period that Dr. Deutch served as the USD(A&T) and as the DEPSECDEF, he routinely entered data on Government-owned computers, at his office and home not designated to process classified information. In particular, Dr. Deutch maintained a daily journal containing classified information that was almost 1,000 pages in length, on computer memory cards, that he reportedly transported in his shirt pocket. In addition, the OIG, CIA, determined that Dr. Deutch and members of his family acccessed his America Online (AOL) account using the same Government-owned computers at his home that he used to process his journal. Dr. Deutch's practice of using computers in this manner was extremely risky in that a computer "hacker" could have gained on-line access to Dr. Deutch's computer and the information stored in temporary files on the hard drive, including the journal.

We find his conduct in this regard particularly egregious in light of existing DoD policy directives addressing the safeguarding of classified information. This situation was exacerbated because Dr. Deutch, while serving as the DEPSECDEF, declined departmental requests that he allow security systems to be installed in his residence. Dr. Deutch, the second highest-ranking individual in the Department, personally addressed the need to properly safeguard information in a memorandum he signed in February 1995. In part, the memorandum states that only "properly reviewed and cleared" information be placed on electronic systems accessible to the public. The evidence we obtained clearly establishes that Dr. Deutch failed to follow even the most basic security precautions.

There are also several other concerns that warrant comment. For example, accurate property accountability practices and procedures for the disposition of computers were lacking within the Office of the Secretary of Defense (OSD). During our inquiry we identified computers that Dr. Deutch used or could have used during his time with the Department. Several of the computers that we recovered contained a significant amount of DoD information. These computers were either donated or sold to private entities through the reutilization process. Security personnel at the ASD(C3I) have determined that none of the information remaining on the hard drives of these computers was classified. This determination, however, does not negate the Department's potential exposure to the improper release and use of classified or sensitive information. Several witnesses told us that they believed that the Department had an existing policy which required that the hard drives used to process classified information must be removed from the computer and destroyed. However, the witnesses were not able to produce and we were unable to document such a policy. Current policy on what is required to dispose of these types of hard drives is not clear. We recommend that the Department implement policy that requires the destruction of all computer hard drives, classified and unclassified, before the computer is disposed of outside the DoD.

II. SUMMARY

Although poor property accountability practices within OSD hindered our investigation, we were able to identify the computers used by Dr. Deutch. Specifically, we found that during his tenure as the USD(A&T) and DEPSECDEF, Dr. Deutch used at least seven different Government-owned computers, all of which were Macintosh. He used a Quadra 800, two Quadra 650s, a Power PC 7100 and three Powerbook laptops: a 180, a 180c, and a 540c. We believe the Quadra 800 and the 180 laptop were later sent to the Defense Reutilization and Marketing Office (DRMO), for destruction as scrap. Our review indicates that after he left the DoD one of the Quadra 650s was reissued and eventually excessed and sent to the DRMO. We could not determine the final disposition of the other Quadra 650. There are indications however, the CIA may have recovered it from Dr. Deutch's residence in **[deleted]** in 1995. The Power PC 7100 was transferred to the CIA when Dr. Deutch became the DCI. The 180c and 540c Powerbook laptops were eventually excessed by the DoD and transferred to Florida A&M University as part of the Educational Institutions Partnership Program. We recovered both of these laptops from Florida A&M and sent them to the National Security Agency (NSA) and the Defense Computer Forensics Laboratory (DCFL) for data recovery.

We also found that during Dr. Deutch's tenure with the Department his email, including "dial-in" access, was processed by a Macintosh Quadra 800 and backed-up by a Macintosh 8150. When Dr. Deutch left his position as the DEPSECDEF to become the DCI, personnel at the CIA made arrangements with DoD personnel which allowed Dr. Deutch to obtain "dial-in" access to the OSD electronic mail (email) server which he used from May 10, 1995, until January 27, 1996. Media analysis of the hard drive of the backup server resulted in the recovery of 1,089 pages of email. Personnel from the ASD(C3I) have determined that none of the emails contained classified information. A description of the DoD computers that were issued to Dr. Deutch during his tenure as the USD(A&T) and as the DEPSECDEF and the disposition of those computers is attached.

