



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)
)
) ISCR Case No. 08-03118
)
)
Applicant for Security Clearance)

Appearances

For Government: James F. Duffy, Esquire, Department Counsel
For Applicant: William Bransford, Esquire, and
Maria Coleman, Esquire

November 24, 2008

Decision

RICCIARDELLO, Carol G., Administrative Judge:

Applicant failed to mitigate the government's security concerns under Guideline K, Handling Protected Information, Guideline M, Use of Information Technology Systems, and Guideline E, Personal Conduct. Applicant mitigated the security concerns raised under Guideline C, Foreign Preference. Applicant's eligibility for a security clearance is denied.

On July 31, 2008, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) detailing the security concerns under Guidelines K, M, E and C. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6; *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant answered the SOR in writing on August 21, 2008, and requested a hearing before an Administrative Judge. The case was assigned to me on September 17, 2008. I was advised through Department Counsel that Applicant and his Counsel requested the first available hearing date. I was available to hear the case on October 1, 2008. With the concurrence of both Department Counsel and Applicant's Counsel, the case was scheduled for October 21, 2008. DOHA issued a notice of hearing on September 29, 2008, and I convened the hearing as scheduled and with the concurrence of both parties. The government offered Exhibits (GE) 1 through 51, which were admitted without objections. The government also presented two witnesses. Applicant offered Exhibits (AE) A through D, which were admitted without objections. An additional exhibit was marked as Hearing Exhibit (HE) I and included in the record. Applicant testified and two witnesses testified on his behalf. The hearing was completed on October 22, 2008, and the record closed. DOHA received the transcript of the hearing (Tr.) on October 30, 2008.¹

Findings of Fact²

Applicant admitted the allegations in SOR ¶¶ 1.a, 1.b, 1.c, 2.a, 3.a, 3.b, 4.a, and 4.b and provided explanations. He denied the allegations in SOR ¶¶ 1.d, 2.b, and 2.c and also provided explanations. His admissions to the allegations in the SOR are incorporated herein. In addition, after a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 50-year-old former Department of State employee. He served with the State Department from 1973 to March 2005, retiring after approximately 32 years. He was assigned to various postings around the world and received promotions to some of the highest positions in the agency. Immediately after he retired from the State Department, he was a contract employee, essentially working in the same job as before retiring. While with the State Department he held a Top Secret clearance and access to Sensitive Compartmented Information (SCI).

The following are the findings of facts for the allegations for which Applicant has admitted:

While employed by the State Department from 1978 to 1994, Applicant committed approximately 21 security violations or infractions. Some of these security violations and infractions occurred while Applicant was working in U.S. embassies overseas. He left classified documents unsecured on his desk or in his office or left his safe that was used for storing classified documents unsecured. Some of the same type of security violations or infractions occurred later at his office in the United States. He

¹ The record of hearing has two volumes and each begins its numbering of pages with the number 1. Therefore, the transcript does not have consecutive numbering. I have referenced the first volume using Tr. and the second volume as Tr.II.

² Some details have not been included in order to protect Applicant's right to privacy. Specific information is available in the cited exhibits.

testified that his office in the United States was located on a secure floor. He testified that it was determined that there was either no compromise of classified information or the likelihood of compromise was minimal.³

Specifically the records reflect from 1978 to 1979, Applicant had five security infractions while stationed at an embassy overseas.⁴ Applicant was counseled after each incident. Applicant was transferred to a new overseas embassy and had two security infractions one in 1982 and one in 1983.⁵ Five of the infractions from 1978 to 1983 involved leaving both confidential and secret documents unsecured. Two of the infractions involved leaving the safe that stored classified documents unsecured. Applicant acknowledged that after each infraction he was counseled and advised of his responsibility to lock the safe and keep the classified documents secured.

From 1987 through 1990, Applicant committed eleven security infractions and one security violation while stationed at another overseas embassy assignment. Nine infractions were for leaving classified documents unsecured and two infractions were for leaving the safe that stored classified documents unsecured. Applicant's security violation was for using an unclassified word processor for classified material. Applicant concurred that he was counseled after each infraction and violation, but stated "I would say in a perfunctory manner..."⁶ He did not recall having individual security briefings as a result of the number of security infractions and violations, but he did not exclude it.⁷

On December 22, 1988, Applicant received a letter from a senior State Department official advising him of official disciplinary action against him for "lack of effective security practices which led to nine security violations."⁸ Applicant's response as noted in the letter and his testimony at the hearing explained that his supervisor at the time was very difficult to work for; the bulk of the violations occurred during a period immediately after he arrived at his assignment and before an inspection; he had a busy office and there was a need to respond to issues on short notice and often after hours; and he was often the last to leave the office. He also noted as a factor in mitigation that there was a great deal of tension and pressure that he felt due to the senior person for whom he worked.⁹ Applicant's response also included that he had met with the security

³ Tr. II at 13; GE 2 at 17.

⁴ GE 13. They occurred on August 2, 1978; August 31, 1978; December 12, 1978; September 18, 1979; and December 13, 1979.

⁵ GE 13. The two infractions occurred on June 7, 1982; and June 15, 1983.

⁶ Tr. II 96; GE 13. The infractions and violations occurred on the following dates: July 8, 1987; August 12, 1987; August 25, 1987; February 25, 1988; March 29, 1988; April 1, 1988; April 23, 1988; April 27, 1988; April 29, 1988; May 7, 1988; March 13, 1989; and March 21, 1989.

⁷ Tr. II 96.

⁸ GE 14.

⁹ Tr. II 17-20.

officer and put into place new procedures that would alleviate future violations, and he had received other helpful suggestions. Applicant was reminded in the official letter that he was a role model to subordinates. In the official letter it also acknowledged that Applicant took his responsibilities seriously. This letter informed Applicant that he was suspended from his duties without pay for 16 days. It also informed him that, although all of the security violations were valid, two of them were discounted, in order to reduce the suspension from 36 days to 16 days, so it would not be a hardship on the office. He was advised that future violations would not be discounted. Applicant was further advised that a copy of the letter would be made a part of his official personnel file where it would remain for a period for two years.¹⁰

Applicant received a second official letter on May 21, 1990, in which he was informed that he would be suspended from his duties for ten days without pay for his “lack of effective security practices which led to eight security violations.”¹¹ Applicant’s response in mitigation prior to the suspension was that he had been “interrupted by an urgent phone call” which he claimed minimized his full responsibility for the violation. He was further advised that the letter would remain in his official personnel file for a period of two years.

Applicant acknowledged at his hearing that these letters constituted “formal disciplinary actions.” He also agreed that being suspended without pay constituted disciplinary action.¹² After Applicant’s two suspensions, he committed two more security infractions after he returned to the United States.¹³

In his answer to the SOR Applicant commented that the State Department determined that none of the security violations resulted in “having compromised security” and that all of the violations occurred within a controlled area with 24-hour security.¹⁴ He further stated in a sworn affidavit the following, “I obtained security briefings, letters of warning and reprimand.”¹⁵

Applicant admitted that while he was assigned a high level position in the State Department and while serving overseas from January 2001 to July 2003, he misused a U.S. Government (USG) computer by accessing sexually explicit internet websites, by viewing and downloading sexually explicit images, and by allowing a guest of his to

¹⁰ Tr. II 96-98; GE 14. The letter does not specifically state whether his suspension was without pay, but Applicant admitted the allegation in SOR ¶ 1.a, which specifically states the suspension is without pay.

¹¹ GE 15.

¹² Tr. II 96-98.

¹³ GE 2 at 18.

¹⁴ Answer to SOR.

