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. (U//FOUO) 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. (U//FOUO) 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. (U//FOUO) 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. (U//FOUO) 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. (U//FOUO) 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 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)

---

[1](U//FOUO) 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.

[2](U//FOUO) 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.

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. (U//FOUO) 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. (U//FOUO) 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 unauthorized access to the information and thereby placing national security information at risk.

8. (U//FOUO) 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

[3] (U//FOUO) Hereafter, the residences will be referred to as Maryland and Belmont.

9. (U//FOUO) 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. (U//FOUO) 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

2. (U//FOUO) 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?

(U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) **[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.

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

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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."

¨ (U//FOUO) 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

[4](U//FOUO) This division has since been renamed the Administrative Law and Ethics Division.

use. He advised that he would discuss the matter with the Principal Deputy General Counsel (PDGC).

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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 the provision of a laptop computer for three months and a desktop computer for up to a year.

[5] (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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]

¨ (U//FOUO) 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."

¨ (U//FOUO) The MFR indicates that **[the two OGC attorneys]** dropped their objections to the loan of the computers, based on 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.

¨ (U//FOUO) 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.

---

[6](U//FOUO) The OIG investigation has not located any contract that includes a third computer.

WHAT INFORMATION WAS FOUND ON DEUTCH'S MAGNETIC MEDIA?

How was the classified material discovered?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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]

¨ (U//FOUO) 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.

¨ (U//FOUO) 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

[7](U//FOUO) 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.

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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

[8](U//FOUO) The former ADDA retired in October 1997.

¨ (U//FOUO) 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 information on Deutch's computers that had Internet connectivity was compromised.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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."

¨ (U//FOUO) Subsequent investigation by OIG revealed that Deutch had paged the contract network engineer at 1000 hours on 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 . . . .

¨ (U//FOUO) 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

[9] (U//FOUO) 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.

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.

¨ (U//FOUO) Indications of Internet, **[an ISP]**,[11] an unclassified Pentagon computer e-mail,[12] and online banking usage were found 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.

¨ (U//FOUO) Recovered computer-generated activity logs reflect, in certain instances, classified documents were created by

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

[11](U//FOUO) 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.

[12](U//FOUO) 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].**

"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.

¨ (U//FOUO) The following text box provides a summary of Deutch's magnetic media that resulted in the recovery of classified information.

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[1]
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.[2] **[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," "Property of /DCI…."	Global Village Internal Modem	Two complete classified documents and text fragments including TS/Codeword.
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?

¨ (U//FOUO) 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.

¨ (U//FOUO) **[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.

¨ (U//FOUO) 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.]**

¨ (U//FOUO) 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]**.

¨ (U//FOUO) Deutch's memorandum to the President found on a PCMCIA card from the Maryland residence also **[discusses a non-CIA controlled compartmented program]**.

¨ (U//FOUO) 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.]**

¨ (U//FOUO) 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]**.

¨ (U//FOUO) 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]**.

¨ (U//FOUO) **[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]**.

¨ (U//FOUO) 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]**.

¨ (U//FOUO) 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]**.

¨ (U//FOUO) Deutch's journal, which was found on a PCMCIA card from the Maryland residence, also covered this topic but in more detail.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) The technical exploitation team determined that high risk Internet sites had placed "cookies"[13] 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?

¨ (U//FOUO) Deutch's government-issued computer at his primary residence in Maryland contained an internal hard drive and was 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.

¨ (U//FOUO) 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

[13](U) 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.

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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.[14]

¨ (U//FOUO) 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."

¨ (U//FOUO) 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.

¨ (U//FOUO) 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 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.

¨ (U//FOUO) 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

[14](U//FOUO) 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.

that he had not spent a significant amount of time thinking about computer security issues.

¨ (U//FOUO) 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?

¨ (U//FOUO) On August 1, 1995, Deutch and several senior CIA officials receive**[d]** various operational briefings.

¨ (U//FOUO) **[During these briefings,]** Deutch was specifically told that data residing on a **[commercial ISP network was vulnerable to a computer attack.]**

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) **[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.

¨ (U//FOUO) **[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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) **[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.

¨ (U//FOUO) 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?

¨ (U) 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.

¨ (U) 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.

¨ (U) 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.

¨ (U) 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.

¨ (U) 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.

¨ (U) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.[15]

¨ (U//FOUO) **[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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

[15](U//FOUO) In his interview with OIG, Deutch confirmed he reviewed the original PCMCIA cards to delete personal information.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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."

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.[16] 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.

[16](U//FOUO) 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."

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.[17] 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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

[17](U//FOUO) C/SIB noted that he did not review Deutch's official security file. OIG reviewed the file.

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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.[18] 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

[18](U//FOUO) 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.

> 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

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

¨ (U) 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.

¨ (U) 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 . . . ."