III. BACKGROUND

Dr. Deutch served as the USD(A&T) from April 2, 1993, to March 11, 1994, at which time he became the DEPSECDEF. He served in that capacity until May 10, 1995, when he became the DCI, a position he held until December 16, 1996. While in the USD(A&T) position, Dr. Deutch received computer support from USD(A&T) Executive Support, Information Technology Branch (ITB). Contractor personnel from Advanced Systems Development, Incorporated of Shirlington, Virginia, augmented the permanent ITB staff. **[Deleted]** was an employee of this firm and a key witness in this matter. **[Deleted]** provided support to Dr. Deutch while he was the USD(A&T) and, on occasion, after Dr. Deutch became the DEPSECDEF. In June 1995, **[deleted]** became a member of a computer support group at the CIA and continued to provide computer support to Dr. Deutch.

IV. SCOPE

During our inquiry, Special Agents of the Defense Criminal Investigative Service (DCIS), the criminal investigative arm of this office, interviewed several former and current OSD employees and DoD contractors that we believed were knowledgeable of Dr. Deutch's use of computers while with the DoD. We attempted to interview Dr. Deutch during the course of our review, however, based on the advice of his counsel, he declined. The DCIS Special Agents also reviewed pertinent procurement and

other inventory records at the Washington Headquarters Services (WHS), the DRMO, the Defense Supply Service-Washington (DSS-W), and the Defense Information Systems Agency (DISA).

We conducted extensive coordination with the OIG, CIA, and the ASD(C3I) to ensure that all documents relating to potential matters of concern to the DoD, including Dr. Deutch's journal, were reviewed. We also coordinated with the NSA and the DCFL to facilitate analysis of the recovered computers we believe Dr. Deutch used while he served as the USD(A&T) and DEPSECDEF.

While conducting our fieldwork we recognized that our findings, to a large extent, would be based primarily on the recollection of witnesses about property transfers that occurred five to six years earlier. In addition, some property transfer and procurement records within the OSD at the time that Dr. Deutch served as the USD(A&T) and the DEPSECDEF (1993-1995) were already destroyed when we initiated our inquiry and the few existing records were often inaccurate or incomplete.

The findings in Section V (below) provide details concerning the computers that we believe were used by Dr. Deutch. We also expended substantial investigative resources in an attempt to identify, locate, and recover other computers within the offices of the USD(A&T) and the DEPSECDEF. As a result of this investigative approach, we identified several additional computers that Dr. Deutch could reasonably have used and we recovered them accordingly for analysis.

The following sets forth the results of our inquiry:

V. FINDINGS

A. What computers did Dr. Deutch use during his tenure as the USD(A&T) and where were those computers located?

Computers that Dr. Deutch used in his USD(A&T) office

Based on witness interviews and the limited documents available, we established that on April 1, 1993, Dr. Deutch received a Macintosh Quadra 800 computer for his office use. The computer was one of two such computers (serial numbers F33080NRCC7 and XB403H0X2D6) assigned to the USD(A&T) front office. No records were retained as to the specific assignment of each computer.[2] During the course of our inquiry, we interviewed the Chief, USD(A&T) Executive Support, and three contractor personnel that were hired to provide support for Macintosh computers within USD(A&T). All of these witnesses told us that, to the best of their recollection, none of the computers in question were of the type designated to process or store classified information. Dr. Deutch used the Quadra 800 computer as a desktop workstation. The other Quadra 800 computer was used as a file server for the USD(A&T) front office.

[2] Two witnesses told us that Dr. Deutch could have received a Quadra 800, an 840 or an 840AV, but they were not positive. Several other witnesses told us that although they could not recall the exact model of the 800 series that Dr. Deutch used, they were certain it was a "tower configuration." Meaning, that the size of the computer's case was large and upright which would indicate that this computer was a Quadra 800. In addition, we found no inventory records indicating that the USD(A&T) received the 840 or the 840AV when Dr. Deutch became the USD (A&T).