¹⁵ GE 2 page 17.

access sexually explicit websites. He explained that he had been using his personal computer for both official and personal use when due to an electrical power surge his personal computer was destroyed. A senior officer associated with the embassy provided a statement that explained:

[Applicant] expressed concern about keeping up with personal and informal correspondence and emails without that computer, not to mention business related messages on off hours and the weekend. I mentioned to [Applicant] that he could use his USG computer to keep up with his correspondence and get access to the internet. I mentioned that was my understanding of the policy regarding USG computers in [government] residences.¹⁶

Applicant testified that he used the USG for both routine official correspondence and personal correspondence. Applicant provided a sworn affidavit that states:

[Person A] said that I did not have to buy a new computer that the [government] would provide me with a computer for personal use and this was done. I know that there is a regulation to not view pornographic material on a government computer, but this was in my residence and for my personal use only. I did do work on the computer as well because I was dedicated to the mission, but nothing of a classified or sensitive nature. I would type speeches, press statements and use email. I do not know if the computer was connected to the [government] intranet. I accessed the internet and did not have to switch between systems as I have had to at other locations so I assume it was not. I saw the Department of State warning banner on the computer, but again I believed that this computer was for my personal use.¹⁷

Applicant also stated that although he did view pornographic material he never did so in the workplace where he knew it was a violation of regulation.¹⁸

A State Department memorandum regarding the investigation about the misuse of the USG by Applicant provided a summary of an interview of Applicant about the event.¹⁹ It stated:

[Applicant] stated that he knowingly and deliberately viewed and accessed sexually explicit websites and downloaded sexually explicit images ... on the USG computer located at his [residence]. [Applicant] stated that he

¹⁶ AE A.

¹⁷ GE 2 page 18.

¹⁸ GE 2 page 19.

¹⁹ GE 16.

knew that his actions were contrary to Department regulation, but 'rationalized it as okay because he was violating regulations at the [residence] and not at his office.'²⁰

In addition, the memorandum stated: [Applicant] acknowledged that he told [Person A] that he accessed and viewed sexually explicit material on the USG computer located at the [residence].²¹ The memorandum also stated that:

[Person A] advised [Applicant] that the Admin section would install a USG computer at the residence for his use. [Applicant] could not recall if he received a briefing or signed a "user access agreement" prior to installation of the computer at the [residence].²²

Applicant stated he did not divulge this information when applying for a security clearance because he did not believe it involved a security violation and he believed he was only required to divulge those issues related to security violations. He further stated he was embarrassed by the event and was attempting to be discreet. Applicant acknowledged that in early 2004 he was suspended without pay for ten days for this violation. He also acknowledged that this action constituted disciplinary action.²³

Applicant acknowledged a guest at his residence also accessed his computer to view sexually explicit material. He was aware his guest was using the computer, but did not know until he asked him that he was also accessing pornographic material. When asked how soon he spoke with his guest after he became aware the Government had discovered his violation, Applicant stated: "I really don't remember how soon it was." He then was asked if it would have been immediately. He responded "No, I don't think it would have been immediately, but I really don't recall."²⁴

Applicant admitted the allegation in SOR ¶ 2.a, but explained he believed the computer was issued to him for her personal use. I find Applicant was aware he was using a government computer to access inappropriate material, albeit at his residence. I do not find his statement credible that he believed the computer was only for personal use. It is clear from the earlier interviews with the investigators that he was aware he was using a government computer for official and unofficial purposes and he was attempting to minimize his actions by stating he only viewed and downloaded material at his residence.

²⁰ GE 16 at 4

²¹ *Id.*

²² *Id.*

²³ Tr. II 98-100. GE 17.

²⁴ Tr. II 116-118.

Applicant admitted the following: He worked for a high ranking military officer from September 2003 to October 2004, in an overseas location. Applicant was also a high ranking State Department employee at the time. After the military officer (Officer B) retired Applicant stayed in contact with him. Applicant stated in his sworn affidavit:

I was aware, through conversation with [Officer B] that [Officer B] was consulting for [overseas command] and also for private companies (no specifics recalled). I assumed that [Officer B] still maintained his security clearance if he was with [overseas command], but I did not check this.²⁵

Appellant additionally stated the following in his sworn statement:

In February 05, [Officer B] emailed me and asked me if there was anything I could send him regarding [Country K]. [Officer B] was going to a [conference] and was going to talk about political issues regarding [Country K]. [Officer B] did not ask for anything in particular and did not ask for anything classified.

I had a summary of what the U.S. policy was on [Country K] and the document was classified Secret. The document was sent to me by the State Department, but I do not know who classified the document Secret. I do not disagree with the classification and I have no authority to declassify material.

The document was on my classified computer at my office in [City Q]. I tried to remove all of the classified marking on the document by highlighting the classified markings and then deleting them. I tried to make sure that I had accomplished this on all of the pages, but I was not sure if I was successful. I intentionally tried to cover up that the document was classified. I was trying to save time and effort on my part. I knew that what I was doing was wrong and a grave mistake.

I downloaded the document to a disc and then uploaded it to my unclassified computer, also in my office. I did this on my own and with no help or assistance from anyone. It was on my classified computer that I removed the classification markings before downloading and emailing the document to [Officer B] on my unclassified computer. Within the body of the email to [Officer B] I had stated something to the effect of not sharing this with anyone or acknowledge having seen it. I did this i[n] an attempt to let [Officer B] know that the information was classified, without actually saying that.

I do not know what [Officer B] did with the email, but after the investigation was completed and we had met for dinner, I believe that he told me that

²⁵ GE 2 page 29.

he destroyed it. We never discussed the content of the email or whether the document was classified or not. I do not recall what happened to the disc that the document was placed on. I gave all discs to my assistant [Ms. N] and I do not know what she did with them.

I realize that the release of this document to the wrong people could negatively affect U.S. security interests because it contained U.S. strategy and classified information on [Country K] and their future. I was not thinking of that and in trying to be expedant (sic) I just emailed the document to [Officer B].²⁶

Applicant went on to say: "Due to the above, my SCI clearance was pulled in Mar/Apr 05 and subsequently terminated."²⁷ In addition he stated: "I feel that I am aware of what is on my desk and have tasked my U.S. assistants with being vigilant with security and watching out for security issues. I take security seriously and watch for security concerns with the help of my assistants."²⁸

At his hearing Applicant testified that he provided the information to [Officer B] because of the following reasons: "[Officer B] asked me for information. Secondly, he was a friend. Thirdly, I knew he was, because he told me, that he was consulting for [command] and therefore had to have a security clearance."²⁹ He also knew [Officer B] would be attending a specific conference related to the information.³⁰ Applicant confirmed that the document he provided was a discussion paper from the State Department prepared for the "Principles Committee" and had been approved by the Deputy's Committee.³¹ Applicant recollected that the document was classified as "SECRET/NO FORN." (Meaning no foreign personnel are authorized access to the document). These markings were the ones Applicant removed or attempted to remove. Applicant affirmed that this document is disseminated to the secretaries of various departments or the head of federal agencies. It is the type of document that is authoritative on the U.S. position of current events in the specific country, a "suggested way forward," "next step in key elements and assumptions," engagement strategy" and "an annex with a time line."³² Applicant reiterated in his testimony that "I made the error of deciding to send that document to [Officer B], even though I knew that it had

²⁶ GE 2 at 29-30.

²⁷ *Id.*

²⁸ Tr. II 110; GE 2 page 30.

²⁹ Tr. II 30.

³⁰ GE 2 page 30.

³¹ Tr. II 31-32.