¨ (U//FOUO) 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.[19] The new procedures are contained in a document, "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," signed by DCI Deutch.

¨ (U//FOUO) According to the Memorandum of Understanding (MOU),

> [w]hen the General Counsel has received allegations, complaints, or information (hereinafter allegations) that an employee[20] 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[21] 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.[22]

¨ (U//FOUO) 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.

---

[19](U//FOUO) 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.

[20](U//FOUO) 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."

[21](U//FOUO) 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."

[22](U//FOUO) 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.

¨ (U//FOUO) 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.[23]

¨ (U//FOUO) 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 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.

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

---

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

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.[24]

¨ (U//FOUO) 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.[25] 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 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

[24](U//FOUO) 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.

[25](U) "811" is Section 811 of the Counterintelligence and Security Enhancement Act of 1994.

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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) The PDGC had supervisory responsibility of the Litigation Division which had the crimes reporting account in OGC at that time.[26] 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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[27] regarding the provisions 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

[26](U//FOUO) 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.

[27](U//FOUO) 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. 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.

[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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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"[28] by Deutch. She reasoned that "intent" was a necessary element, "otherwise everyone [inadvertently] carrying classified information out of a 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

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

the computer would have been to remove and secure the computer's hard drive.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.[29]

¨ (U//FOUO) 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.

[29](U//FOUO) 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.

SHOULD APPLICATION OF THE INDEPENDENT COUNSEL STATUTE HAVE BEEN CONSIDERED?

¨ (U) 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.

¨ (U) 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.

¨ (U) 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 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.[30]

¨ (U) 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 . . . .[31]

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

---

[30] (U) 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.

[31] (U) 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.

> 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.

¨ (U) 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.

¨ (U//FOUO) 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. 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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."

¨ (U//FOUO) 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?

¨ (U) 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.

¨ (U//FOUO) 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);

¨ (U) 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)[32] 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.

¨ (U//FOUO) According to the Director of the CIA's Office of Congressional Affairs (OCA), OCA is responsible for notifications to

[32](U) The Intelligence Oversight Board is a standing committee of the President's Foreign Intelligence Advisory Board.

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.

¨ (U//FOUO) At the January 6, 1997 meeting to discuss the planned investigation of the finding of classified information on Deutch's 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.

¨ (U//FOUO) 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.[33]

¨ (U//FOUO) 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.

¨ (U//FOUO) 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."

¨ (U//FOUO) Slatkin stated she could not recall any discussion or recommendation regarding the need to notify the Congressional committees

[33](U) 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.

about the Deutch matter. In her interview with OIG, she stated that, "surely, yes, the Committees should have been notified—but at what point?"

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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,[34] 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.

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

[34](U//FOUO) 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.

WHAT WAS OIG'S INVOLVEMENT IN THIS CASE?

When did OIG first learn of this incident?

¨ (U//FOUO) The former C/DCI Administration spoke with then-IG Frederick Hitz on December 18, 1996[35] 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,[36] 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

[35](U//FOUO) Hitz served as CIA IG from October 12, 1990 until April 30, 1998, when he retired.

[36](U//FOUO) The former C/DCI Administration provided a copy of his MFR to Hitz, Calder, and C/SIB.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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."

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.[37]

¨ (U//FOUO) 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?

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

[37](U//FOUO) 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.

¨ (U//FOUO) 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.[38]

¨ (U//FOUO) 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 "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[39] were discussed relative to SIB's ongoing investigation, nor were any requested.
>
> ¨ (U//FOUO) 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

[38] (U//FOUO) Hitz corroborates the OPS Legal Advisor's account of this meeting.

[39] (U//FOUO) 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.

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."

¨ (U//FOUO) 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 Investigations does not recall knowing at the time that the OPS/SIB investigation involved classified information.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) Hitz explained that a security violation of this nature would not normally be a matter investigated by OIG.[40] 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 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?

¨ (U//FOUO) 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."

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

---

[40](U//FOUO) 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.'"

¨ (U//FOUO) 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?

¨ (U//FOUO) 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?

¨ (U//FOUO) 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

¨ (U//FOUO) Former DCI John Deutch was specifically informed that he was not authorized to process classified information on government computers configured for unclassified use.

¨ (U//FOUO) Throughout his tenure as DCI, Deutch intentionally processed on those computers large volumes of highly classified information to include Top Secret Codeword material.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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.

¨ (U//FOUO) DCI George Tenet should have involved himself more forcefully to ensure a proper resolution of this matter.

¨ (U//FOUO) 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.

¨ (U//FOUO) 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. (U//FOUO) John Deutch's continued suitability for access to classified information should be reviewed immediately.

2. (U//FOUO) 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. (U//FOUO) 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

[40](U//FOUO) 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.

[40](U//FOUO) 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.