In January 1994, the USD(A&T) front office began to utilize Macintosh Quadra 650 computers. During a period of about a year beginning in January 1994, USD(A&T) also received approximately 75 Macintosh Quadra 650 computers. Based primarily on witness statements, our review indicates that of the 75 computers obtained by USD(A&T), Dr. Deutch received two Quadra 650s, one for his office and one for his residence. We could not determine by serial number which of the Quadra 650s were assigned to Dr. Deutch. However, based on witness statements and documents, we believe that the most likely serial numbers were FC40606E209 and FC40006W2D9. One of the Quadra 650s replaced the Quadra 800 that Dr. Deutch had been using as a desktop workstation. That Quadra 800 computer was then reconfigured for use as a file server within USD(A&T).

We could not establish with any degree of certainty the final disposition of either Quadra 800 computer. However, inasmuch as both computers were deleted from the USD(A&T) inventory at the same time in 1998, it appears that both were sent to the DRMO for disposal. Records indicate that one of the computers was sent to the DRMO at Fort Belvoir, Virginia, and later sent to the DRMO in Williamsburg, Virginia, for final disposal. During our fieldwork, we identified a contractor, Port Royal Metals, Inc., from Sheldon, South Carolina, who was the exclusive contractor for electronic scrap disposal during the period that the Quadra 800s would have been sent to the DRMO.[3]

[3] Because Port Royal Metals, Inc., had the DRMO contract for electronic scrap, computers were initially sent to the DRMO at Fort Belvoir and then sent to the DRMO-Williamsburg for final disposal.

The contractor advised us in writing that

> "...the DRMO Williamsburg demolished any equipment we picked up prior to loading. **[Deleted]** the crane operator was most diligent in destroying any material so that it would not have any commercial use except for scrap recovery. In fact, they so destroyed the material that we complained that their destruction of material made it most difficult to process at our plant."

Computers that Dr. Deutch used in his residence during his tenure as USD(A&T)

In April 1993, Dr. Deutch was issued a Macintosh Powerbook 180 laptop computer, serial number FC325NJP796. **[Deleted]** told us that at some point before Dr. Deutch left this position he **[deleted]** inadvertently "shorted out" the computer's main board. However, because the hard drive was still functional, it was removed from the damaged computer and installed into a new Macintosh Powerbook 180c laptop, serial number FC325MYC796, that Dr. Deutch used well into his tenure as the DEPSECDEF.4 The damaged computer stayed within the USD(A&T) office until it was excessed to the DRMO on June 25, 1997.

[4] Several witnesses told us that Dr. Deutch's first laptop computer was a 180c. However, based on a combination of other witness statements and documents we believe that Dr. Deutch's first computer as the OSD(A&T) was a 180. **[Deleted]** told us that he destroyed the main board of the 180. His statement to us was corroborated by another contractor and we were able to track the 180 through disposal records. Of greater significance is that any data that was on the 180 at the time the main board was damaged would have been transferred to the 180c which we ultimately retrieved from Florida A&M University.

Documents and witness statements established that Dr. Deutch used the 180c laptop computer until approximately August 1994, when he received a new Macintosh 540c laptop computer, serial number FC37N5J2T0. At that time the 180c was returned to the OSD Help Desk and used by other OSD personnel. Dr. Deutch used the 540c until he left his position as the DEPSECDEF. This computer was also returned to the OSD Help Desk and used by other personnel. In July 1998, the 180c and 540c laptop computers became excess property and were donated to Florida A&M University as part of the Educational Institutions Partnership Program. Under this program, DoD transfers used DoD computers to educational institutions. DoD regulations provided that all commercial off-the-shelf operating systems and any sensitive or personal data contained in computers being excessed in this manner be removed before the computer is donated. **[Deleted]** told us that Dr. Deutch used these two computers to store his journal, which was later found to contain classified information.

[Deleted] also told us that in January 1994 when the USD(A&T) front office began to receive the Quadra 650 computers, he installed a Quadra 650 in Dr. Deutch's personal residence in **[deleted]**. This computer was in addition to the computer that Dr. Deutch used in the office.