³² Tr. II 101-105.

classification on it.”³³ He further admitted he knew he was doing something wrong when he removed the classifications. He did this because he did not want to cause Officer B a problem. His purpose was to help Officer B to help promote the U.S. interests.³⁴

Officer B testified on Applicant’s behalf. After he retired from the military he stayed in contact with Applicant. Applicant had dinner with Officer B and his wife at their home and they also emailed each other. He considered Applicant a critical advisor when he was on active duty. Subsequent to his retirement, Officer B was to be a speaker at a conference and he admitted he asked Applicant if he could provide him with an update on Country K. He sent him an email and he received a response with an attachment to the email. The attachment showed a classification marking as “Secret.” Officer B stated he thought the document was misclassified or was going to be declassified.³⁵ He verified that there were foreign nationals in attendance at the conference who did not have a security clearance.³⁶

Officer B confirmed that GE 18 was a copy of the email that was sent from Applicant to Officer B and Officer B’s response. In Applicant’s email he stated: “PLEASE do not share this with anyone or acknowledge having seen it.” Officer B’s response to the email was: “Thanks for the info.” Officer B denied remembering the specifics of the document. He stated when he made the request to Applicant he did not request classified material and Applicant did not tell him he was sending a classified document. Officer B acknowledged that when he received the document he held a security clearance. He also acknowledged he received the classified document on his unclassified computer. He did not report that he received a classified document on his unclassified computer because he thought the document was unclassified and someone forgot to take the markings off of the document. He did not think to make such a report. He stated he assumed Applicant would not send a classified document. He also stated that it did not strike him as odd or unusual that Applicant specifically asked him not to share the document with anyone or acknowledge having seen it. Officer B acknowledged that he was never asked by Applicant if he still held a security clearance. Officer B was going to see Applicant at the conference the next day. He never asked Applicant about the classification of the document while at the conference. He stated he saw no need to verify the classification of the document until he was notified several weeks later that the matter was being investigated.³⁷

³³ Tr. II 32.

³⁴ Tr. II 33, 106-109.

³⁵ Tr. 304-307. Officer B provided his personal assessment of the importance of the information contained in the classified document. His personal assessment, although admissible, is mainly relevant as to the extent of potential damage to national security.

³⁶ Tr. 321-322.

³⁷ Tr. 304-310. Officer B’s computer was seized and searched by forensic investigators. He subsequently was interviewed by the Federal Bureau of Investigation.

Officer B has continued his association with Applicant and considers him a good friend. His opinion regarding his honesty, trustworthiness and ability to tell the truth is “extremely positive”. He felt honored that Applicant accepted the position at the command when he was in charge. He and Applicant worked closely for more than a year on high level and sensitive negotiations and his opinion regarding Applicant’s ability to safeguard classified material was that he was “very mindful” and made sure that all classified material was handled appropriately. He believes Applicant was properly trained and aware of the rules regarding security.³⁸

Applicant stated when he lost his access to SCI he did not appeal the decision because he was advised by the central adjudication facility that it would have no bearing on his security clearance status. Applicant felt he did not need access to SCI.³⁹

Applicant applied for and obtained recognition as a citizen of the Republic of Ireland. He admitted he applied for an Irish passport in 1991 and possessed it until relinquishing it before his hearing due to the security clearance implications.⁴⁰ He sought recognition as an Irish citizen because of his Irish heritage and because two of his grandparents were born in Ireland. He became an Irish citizen for sentimental reasons. He also had in the back of his mind that he might buy property in Ireland one day and perhaps live there part of the year. He thought it might be useful to have Irish citizenship and an Irish passport. In the past he has visited Ireland annually, but used his U.S. passport. He has never traveled using his Irish passport. He admitted that he did not advise the State Department at the time he was recognized as a dual citizen. He did not recall if he had told his supervisor at the time that he was applying for recognition as an Irish citizen. When questioned if he had informed any official in the State Department he stated: “Not in a proactive way. I would have informed them on the next security update or any, for example [official governmental] forum, which came down the road about five years later for the position in [Country M].”⁴¹ Applicant provided a “declaration of alienage” to relinquish his Irish citizenship.⁴² His Irish citizenship was terminated on October 15, 2008. Copies of his current and expired Irish passports were provided.⁴³ Applicant testified he surrendered his Irish passport to the Irish authorities, but did not provide documentation of his surrender or verification of such.⁴⁴

³⁸ Tr. 310-313, 324, 336-338.

³⁹ Tr.II 36.

⁴⁰ Answer to SOR.

⁴¹ Tr.II 86-89, 93-94.

⁴² AE D. This document does not verify that Applicant’s passport was surrendered, but it does verify his Irish citizenship has been terminated.

⁴³ GE 23 and 24.

⁴⁴ Tr.II 86-89, 91; GE 24. Other than Applicant’s testimony there is no other proof that he surrendered his Irish passport.

The following are the findings of facts for the allegations for which Applicant has denied:

Applicant was interviewed as part of a security clearance update in his office on June 7, 2006, by an investigator from the Office of Personnel Management (OPM). The investigator credibly testified that she uses a list of questions directly from the investigator's handbook and other questions she developed when questioning people. She uses these questions in all of her cases. She took very detailed notes during the interview with Applicant and later used her notes to write a summary of the interview. With regards to all pertinent information she would always make sure she wrote the information down in her notes. Prior to the interview the investigator administered to Applicant an oath which required him to tell the truth and cited the pertinent criminal code citation for violating the oath.⁴⁵ The investigator confirmed that GE 3 was an accurate summary of her interview with Applicant.⁴⁶

The investigator credibly testified that she asks a series of standard questions regarding every employment entry on the security clearance application (SCA).⁴⁷ One of the questions is: "Have you ever committed any security violations or had any disciplinary action taken against you?" When Applicant was asked this question he indicated "he had not." When she asked if he had any disciplinary action, he indicated "he had not." Later during the interview the investigator, as part of her regular procedure, goes over the SCA and re-asks the questions in the document to make sure that the answers have not changed since the date the SCA was completed. She also asks supplemental questions that are required by OPM for each question. She asked Applicant whether he had been investigated by the U.S. government for any reason. Applicant indicated he was currently under investigation by the Federal Bureau of Investigation (FBI). He indicated to the investigator that on the advice of his attorney he did not want to provide any information about the case. He intimated it was an investigation related to a security issue. Applicant also noted that there was a second investigation associated with his present command. He declined to comment on that case also on the advice of his attorney.⁴⁸

Based on being informed of the two pending investigations the investigator testified as follows:

Since it was in direct contradiction to his earlier statements about security violations and his employment, I asked if there w[ere] any other security

⁴⁵ The investigator cited 18 U.S. Code § 1001.

⁴⁶ Tr. 42-50.

⁴⁷ Tr. 52-53. The other questions the interviewer asked were: Have you ever had any problems with your supervisor or coworkers? Have you ever had a negative performance review? Have you ever committed any security violations or had any disciplinary action taken against you?

⁴⁸ Tr. 52-57.

violations that he had not indicated. And he indicated there were a few minor ones when he was employed with the State Department and located [in various overseas locations], I believe. And he stated those were minor security violations that did not result in any compromise of any sensitive information. And he provided that those were mostly instances of him leaving documents on his desk in a secure location and that the Marine security guards, the MSGs⁴⁹ at the [places] would do sweeps for classified information and if they found it on his desk, they would report it to their supervisor.⁵⁰

The investigator testified when a subject indicates he had a security violation she asks, as part of her regular procedure, for the details, including the dates, if there was a compromise, and if there was any disciplinary action. She asked Applicant those questions. She testified:

Well, he provided as much information as he could recall. He couldn't recall specific dates. He did provide the type of violation as I described and that there was no compromise [of] sensitive information. And when I asked about disciplinary actions, he said that he could not recall any disciplinary actions being taken against him regarding those security violations.⁵¹

The investigator then proceeded to ask standard wrap-up questions. She would ask one general question as it is stated on the SCA. She stated she asked "if there is any information that they think would be pertinent to our case that we haven't gone over that they would like to disclose to the government at this time." Applicant indicated he had no further information.⁵²

The investigator confirmed that during her interview with Applicant she questioned him twice about disciplinary actions. Asking him, "Once for every employment and then again after he gave me the information about the investigations on him." His response was the first time that he did not have any disciplinary actions and at the end when we were discussing the earlier security violations he indicated he "could not recall any disciplinary actions."⁵³ When questioned further about the FBI and command investigation, he did not indicate any other investigations he had been

⁴⁹ MSG are the initials for "Marine Security Guard."

⁵⁰ Tr. 57-58.