B. What computers did Dr. Deutch use during his tenure as DEPSECDEF and where were the computers located?

Computers used by Dr. Deutch in his office

When Dr. Deutch became the DEPSECDEF, he took USD(A&T) computers with him to his new position. The Quadra 650 Dr. Deutch was already using as a desktop workstation in his USD(A&T) office was simply moved to his new office and used by him until he left the DoD. Another computer that transferred with him was the 180c laptop. According to **[deleted]** another computer, a Quadra 650, which had been previously installed in his residence, was allowed to transfer when he became DEPSECDEF. Dr. Deutch used the 180c laptop until August 1994 when a new Powerbook 540c was procured for his use. The Quadra 650 was believed to have been retrieved from Dr. Deutch's residence in September 1995 and placed in storage at the CIA.

Disposition of computers Dr. Deutch used at his DEPSECDEF office

We found no documentation reflecting the exact disposition of the Quadra 650. However, a witness told us that the subject Quadra 650 was "wiped" of data, applications reloaded and reissued within OSD. No records were located to confirm or refute this witness's statement. In the summer of 1998, the 180c and the 540c that Dr. Deutch used were transferred to Florida A&M under the Educational Institutions Partnership Program. We subsequently recovered those computers and sent them to NSA and DCFL for data recovery.

Disposition of computers that Dr. Deutch used at his residence while DEPSECDEF

As mentioned previously, in January 1994, Dr. Deutch, while still USD(A&T), was issued a Quadra 650 for use at his residence. In January 1995, Dr. Deutch was issued a Macintosh Power PC 7100 serial number FC452lW944H, for use at his personal residence. When Dr. Deutch left his DEPSECDEF position to become the DCI, the Power PC 7100 remained at his residence. Property records maintained by the WHS reflect that the DoD transferred ownership of the Power PC 7100 to the CIA in March 1996. **[Deleted]** told us that in September 1995, after Dr. Deutch became the DCI, he was at Dr. Deutch's residence performing computer maintenance on the Power PC 7100 when Dr. Deutch **[deleted]** asked him to remove the "old system" because Dr. Deutch no longer used it. **[Deleted]** told us that he believes that the "old system" was actually the DoD-purchased Quadra 650 that he installed in Dr. Deutch's residence in January 1994. **[Deleted]** told us that he distinctly recalls retrieving the computer, taking it to the CIA computer storage room, and labeling it as belonging to Dr. Deutch. This statement however is inconsistent with information provided by the Chief, USD(A&T) Executive Support, ITB. The Chief told us that he did not recall a Quadra 650 ever being installed in Dr. Deutch's residence. We were unable to resolve this discrepancy and determine whether a DoD-owned Quadra 650 was or was not installed in Dr. Deutch's residence.

C. Did Dr. Deutch store classified information on unclassified computers while serving as the USD(A&T) or as the DEPSECDEF?

In this section we address the storage media used by Dr. Deutch while with the Department and as the DCI, the procedures that were in place to ensure that sensitive or classified data were not inadvertently released; and whether the NSA and the DCFL

recovered data from the computers he used.

Several witnesses told us that none of the computers that Dr. Deutch used during his tenure with the Department were designated to store classified data. Witnesses also told us that Dr. Deutch kept a detailed journal of his daily activities during his tenure with the DoD. This journal formed the basis for several issues previously investigated by the OIG, CIA and was found to contain classified information. While Dr. Deutch was the USD(A&T) and the DEPSECDEF, he maintained the journal on floppy disks. As mentioned previously Dr. Deutch was known to transport these floppy disks in his shirt pocket. **[Deleted]** told us that while Dr. Deutch was still with the DoD he began to experience a number of disk "problems." As a result, after he became the DCI, Dr. Deutch changed from using floppy disks to store his journal to using Personal Computer Memory Card International Association (PCMCIA) cards that were provided to him by the CIA. The OIG, CIA, investigation revealed that Dr. Deutch had four PCMCIA cards that contained nearly 100,000 pages of information, including the daily journal covering the period of Dr. Deutch's service as the USD (A&T), DEPSECDEF, and the DCI.

During his OIG, CIA, interview Dr. Deutch said that he became accustomed to exclusively using unclassified Macintosh computers while serving in the DoD. He also acknowledged that before becoming the DCI, he was aware of the security principle requiring physical separation of classified and unclassified computers. However, he also told the OIG, CIA, that he believed that when a file or document was deleted (i.e., placed in the trash folder) the information no longer resided on the magnetic media, nor was it recoverable. Dr. Deutch also said during his interview that it was his usual practice to create a document on his desktop computers, copy the document to an external storage device (i.e., floppy disk) and then delete the initial document.