⁵¹ Tr. 58.

⁵² Tr. 59.

⁵³ Tr. 60.

involved in.⁵⁴ He did not divulge the investigation regarding his misuse of a government-issued computer and the disciplinary action taken.⁵⁵

As part of the investigator's follow-up investigation, she was provided access to Applicant's State Department file and discovered he had security violations that led to disciplinary actions and an investigation regarding his misuse of a government-issued computer.⁵⁶

The investigator acknowledged that she had advised Applicant that her interview was for a periodic update to his security clearance.⁵⁷ Applicant testified he believed the update covered the past five years.⁵⁸ The investigator confirmed that the specific questions she asked Applicant were "[D]id you receive any disciplinary actions while you were with said employer, the State Department? And did you commit any security violations while you were with the State Department?"⁵⁹ Applicant readily acknowledged the two pending investigations with the FBI and the command.⁶⁰

The background investigation conducted on Applicant was his first Department of Defense investigation. The investigator acknowledged that Applicant should refer back ten years. She acknowledged that often times she would not have access to State Department or FBI records of investigation, so she would go back ten years. The investigator credibly testified she questioned Applicant about any past disciplinary action he may have received. She stated, "There was no time limit on that because we cover the entire span on someone's employment when it is a single employment. I said did you ever have any disciplinary actions, security violations, negative performance appraisals, etc. . . ." She could not remember specifically if she used the word "ever" but she was certain that she used the word "any."⁶¹

The investigator confirmed that Applicant never admitted during his interview that he was disciplined for security violations and he also never divulged his more recent disciplinary action for misuse of a government-issued computer.⁶² She confirmed that she asked a general question to the effect of while you were employed at the State

⁵⁴ Tr. 61.

⁵⁵ *Id.*

⁵⁶ Tr. 61-62.

⁵⁷ Tr. 65.

⁵⁸ Tr. II 21.

⁵⁹ Tr. 69.

⁶⁰ Tr. 70.

⁶¹ Tr. 80-83.

⁶² Tr. 86-87.

Department were you subject to any disciplinary action?" Applicant indicated he was not.⁶³ The investigator was confident Applicant understood the question.⁶⁴

Applicant testified that he remembered his interview with the OPM investigator, but he had a poor recollection of the specifics. He testified his main concern was how to address the two on-going investigations. He remembered that part of the interview, but with regard to his overall recollection he stated "To the best of my recollection I want to emphasize again that my recollection is very fuzzy about that entire interview."⁶⁵ He confirmed he did not have a clear memory of the questions and answers during the interview about his security violations with the State Department. He did not take notes on the interview. He did not recall denying that he had security violations. He did not have any specific recollection about the investigator asking him about any disciplinary actions. He stated:

I may have misunderstood her question. Perhaps it was not posed precisely as she said it was in her notes. I don't know. Could have discussed the fact that I have not suffered adverse consequences in my career, heretofore as a result of these security violations and the reprimands and suspensions.⁶⁶

He went on to say:

So from my point of view, I didn't suffer adverse consequences as a result of this record and I may, given what her testimony, that may have been what I was responding. But I do not have specific recollection of any part of the interview other than the two investigations that I had focused on and that I had thought in advance about how I would address those in the discussion with her.⁶⁷

Applicant could not "recall" or "recollect" most of the specifics of his interview with the investigator. He said he does not have any reason to dispute her testimony or agree with it.⁶⁸ However, he did remember that he did not divulge his investigation about

⁶³ Tr. 87-92.

⁶⁴ Tr. 42-100. The transcript at these pages records the entire testimony of the OPM Investigator. Repeatedly throughout her testimony she confirmed that she requested but Applicant did not divulge that he had prior disciplinary actions by his previous employer, the State Department. He did not divulge the investigation regarding his misuse of a government-issued computer. She was asked many questions in different forms and different ways and her answers remained consistent.

⁶⁵ Tr. II 124.

⁶⁶ Tr. II 20-28.

⁶⁷ *Id.*

⁶⁸ Tr. II 123.

misuse of a government-issued computer because it was in his view not a security matter.⁶⁹ He stated:

Well I may have been in error in not considering the misuse of the computer in the way I did misuse it as relating to security, but that was my view at the time. Now that I've been in this procedure and I've seen all the different criteria that are being applied in the case in DOD documents, I understand the relevance of it. This was not my situation when I was interviewed by [investigator]. I didn't know about these criteria, my judgment was that this was not a security related matter and that I did not need to disclose it.⁷⁰

In response to a question whether the interviewer said anything to lead him to believe that she was only focused on security matters, he responded:

I don't have a clear enough recollection of the exchanges between the two of us to assert that. But it was a security update, she was an investigator for my security clearance, I did not think that that misuse of the computer is relevant. I now know there are criteria which make it relevant, I did not realize that at the time.⁷¹

Applicant then testified that when he was asked a general question about whether there was anything else that was relevant concerning his security clearance, he did recall this part of the interview, but did remember that he volunteered the information about the two ongoing investigations by the FBI and other local command investigation.⁷² Applicant could not recall if he advised the investigator about his disciplinary suspensions or the letters of reprimand he received.⁷³

Applicant was asked the following question by his attorney and his response is provided:

Q. Did you know when you were interviewed by [OPM Investigator] in June of 2006 that she would find out about [country] or the [country] computer incident if she looked at your State Department files?

A. I wasn't sure because these were personnel files and not security files. So I didn't know that—whether she would have access to personnel files. Certainly, she would have access to the files contained—

⁶⁹ Tr. II 126.

⁷⁰ Tr. II 127-128.

⁷¹ Tr. II 129.

⁷² *Id.*

⁷³ Tr. II 129, 189.

that diplomatic security had, which dealt with the security violations in the embassies. But, diplomatic security was not part of the process on the misuse of the computer, it was a panel composed just of personnel and legal.⁷⁴

I find Applicant's testimony was not credible or believable. Applicant clearly had selective memory and his responses were evasive. I find Applicant intentionally failed to fully divulge his past security violations, disciplinary actions, and investigations.

While serving in a high level position overseas Applicant had a foreign national (FN D) who worked for him. While working for Applicant FN D held a security clearance, granted through his country. Applicant had both a professional and personal relationship with FN D and considered him to be a subject matter expert in an important area of international significance and a valuable employee. Applicant was advised in June 2005 by higher authority that FN D's security clearance was revoked by his country. Applicant was told by FN D that the revocation was due to a technical issue and would be resolved. When FN D's security clearance was revoked it also revoked his employment contract because his position required a security clearance. Applicant was aware once a security clearance is revoked a person is not to have access to classified information. Applicant denied knowing FN D had access to classified material.⁷⁵

Applicant personally advocated and requested that FN D be rehired, but with a contract that did not require access to classified information. He testified that his goal was to rehire FN D because he believed FN D would be vindicated and then could resume the position he had previously held.⁷⁶ He further testified that he personally told FN D that his contract work was only to involve unclassified material. He stated he communicated this to the Chief of Staff of the command (COS-M) and to his personal Chief of Staff (COS). Not having a security clearance meant that FN D did not have unescorted access to the building where he previously worked. This was the same building where Applicant and his staff worked. Applicant denied any responsibility for ensuring FN D did not have access to classified material beyond advising and delegating this responsibility to his COS to ensure FN D did not have access.⁷⁷ He stated: "I never had concerns that he was getting into classified areas. And I've testified

⁷⁴ Tr. II 185-186.

⁷⁵ Tr. II 135-140. The counterintelligence officer who testified verified that once a security clearance is revoked by the person's country, there is no middle ground. The requirement is that upon a suspension, termination, or revocation, the individual's employment must be immediately terminated. He emphasized that once a country withdraws a clearance, it is "pretty sacrosanct," and we must "ax them." "There is no middle ground, no wiggle room." The command has no right to request the reason for the revocation as it is a sovereign issue. Tr. 190-196.

⁷⁶ Tr. II 149-151, 154.