Computer experts have advised us that each time the journal was updated the computer automatically created a temporary file that would be stored on the hard drive of the computer in use. Of particular concern is the fact that the OIG, CIA, discovered that Dr. Deutch accessed the Internet via his America Online (AOL) account using the same computer at his home that he used to update his journal.[5] Therefore, it is feasible that a computer "hacker" could have gained access to Dr. Deutch's computer and the information stored in temporary files on the hard drive, including the journal.

[5] During his interview with the OIG, CIA, Dr. Deutch said that **[deleted]** used the Government-owned computer in their **[deleted]** residence, as did **[deleted]**.

As mentioned previously, two computers (the 180c and the 540c) were donated to Florida A&M, and several computers and hard drives went to other private entities. In addition, the OIG, CIA, during its investigation of Dr. Deutch recovered the Power PC 7100 from Dr. Deutch's residence.

According to **[deleted]** Dr. Deutch used the 180c and the 540c to store his journal. We recovered these computers from Florida A&M and interviewed the professor that ultimately received them for his use. The professor told us that the hard drive of the 180c did not work and therefore he never used the computer. However, he did turn on the 540c, but could not get his email program to work on this computer. He then simply put the computer on a shelf, and never used it again.

The Compromise and Computer Forensics Counterintelligence Services of the NSA and the DCFL performed forensic recovery examination of the hard drives of these two computers to determine whether the hard drives contained any data placed on them by Dr. Deutch. Both the NSA and the DCFL were able to recover a substantial amount of DoD information. Data analysis by the ASD(C3I) of the information recovered determined that the information was not classified. The ASD(C3I) will separately report his findings. The OIG, CIA, has advised us that Dr. Deutch processed classified information on the Power PC 7100 that they recovered from his residence during their investigation.

In addition to the aforementioned computers, we identified several other computers to which Dr. Deutch may have had access. Based on existing property accountability records, personnel within WHS generated a list of computers that Dr. Deutch may have used . All of these computers were found to have been sent to the DRMO for disposal. Subsequently, a private company, Olson Electronics of Baltimore, Maryland, purchased these and other DoD computers from the DRMO. Because the computers were purchased as "scrap," serial numbers were not always recorded as part of the transaction. However, we were able to trace and recover some of them. Contrary to the earlier practice of demolishing all computer hardware, the DRMOs at the time were selling computers intact.

We found that one Quadra 650 had been resold to a computer store in Crofton, Maryland, while five other Quadra 650s were resold to a Mennonite School in Ephrata, Pennsylvania. Two of the Quadra 650s at the school did not have hard drives in them. Also located at the school were six loose hard drives, of which two came from the two Quadra 650s mentioned above.[6] We retrieved all of the computers and the loose hard drives, which we sent to the DCFL for analyses. The DCFL has advised us that only one of the six hard drives that we recovered contains DoD-related information, and that information was not attributable to Dr. Deutch. The ASD(C3I) has determined that this information is not classified.

[6] We noted that inventory records for these computers were highly inaccurate.

Although media analysis did not disclose storage of classified information, it does not necessarily mean that such information was not processed on the computers. Information is automatically stored as a temporary file and could have later been overwritten with other processing.

The overall standard for information security is DoD 5200.1-R. That regulation requires that classified information be destroyed so that it cannot be reconstructed. The ADP Security Manual, DoD 5200.28-M provides a number of ways to remove such classified information, depending on the medium and the condition of the equipment. Those methods include overwriting a minimum of three times, exposure to a permanent magnet, and setting the memory locations alternately to ones and zeros for 1000 cycles.

The Defense Material Disposal Manual, DoD 4160.21-M, provides that before material is accepted for disposal by a DRMO, an accountable officer must certify that any information remaining on the computer is unclassified or has been declassified and that the material does not contain data unauthorized for release. That certification is to ensure that classified media has been declassified under procedures in the ADP Security Manual and that any information exempt from release under FOIA (e.g., proprietary, criminal investigation reports and personal data) has been removed. We found no certification documents for any of the computers used by Dr. Deutch during his tenure with the DoD.