⁷⁷ Tr. II 153.

to that fact and I've sworn and affirmed it over and over again. I was not aware he was getting into classified material."⁷⁸

Applicant's COS raised his personal concerns with Applicant about the arrangements for FN D to remain in the same office he had occupied prior to losing his security clearance and his job. He also was concerned that FN D was attending weekly staff meetings. Applicant acknowledged that the COS raised the concerns, but believed it was only once or twice, instead of the numerous times that the COS claimed he raised the issues. Applicant confirmed that the COS did not think it was right for FN D to be working on the contract because his security clearance had been revoked. He stated the staff meetings were not classified. Applicant testified he believed FN D was working on an unclassified project and he believed FN D would be vindicated and his clearance reinstated. He acknowledged he did not personally inform his staff that FN D's security clearance had been revoked; rather he relied on his COS to ensure compliance with his directions. He also acknowledged that no announcement went out telling others in the command that FN D no longer had a security clearance, even though he was working in the same building, in the same office, and for the same people. Applicant was unaware of any efforts made to make an announcement and he did not personally do so. When FN D came to his private office he did not verify if he was being escorted.⁷⁹

Applicant admitted that he was attempting to establish a temporary position and a permanent position for FN D. He was working with the personnel office to write up a position description and the required qualifications. FN D was contacting the personnel office and advising them what the qualifications should be to hold the position. This position was to be advertised so others could compete to be hired. In effect, FN D was providing input on a position he was going to apply for. Applicant sat on the selection board for the position. Regarding a certain person who applied for this position, Applicant stated that FN D "may have" provided me input on this particular applicant based on the applicant's paperwork, but he was not part of the interview process. This person was not selected. Applicant confirmed that FN D had input into writing the position description and it was designed for him to get the job. Applicant believed as long as the description and qualifications were valid for the position it was okay. Applicant did not believe these actions were subverting the system or that it was improper for FN D to be involved.⁸⁰

FN D continued to occupy the same office he had prior to the revocation of his security clearance. He continued to attend some classified briefings and meetings

⁷⁸ Tr. II 153.

⁷⁹ Tr. II 149-157.

⁸⁰ Tr. II 163-168. The compliance and violation of personnel and administrative rules are not at issue in this case and are not considered for disqualifying purposes. The facts related to this area, however, will be considered when analyzing the whole person and credibility issues. GE 48 indicates a lengthy email correspondence on the efforts by the Applicant and those acting on his behalf to retain FN D as a full time employee.

because those in attendance had not been advised that his security clearance was revoked. He produced weekly summaries on his particular area of expertise sponsored by Applicant's office that included sensitive, restricted, confidential or classified information and listed himself as the author on the weekly summaries.⁸¹ Applicant confirmed if he was in the office he would approve the weekly summaries before they were published. If he was not available the COS would handle it. He stated "I didn't pay attention to the classification markings on each of the individual paragraphs. I reviewed those documents for substance, not for format, not for classification. That was COS' responsibility."⁸² In addition, point papers were prepared by FN D that noted the classification as "restricted" material. On the point papers FN D included his title, which was the same title he held prior to having his contract terminated and his clearance revoked.⁸³

Applicant admitted he "misplaced" his trust in FN D. He stated:

And had I realized the extent to which he was prepared to violate the rules, I would never even have contemplated allowing him to stay, but I had no reason to believe that and I had faith and confidence in him and it turns out to have been mistrusted, or misplaced, I beg your pardon, And I regret that very much, Yes, in retrospect, my supervision should have been more careful in this regard and I wish that I had been more careful to have avoided these problems.⁸⁴

Applicant denied he condoned or permitted access to classified material to FN D. Applicant believed he fulfilled his security obligations by delegating them to his COS.⁸⁵

A high level inquiry was conducted concerning FN D's access to classified information. The inquiry was completed by two senior personnel security and counterintelligence officers.⁸⁶ Some of the findings of the inquiry are as follows:⁸⁷

⁸¹ AE 30, 31, 32, 33, 34, 35, and 36.

⁸² Tr. II 140.

⁸³ AE 37-40.

⁸⁴ Tr. II 183.

⁸⁵ Tr. II 184.

⁸⁶ It is noted that the counterintelligence officer who was one of the two who prepared the report testified to its accuracy. The original report, which was classified, was signed by him. The difference between the classified and unclassified reports is that the classified version uses the actual names of the individuals and was signed. This witness testified that he specifically used the term "inquiry" vice "investigation" due to the sensitive political and international ramifications of the issues. I have not included all of the findings of the report, although they are included in GE 20. I have only included those that specifically pertain to the issues of this case and Applicant. I have also made independent findings of facts from the testimony of the witnesses, Applicant, and all of the other evidence presented and considered all of it. The witness provided a lengthy explanation as to how the inquiry was conducted,

- “In June 2005, Subsequent to [Security Office] notification of [command] that FN D’s security clearance had been revoked, [command] took appropriate steps to terminate FN D’s access to ...classified information and FN D’s employment (E.g. FN D’s ...access was terminated and FN D’s Class II security area building access pass was confiscated.)
- “Circa August/September 2005, at the behest of the [Applicant], FN D was returned to employment at [command] as an ‘unclassified consultant.’”
- “However, FN D was effectively returned to the same duty position within the same office of a Class II secure area.”
- “No one outside of the Command Group and FN D’s direct co-workers was informed of the fact that FN D had no security clearance.”
- “As a result, FN D continued to be the recipient of . . . classified information. The information ranged from ...RESTRICTED to . . .SECRET, and was provided to [different commands and headquarters].”
- “Approximately one linear meter of ...classified documents was discovered in FN D’s office. The majority of these documents were originated prior to the revocation of FN D’s security clearance. However, upwards of 20-25% of the documents were originated subsequently to the revocation of FN D’s security clearance.”⁸⁸
- “Although the [Applicant] instructed [COS] to ensure that FN D had no access to classified information, this was done to present the illusion of compliance with ...security relations.”
- “[COS] indicated that the [Applicant] was knowledgeable that [FN D] continued to have access to classified information, and in some cases authorized such access.”
- “In fact, [FN D] continued to produce classified materials, to include the ...Weekly Summary, at the ...Restricted and ...Confidential level and they were distributed to the [Applicant]. These documents were clearly marked with classification markings and indicated [FN D] as the author. The ...Weekly Summary was disseminated to the [Applicant] and the Command Group,⁸⁹ as well as places on the ... classified LAN.”
- “FN D’s continued physical presence in a Class II security area⁹⁰ without a valid security clearance constituted a violation of ...Security Regulations. Additionally,

including interviewing between 50-60 people, searching and seizing documents from FN D’s office, viewing computer hard drives, etc. Tr. 199-202.

⁸⁷ Tr. 205-207. The witness also verified that GE 21 and 22 are the security regulations that were applicable during the time of the inquiry.

⁸⁸ This information was confirmed by the counterintelligence officer at the hearing. Tr. 202-203. Some of the documents seized are GE 30-40. The classified information that appeared in the document has been redacted.

⁸⁹ Tr. 142-143. The Command Group is made up of the highest ranking officers in the command.

⁹⁰ Tr. 143. A Class II secured area requires personnel to have a security clearance or be escorted at all times.

no effort was made to remove [FN D's] previous classified holdings from [his] office prior to [his] reoccupancy of this work space.”