D. Did Dr. Deutch have access to an OSD email server during his tenure as the USD(A&T) and DEPSECDEF and which computers did he use?

We found that in April 1993 the Chief, Information Technology Division, OSD, assisted Dr. Deutch in establishing what is referred to as "dial-up" scripts. According to this witness, he established three such "dial-up" scripts for Dr. Deutch which could be used on both office and home computers. One script enabled Dr. Deutch to have access to the Internet service provider at the Massachusetts Institute of Technology. The second script allowed Dr. Deutch "dial-up" service to **[deleted]** with respect to his personal banking services. The third script was for the Pentagon's dial-up service which allowed Dr. Deutch to "dial into" the OSD email server to receive and send email. Dr. Deutch's access continued during his tenure as the DEPSECDEF and was terminated on May 10, 1995, the day prior to becoming the DCI. As described later in this report, Dr. Deutch's access to the DoD email server was reinstated and continued until January 1996 when the CIA established "dial-in" capability to the CIA email server.

The computers that Dr. Deutch used as an email/fileserver during his tenure as the USD(A&T) and DEPSECDEF

In this section, we address two different OSD servers, a Macintosh 800 and a Macintosh 8150. The Macintosh 800 was the primary email/fileserver. The 8150 serial number XB5180184UK, was used to create backups of email. We were unable to determine the type of computer that was used as the USD(A&T) front office primary email/fileserver for the period of April 1993 to January 1994. However, we believe that when the USD(A&T) front office converted from using Quadra 800 computers to the Quadra 650 computers in January 1994, one of the two previously mentioned Macintosh Quadra 800s that was assigned to the USD(A&T) front office was reconfigured to become the primary email/fileserver. As mentioned above, we were not able to determine the final disposition of the Quadra 800, but we believe that this computer was sent to the DRMO for disposal.

We determined that the primary 800 email/fileserver supported the Macintosh computers within OSD. The 800 automatically retained a copy of all email traffic from the DEPSECDEF email accounts. The 800 continued to support OSD until OSD converted from using Macintosh computers to a Microsoft based email system.

The 8150 created incremental backups of the email/fileserver. There were three copies of email traffic, with the oldest copy being overwritten each time a backup was made. A witness told us that after the Microsoft based email system was in place for some time he deleted the archive of emails in order to free space on the hard drive of the 8150. In 1998, OIG, CIA, as part of their investigation, requested that the Department recover any data remaining on the hard drive of the 8150 which may have contained archived emails sent or received by Dr. Deutch while the DCI. As part of their investigation, the OIG, CIA, request focused on the 8150 because by this time the Quadra 800s had already been sent to the DRMO. During the resulting analysis, approximately 1,089 pages of email were recovered. Information recovered from the 8150 was subsequently copied onto several disks and retained. The server itself was also retained for about eight months and then, ultimately turned in to WHS for disposal. The computer disks containing the email information were turned over to ASD(C3I) security personnel for review. We have been advised that none of the recovered email documents were classified.

During our inquiry, it was determined that WHS had not disposed of the 8150. The 8150 was recovered and provided to the NSA and subsequently to the DCFL to determine whether any additional data remained on the hard drive. The NSA advised us that no additional data could be recovered from the 8l50 as it had been properly "clean-swiped."

E. Did Dr. Deutch have access to the OSD email/fileserver after he became the DCI and which file server did he use?

When Dr. Deutch transferred to the CIA, his access was terminated to the OSD email/fileserver. However, the next day, May 11, 1995, Dr. Deutch asked **[deleted]** who, by this time was a CIA employee, to restore his access. **[Deleted]** coordinated Dr. Deutch's request with the Chief, OSD Computer Support Branch and Dr. Deutch's access was reinstated. His access to the OSD email/fileserver continued until January 1996 when the CIA established "dial-in" capability for the CIA email server.[7] According to **[deleted]** Dr. Deutch only used the OSD email server and did not have access to other files.