- “... classified documents at the ...RESTRICTED⁹¹ and ...CONFIDENTIAL [level] were produced on an Unclassified Internet enabled computer by [FN D].”
- “[FN D] also continued to attend ... classified meetings and conferences albeit without the knowledge of the chairs of these fora that [FN D] had no security clearance.”
- “A number of [FN D's] co-workers admitted to providing [FN D] classified information with at least some level of knowledge that [FN D] had no security clearance. However, the general claim of his co-workers was that they were never informed that [FN D's] security clearance was removed, but rather that there had been an administrative error with [his] security clearance that would be corrected shortly.”
- “[COS] admitted that [he] had been informed that [FN D's] security clearance had been removed, but also stated that the [Applicant] indicated that this was an administrative oversight on the part of the ...authorities. As such, the [Applicant] indicated to [COS] that [FN D] should continue to have access to relevant classified information necessary for [FN D] to work on [subject operation] and [subject project]. [COS] indicated that as time progressed, both the staff of [Applicant's] office and [COS] became increasingly uncomfortable about [FN D's] lack of security clearance. As such, [COS] claimed to have discussed this issue with [Applicant] on a number of occasions. When the [Applicant] did not react, [COS] informed [COS-M] in January or February 2006.”⁹²
- “Interviews of numerous individuals found that most were unknowledgeable of [FN D's] security clearance status, and as a result, were unable to precisely indicate what specific classified information was provided to [FN D].”
- “However, the inquiry determined that [FN D] was involved in a diverse range of classified areas. For example, [FN D] was involved with”
- “Numerous individual's claimed to have raised their concerns about [FN D's] access to classified information with the [Applicant]”
- “On 9 March 2006, [FN D] telephoned investigators and requested to meet with investigators.” (Additional information is contained in the report that is not specifically pertinent.)
- “[FN D] stated from June 2005 until February 2006, that [he] worked as an unclassified consultant with no access to classified information. When asked about classified documents in [his] office, [FN D] could offer no explanation. When asked about receipt of classified information subsequent to the revocation of [his] security clearance, [FN D] could offer no explanation.”

⁹¹ Tr. 212-213. “Restricted” by definition from the Treaty is a security classification and is considered classified information.

⁹² Tr. 125-126. COS-M testified that he recalled that COS came to his office to discuss FN D. He stated he did not remember the specifics of the conversation, but believed it had to do with what level of access FN D should have. He stated his direction was that FN D should have unclassified access and have escorted access to the building.

An additional note was made in the report that stated the following: “Historically, both [COS-M] and [Applicant] routinely made extraordinary efforts for FN D.” Examples of such are included in the report.⁹³

The conclusions of the inquiry are as follows:

- “[Command] created conditions that resulted in a major compromise of ... classified information to FN D.”
- “Actions on the part of [COS-M], and the [Applicant], U.S. national, to accommodate the continued employment of [FN D], following the revocation of his national security clearance, violated the intent of both the ...Security and Civilian Personnel Regulation, and were the direct cause of [FN D’s] continued and routine access to ... classified information.”
- “The manner in which [FN D] was subsequently employed constituted a direct and deliberate violation of ... Security Regulations.”
- “[COS] allowed [FN D] continued access to ...classified information with the knowledge that [FN D] had no security clearance. However, [COS] did so with the informed consent and under the implied direction of [Applicant].”⁹⁴
- “[Applicant] was undoubtedly aware of [FN D’s] continued access to classified information without a security clearance, although [Applicant] denied any such knowledge.”
- “The actions on the part of the [Applicant] placed the subordinate members of his office at serious risk of violating national espionage statutes involving the mishandling of classified information.”
- “The full extent of the magnitude of the compromise is impossible to determine and, as such, a damage assessment cannot be conducted.”
- “Lastly, although not a part of the ...inquiry, “[COS-M]” and [Applicant’s] actions relative to FN D were part of a clear and continuing pattern to violate ...rules on FN D’s behalf; to include violation of ...Civilian Personnel Regulations, ...Security Regulations, ... Financial Regulations and possibly ... Contracting Regulations.

⁹³ Testimony by the counterintelligence officer confirming his findings in the inquiry are located at Tr. 209-291. Additional findings are included in the report regarding the irregularities in the personnel hiring regulations.

⁹⁴ At the hearing the counterintelligence officer explained that this finding meant that COS had complained to Applicant as time progressed and that his staff was, in turn, complaining to COS and that the implied direction is the instruction from Applicant to ensure FN D has everything he needs to do his work on a specific operation. In addition, COS as well as others in Applicant’s office were aware that FN D was attending classified meetings and this was allegedly conveyed to Applicant. It was confirmed that COS had a responsibility to ensure FN D was restricted to only unclassified information and that he be restricted while in the building. The counterintelligence officer’s report confirmed COS permitted FN D access to classified information and the COS’ contention was he was acting on the implied consent of COS M and Applicant. Tr. 254-258.

Also, the civilian recruitment process was corrupted in an extraordinary effort to create a civilian position that was solely designed to be occupied by FN D.”⁹⁵

The final conclusion of the in-depth inquiry was as follows:

The final conclusion of the inquiry should indicate that [COS-M] and [Applicant] were responsible for creating the conditions that resulted in a major compromise.⁹⁶ [COS], while not blameless, should not be singled out as the primary responsible party.

The counterintelligence officer who conducted the inquiry confirmed that FN D had access to classified information after his clearance was revoked.⁹⁷ He confirmed that he met with the country representatives that had originally authorized a security clearance to FN D and they were outraged because they believed the [Command] was non-responsive to their national decision and that both COS-M and Applicant had both provided memorandums of support for FN D in his legal battle, which they viewed as an interference in a national judicial matter.⁹⁸ I find the counterintelligence officer’s testimony credible.

Applicant denied he was aware of the situation or responsible as outlined above.⁹⁹ I find Applicant’s testimony was evasive, not credible and not believable.¹⁰⁰

⁹⁵ GE 20. It is noted that some of the findings and conclusions of the inquiry are not considered for disqualifying purposes, but are considered in the whole person analysis and to show the relationships between the different people, a pattern, credibility, and a course of conduct. Conduct not alleged in the SOR may be considered: “(a) to assess an applicant’s credibility; (b) to evaluate an applicant’s evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether an applicant has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for whole person analysis.” ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006) (citations omitted).

⁹⁶ COS-M testified at the hearing. COS-M was asked if while attending a high level meeting whether the command’s legal advisor advised the Commander and others at the meeting that FN D’s continued unescorted presence in [Class II secured spaces] was a violation of ... security regulations. COS-M’s response was “She may have done but I cannot remember.” Tr. 145. He also stated that he did not read the weekly summaries thoroughly, but rather skimmed them and did not notice anything that FN D had written that may or may not have been classified. Tr. 146.

⁹⁷ TR. 196.

⁹⁸ Tr. 197-198. Although the issue of interference in a nation’s sovereignty is not at issue in this case, this information is relevant in analyzing the relationships and actions by Applicant during this time.

⁹⁹ COS-M was asked if during the time in question if he was “aware of any circumstances or any situation where FN D accessed, or used, or discussed, or developed classified information.” His answer was “I was not actually aware of that practice, no.” Regarding whether he was aware if Applicant allowed or permitted the access of classified information by FN D, he answered “no, I was not and I would have been highly surprised had I become aware of it.” He was further asked if anyone complained to him about FN D accessing classified information or possessing classified information. He stated “There was one occasion, and I could not tell you when it was, COS did come up to my office and my aide opened the door and the three of us stood in my doorway and discussed it. And I reaffirmed the absolute intent, which

Applicant submitted character statements from two high ranking supervisors. One supervisor wrote that, despite the allegations in the SOR, they “bear no resemblance” to Applicant, with whom he worked closely with for two years. He considers Applicant honest, trustworthy and reliable, and never doubted his loyalty. He referred to Applicant’s constant exposure to highly classified documents and being entrusted with the most sensitive information during certain negotiations, and at no time did he witness or hear that Applicant jeopardized that trust. He went on to say, “I can state unequivocally that he upheld the highest standards for handling classified material during our service together”.¹⁰¹

A second supervisor characterized Applicant as one of his most “invaluable advisors.” He was relied upon for his “expertise, his insightful analysis, and his sound judgment.” He has his fullest faith, trust and confidence in his “fidelity and loyalty to the United States of America, and I trust him to represent me personally before heads of state.” He confirmed that he is aware of the allegations against Applicant and believes they are inconsistent with his character and do not cast doubt on his opinion of Applicant.¹⁰²

COS M testified Applicant’s loyalty to the U.S. is absolute and faultless. He commented on Applicant’s devotion to his work and his strong work ethic.¹⁰³

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, “no one has a ‘right’ to a security clearance.”¹⁰⁴ As Commander In Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information.¹⁰⁵ The President has authorized the Secretary of Defense or his

was shared in the Command Group, that FN D was denied access to anything above unclassified. His [access] account was closed and his access to the building was on an escorted basis.” COS-M could not remember if COS raised the issue that he believed FN D did possess or have access to classified information. He denied he permitted FN D to attend classified meetings. Tr. 125-126. COS-M could not recall being made aware that the continued contractual hiring of FN D on five successive contracts was in violation of civilian personnel regulations. Tr. 155-164.

¹⁰⁰ I have made independent findings based on all of the evidence presented, including the testimony of all of the witness and consideration of all of the documentary evidence.

¹⁰¹ AE B. I have considered the entire statement.

¹⁰² AE C. I have considered the entire statement.

¹⁰³ Tr. 131-132.

¹⁰⁴ *Department of the Navy v. Egan*, 484 U.S. 518 (1988).

¹⁰⁵ *Id.* at 527.

designee to grant applicant eligibility for access to classified information “only upon a finding that it is clearly consistent with the national interest to do so.”¹⁰⁶ When evaluating an applicant’s suitability for a security clearance, the administrative judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an Applicant’s eligibility for access to classified information.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the revised adjudicated guidelines (AG). These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge’s over-arching adjudicative goal is a fair, impartial and common sense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information. Clearance decisions must be “in terms of the nation interest and shall in no sense be a determination as to the loyalty of the [A]pplicant concerned.”¹⁰⁷ Thus, nothing in this decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant’s allegiance, loyalty, or patriotism. It is merely an indication Applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the government must establish, by substantial evidence, conditions in the personal or professional history of the Applicant that may disqualify an Applicant from being eligible for access to classified information. The government has the burden of establishing controverted facts alleged in the SOR.¹⁰⁸ “Substantial evidence” is “more than a scintilla but less than preponderance.”¹⁰⁹ The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant’s security suitability.¹¹⁰

¹⁰⁶ Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

¹⁰⁷ See Exec. Or. 10865 § 7. See also Executive Order 12968 (Aug. 2, 1995), Section 3.

¹⁰⁸ See *Egan*, 484 U.S. at 531.

¹⁰⁹ See *v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994).

¹¹⁰ See ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts.¹¹¹ An applicant “has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance.”¹¹² The burden of disproving a mitigating condition never shifts to the government.¹¹³ “[S]ecurity clearance determinations should err, if they must, on the side of denials.”¹¹⁴

Analysis

Guideline C, Foreign Preference

Under AG ¶ 9 the security concern involving foreign preference arises: “When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.”

AG ¶ 10 describes conditions that could raise a security concern and may be disqualifying: I have specifically considered AG ¶ 10 (a) (“exercise of any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member”), including but not limited to (“possession of a current foreign passport”) and (b) (“action to acquire or obtain recognition of a foreign citizenship by an American citizen”). Applicant applied for and obtained recognition of dual citizenship with Ireland while serving as a State Department employee. He retained an Irish passport from 1991 until 2008. I find both disqualifying conditions apply.

I have considered all the mitigating conditions applicable to this guideline. Specifically I have considered AG ¶ 11 (a) (“dual citizenship is based solely on parents’ citizenship or birth in a foreign country”); (b) (“the individual has expressed a willingness to renounce dual citizenship”) and (e) (“the passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated”). Applicant’s dual citizenship status is based on his affirmative actions to be recognized as a citizen of Ireland. I find (a) does not apply. Applicant provided a document to support his renunciation of his dual citizenship status with Ireland. He stated he was required to relinquish his passport. He did not provide documentation to show that he actually did relinquish it. However, under the circumstances I find it is likely he did relinquish it.¹¹⁵ Therefore, I find (b) and (e) apply.

¹¹¹ Directive ¶ E3.1.15.

¹¹² ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

¹¹³ See ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

¹¹⁴ *Egan*, 484 U.S. at 531; See AG ¶ 2(b).

¹¹⁵ It is troubling that Applicant applied for and retained dual citizenship while serving in high level positions in the State Department and did not advise or request permission from his superiors prior to

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information: “Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual’s trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.”

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. I have specifically considered (a) (“deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences”); (c) (“loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, “palm” or pocket device or other adjunct equipment”); (e) (“copying classified or other protected information in a manner designed to conceal or remove classification or other documents control markings”); (g) (“any failure to comply with rules for the protection of classified or other sensitive information”); (h) (“negligence or lax security habits that persist despite counseling by management”) and (i) (“failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent”).

Applicant has a long documented history of security violations and infractions. His irresponsible attitude toward protecting classified information existed from 1978 to 1994. It then remained dormant for a period of years until it escalated to deliberately disregarding security rules and regulations for protecting classified information. His attempt to minimize and mitigate his actions during the early period by explaining he was working for a difficult supervisor, was under a great deal of stress, or had a busy office and was interrupted by someone, is without merit. The repetitive security infractions and violations denote a lack of regard for the importance of his duties with regard to protecting classified information. He was repeatedly counseled about his conduct after each infraction or violation and received not one, but two suspensions without pay for his actions.

Applicant has held increasingly more responsible and prestigious jobs in the State Department. With those important promotions came a higher degree of trust, responsibility and access to classified material and awareness of security rules. Perhaps his earlier infractions and violations could have been mitigated by time, but instead Applicant escalated his irresponsible attitude and lack of adherence to the rules, by deliberately downloading a “SECRET” document from a classified computer, placing the information on a disc and then removing the “SECRET” classification markings, and emailing it on an unclassified computer to Officer B, without first confirming if Officer B

obtaining this status. He acknowledged it was likely that he provided information about his dual citizenship years later when he provided this information during a routine update.

still retained a security clearance. He does not know what happened to the disc on which the classified document was downloaded, as he gave it to his assistant. He acknowledged his wrongful actions. Applicant's access to SCI was denied due to security concerns and security violations. It was also determined that the information was to be used at a conference where foreign nationals were present. Applicant acknowledged that this document is the type that contained the "U.S. position of current events in the country", "a suggested way forward", "next step in the key elements and assumptions", "engagement strategy" and an annex with a time line.

Applicant was in a high level position of trust and responsibility during his last job with the State Department and then when he became a contracted employee with the same command. He was responsible for ensuring FN D did not have access to classified information. His abdication of his ultimate responsibility to ensure FN D did not have any access to classified information is confirmed. His denial that he did not know FN D had access to classified information is not believable. The overwhelming evidence is that he was actively involved with FN D at many levels. He received weekly updates from FN D that showed FN D had access to classified material. I find Applicant was an active participant in the process that violated the security rules. I find Applicant was personally, deliberately and intimately involved and aware that FN D had access to classified information. I find Applicant knowingly and deliberately permitted FN D access to classified information. His testimony with regard to this issue was evasive and not believable. His attempt at passing all responsibility onto COS is also not believable. I also find that, even if one were to believe the facts as presented by Applicant, he merely gave the order and then was totally unaware that FN D continued having access to classified information. He never noticed weekly summaries or point papers to the contrary, or never heard complaints from his subordinates. Even if viewed in the most favorable position to Applicant, he did not act responsibly as FN D's supervisor to ensure all classified material was protected. Even if Applicant were to be believed that he did not know what was going on, at some point, COS addressed the situation with him and he did not take appropriate action. He basically ignored all information that there was something terribly wrong happening.

I find Applicant's actions as noted above were deliberate and negligent. I find (a), (c), (e), (g), and (h) all apply. Although there was evidence that classified material was compromised there was no direct evidence that National Security was breached, and therefore (i) does not apply.