[7] There is a conflict between two witnesses regarding the dates that Dr. Deutch was granted access to the OSD email server. One witness believes that Dr. Deutch was granted access the day after he became the DCI. Another witness believes that Dr. Deutch did not receive access until several months after he became the DCI. We do not view this discrepancy as significant as the issue is whether Dr. Deutch transmitted classified information using the OSD email server at any time during his tenure with the Department.

VI. CONCLUSIONS

A. Dr. Deutch used at least seven different Government-owned Macintosh computers while with the DoD. He used a Quadra 800, two Quadra 650s, and a Power PC 7100. He also used three Macintosh Powerbook laptops: a 180, a 180c, and 540c. The Power PC 7100 was transferred to the CIA when Dr. Deutch became the DCI.

B. Dr. Deutch processed his journal that contained classified information on unclassified computers both at his residence and his office.

C. Dr. Deutch obtained access to and used the OSD email server after he left the Department.

D. Dr. Deutch's Government-owned computers were used by Dr. Deutch and his family to access his AOL account.

E. Several computers used by Dr. Deutch while he was with the Department were not adequately "clean-swiped.

VII. RECOMMENDATIONS

A. Implement policy requiring that all hard drives of computers to be disposed of outside the DoD be destroyed.

B. Reemphasize the prohibitions of placing classified material on computers not designated to store such information.

C Reissue warnings advising DoD personnel of the dangers of using the Internet while operating Government computers.

D. Examine property accountability practices for computers within OSD including computer hardware and software applications.

E. Review the procedures for granting access to the OSD email server to ensure that such access is granted to only those personnel that have a requirement to conduct departmental business.

Source: Hardcopy
Original Classification: Unclassified, For Official Use Only
HTML by Steven Aftergood

FAS | Government Secrecy | Other Gov Docs ||| Index | Search | Join FAS

EXHIBIT 12

From: GaryM Stern [redacted]@nara.gov> [redacted]@nara.gov>
Sent time: 09/06/2021 11:59:47 AM
To: Per. 38 [redacted]@gmail.com>
Subject: Re: Need for Assistance re Presidential Records

P. 38 fyi, I spoke with Jonathan Su after we talked on Friday. I'm not sure if you've connected with him yet as well, but he suggested that the three of us talk first early this week, before we try to set up the meeting that you had in mind. I can follow up set up a call.

Also, here's additional background on the social media issues we discussed. On page 2 of the Archivist's March 30, 2017, response to queries from Senators McCaskill and Carper, he stated that "NARA has advised the White House that it should capture and preserve all tweets that the President posts in the course of his official duties, including those that are subsequently deleted, as Presidential records, and NARA has been informed by White House officials that they are, in fact, doing so." The letter was vetted and cleared by your predecessors in the Counsel's Office.

- No steps were taken to capture deleted content from any Trump Administration social media records other than @realDonaldTrump until the Administration procured a third party social media archiving tool in February 2018. After that, use of the tool was widespread but not timely. For example, most accounts were eventually enrolled but may have been active for weeks, months, or years prior to enrollment, during which time deleted content was not captured.

- At the end of the administration, NARA learned that the White House stopped using the social media archiving tool to capture deleted Tweets in April 2020, and Twitter was unable to provide the deleted Tweets to us after the fact. Accordingly, NARA was unable to obtain a complete set of these Presidential records from the White House. NARA is considering utilizing what was collected by non-governmental sources as an adjunct to our archival collection.

- The third party tool used to capture social media content from Twitter, Instagram, and Facebook included the ability to capture direct messages on the platforms. The Administration opted not to enable capture of direct messages, but was unable to report whether direct messaging was used on any of the platforms by the account holders.

- NARA identified seven Twitter accounts that we believe contain PRA records but were not captured by the Trump Administration. NARA obtained the publicly available tweets at the end of the administration through a third party to supplement its archival collection. These include accounts from Andrew Giuliani, Chad Gilmartin, Ivanka Trump, Kayleigh McEnany, Kellyanne Conway, Mark Meadows, and Peter Navarro.

- In its last weeks, the Trump Administration advised NARA that two social media accounts it believed should be treated as containing PRA content were not enrolled in their third party archiving tool and could not be retroactively enrolled. These accounts were Donald J. Trump on Facebook and @realDonaldTrump on Instagram. NARA endeavored to work with Facebook to obtain access to the accounts but was never able to do so.

- SnapChat was used by the Trump Administration (realdonaldtrump and whitehouse), and NARA was advised that they were capturing content posted to the platform. NARA reviewed the transferred social media records and has not located any SnapChat content. SnapChat ultimately banned President Trump from the platform and it is not possible to see any previous content. SnapChat advised NARA that the Trump administration used the White House account approximately five times during four years. However, the realdonaldtrump account was used regularly. News reports indicate the account had 1.5 million followers on the platform. It is not known whether direct messaging was enabled on the account.

Finally, on a separate but related note, we are arranging to pick up the PRA materials from Dr. Birx on Tuesday (tomorrow). As I mentioned to you before, her attorney has asked for assurances that Dr. Birx will be allowed access to these documents at the Archives so she can be prepared in the future for questions she may be asked about the period when she was coordinating the Coronavirus task force. You had indicated that this should not be a problem. Please confirm that we can provide such access to Dr. Birx.

Thanks,
Gary

Gary M. Stern
General Counsel
National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740
[redacted]

EXHIBIT 13

From: Person 21 @nara.gov>
Sent time: 09/16/2021 09:56:09 AM
To: Per. 48 @nara.gov>
Cc: @nara.gov>
Subject: LW Update 09/15/2021

P. 48

Here are a few things I wanted to alert you to. None of this has to due with the upcoming meeting.

1) Gary and I have a meeting at the White House tomorrow. We don't know what it is about; we just know we are meeting in a SCIF. Looking at the guest list, I'm guessing this is routine and not anything out of the ordinary. I'll let you know.

2) The White House has requested P. 40 and Per. 39 deputy) folders related to the 24 Trump boxes that were in the Residence. Per. 38 has signed off. We will get those over there today. This is in prep for what will likely be a meeting involving the Trump reps, P. 40 White House Counsel, and maybe GMS and me. The Trump folks still say that they only have 12 boxes and they are full of newspaper clippings. I'll keep you posted.

3) It looks like the plan is to decouple the 24 box issue from the missing social media issue. I believe this is happening for two reasons First, until the P. 40 /Trump/WH meeting happens, David isn't planning on going to DOJ. Second, the 1/6 Committee has asked for tweets from @realDonaldTrump that we don't have because the White House failed to keep the account enrolled. It's fuzzy how all of this is going to play out, though. It also ties in to us beginning to offer what we do have (@RDT and other Trump accounts not still on their native platform for download). That is tentatively scheduled for 10/4. All the language has been approved for updating the Trump Library webpage, and Natalie and Innovation are testing all of the links.

4) Stephannie, Hannah, and I have Gary convinced that trying to supplement/fill in the missing gaps of @RDT is not the way to go. GMS thought this was a good idea, and according to GMS, David asked what we were going to do to get a complete record. I'm happy to provide more info as to why we think this is a bad idea.

5) N/A has set up a 15 minute meeting today to address his question of how do we know that we got everything, re: Trump electronic records. The attendees are mostly his IT staff, but Jay has been added to this one. Gary has already explained to him that we only know what we know and as with any transfer or accession on the Federal side, we go by what they tell us. This particular issue, as best I can tell, was sparked by a question about the photos. But I am unsure. I don't think anything will come from this other than Jay and N/A thinking that we should do a better job.

6) On (I think) the other photo issue that I mentioned in our last update, WH/OA is still trying to track down the issue. But it looks as if there isn't a major glitch. But they are still looking into it.

7) I thought Abigail and I would be able to get all these classified pages numbered (per the NARA 202 "Sandy Berger" rules). I don't think that is going to happen. So I'm going to look into asking for a waiver.

8) Per. 58 and I continue to try to piece together what is going on with the calligraphy binders. I owe her a call. We'll see what she says.

9) Scanning N/A correspondence has slowed because they found a classified document in the mix. So they are having cleared staff screen everything. Also, they have agreed to scan the other six boxes. When we realized that all the material was responsive and that it was just a straight copy job, Denise and company (with Ann's approval) agreed to take that on as well.

Per. 21

--

Per. 21
Director,
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408-0001

[redacted](a)
[redacted]@nara.gov