I have considered all of the mitigating conditions applicable to this guideline. Specifically I have considered AG ¶ 35(a) ("so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual currently reliability, trustworthiness, or good judgment"); (b) ("the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities") and (c) ("the security violations were due to improper or inadequate training"). Applicant has a history of security violations starting in 1978. He had 21 security violations and infractions from 1978 to 1994. He

admitted he was counseled about the violations. He received two suspensions without pay. He then committed two very serious violations, one deliberately changing classification markings on a classified document and transmitting it on an unclassified computer to a person he had not verified as retaining a security clearance and another event where he allowed a person to have access to classified information for a significant period of time, after his security clearance was revoked. Applicant has exhibited a 28-year history of security violations that escalated in seriousness and ultimately compromised classified information. Despite counseling and suspension his attitude did not change. He has not demonstrated a positive attitude toward the discharge of security responsibilities, but rather has ignored his own personal accountability and abdicated and abused his supervisory responsibilities. It is undeniable that Applicant has had a prestigious and successful career serving his country, and that he is respected and admired for his experience and aptitude. However, there is also a prevalent and troubling attitude and disregard for the importance of following security rules, even at the highest levels, in essence that the “end justifies the means”, which is dangerous when one has a duty to protect classified information and is in a high position of trust and authority. He has repeatedly reflected irresponsible conduct and has been personally responsible for security violations. I find none of the mitigating conditions apply.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern pertaining to personal conduct: “Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.”

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. I have specifically considered (b) (“deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative”) and (e) (“personal conduct, or concealment of information about one’s conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person’s personal, professional, or community standing..”). Applicant admitted that he viewed and downloaded sexually explicit images and permitted a guest to access sexually explicit websites on a government-issued computer. He stated he believed the government-issued computer was for his personal use. Based on all of the evidence I did not find his statements believable. The computer had a pop-up government banner warning about its proper use. Other evidence presented at his hearing showed he was aware that he was using a government-issued computer, but he attempts to mitigate his actions by explaining he was only using it at his residence. He acknowledged he was embarrassed by his actions. I find (e) applies with regard to his actions of viewing and downloading sexually

explicit images and websites and allowing his guest to inappropriately use a government-issued computer.

Applicant denied he falsified material facts when he told the OPM investigator that he could not recall suffering any disciplinary actions as a result of his past security violations. At first during his interview with the OPM investigator he denied any security violations, but then later mentioned he had some earlier in his career. It is simply inconceivable that he would “not recall” that he was suspended without pay twice, once for sixteen days and again for ten days. These disciplinary actions are extraordinary events in one’s professional life, and Applicant’s assertion that he could “not recall” is simply not believable. He was asked about any disciplinary consequences in his past and could not recall any. Even if he believed he only had to divulge disciplinary actions regarding security violations, he failed to do so. Even if he only believed he had to divulge disciplinary actions within the past five years, he did not divulge his suspension for misuse of a government-issued computer in 2004. Applicant did not dispute the OPM investigator’s testimony; he simply could not recall or recollect what had occurred. I found her testimony credible. I find Applicant deliberately provided false and misleading information about his past violations, both security-related and otherwise, and his past disciplinary actions. Therefore, I find (b) applies.

With regard to SOR ¶ 2.c, Applicant provided a written response to DON CAF denying his involvement in allowing an employee (FN D) access to classified information. I have found, based on the entire record, that Applicant knowingly and intentionally allowed FN D access to classified information and the computer system. My analysis is provided above. Therefore, I find (b) applies.

The guideline also includes examples of conditions that could mitigate the security concerns arising under personal conduct. I have considered all of them and especially considered AG ¶17 (a) (“the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts”); (c) (“the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual’s reliability, trustworthiness, or good judgment”); (d) (“the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused the untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur”); (e) (“the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress”) and (f) (“the information was unsubstantiated or from a source of questionable reliability”). Applicant’s testimony throughout the proceeding was troubling. On one hand he denied providing false statements. On the other hand he could not recall any of the pertinent parts of the interview with the OPM investigator, yet he could recall why he decided he did not have to divulge certain negative incidents in his past. I found the OPM investigator’s testimony credible. I found Applicant’s testimony was not credible. I find none of the mitigating conditions apply.

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems: “Noncompliance with rules, procedures, guidelines, or regulations, pertaining to information technology systems may raise security concerns about an individual’s reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.”

AG ¶ 40 describes conditions that could raise security concerns and may be disqualifying. I have considered all of them and especially considered (d) (“downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system”); (e) (“unauthorized use of a government or other information technology system”); (g) (“negligence or lax security habits in handling information technology that persist despite counseling by management”); and (h) (“any misuse of information technology, whether deliberate or negligent, that results in damage to the national security”). The allegations in SOR ¶¶ 1.b and 2.a are cross alleged under Guideline K, handling protected information, and Guideline E, personal conduct. The facts and analysis are the same as addressed above. Applicant admitted he deliberately removed “SECRET” markings from a document and emailed it on an unclassified computer to a person he had not verified had a security clearance. He put the document on a disc, but did not provide information as to the disc’s whereabouts other than to say he gave it to his assistant. In addition, he admitted he inappropriately downloaded sexually explicitly material on his government-issued computer and permitted a house guest to do the same. I find (d) and (g) apply. I find (h) does not apply under these facts as there is no evidence of damage to national security.

I have considered all of the mitigating conditions under this guideline. Specifically I have considered AG ¶ 41(a) (“so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual’s reliability, trustworthiness, or good judgment”); (b) (“the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one’s password or computer when no other timely alternative was readily available”) and (c) (“the conduct was unintentional or inadvertent and was followed by a prompt good-faith effort to correct the situation and by notification of supervisor”). Applicant made a deliberate and conscious decision to violate the security rules and download, copy, change classification markings and transmit classified information over an unclassified computer and internet based system. His behavior is recent and considering his present and past history of violating security rules and misusing information technology, I find it casts doubt on his reliability, trustworthiness and good judgment. His actions in deliberately violating security rules and also his actions of misusing a government-issued computer to download sexually explicit material and allow his guest to do the same are not minor. Even taking the evidence in the light most favorable to Applicant regarding his misuse of

a government-issued computer, when asked how soon after he became aware the government had discovered his violation did he speak with his guest, Applicant stated: "I really don't remember how soon it was." He then was asked if it would have been immediately. He responded "No, I don't think it would have been immediately, but I really don't recall." His conduct and response is troubling. He did not take prompt corrective action regarding his guest's misuse of a government-issued computer. I find none of the mitigating conditions apply.

Whole Person Concept

Under the whole person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the Applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a): "(1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence." Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall common sense judgment based upon careful consideration of the guidelines and the whole person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant has a long and distinguished career with the State Department and has the support of high ranking officers. His loyalty and devotion to the mission is not in question. He has received regular promotions and served at some of the highest and most prestigious positions in our government. He is admired for his unique skills by those for whom he has worked. Among those who provided character statements, he is revered for his work ethic, his knowledge and unquestionable loyalty to the United States.

Applicant has a long history of negligent and deliberate security infractions and violations, beginning early in his career in 1978 and continuing intermittently throughout his career. Some security violations were intentional, serious, involved knowledgeable participation and occurred after Applicant was trained on security matters. He received two periods of suspension without pay for his security violations from 1978 to 1990. In 2001 to 2003, he intentionally accessed sexually explicit websites and downloaded images on his government-issued computer and allowed his guest to do the same. He was counseled and suspended without pay for a ten-day period in 2004 for this offense. In 2005, Applicant knowingly and intentionally permitted a foreign national whose security clearance was revoked and for whom he had direct supervision, continued access to classified information. He intentionally bypassed security rules and abdicated his supervisory responsibilities. In 2006, Applicant again deliberately and intentionally violated the security rules by personally downloading a classified secret document from

a classified computer, removing the secret classification markings, then transmitting it on an unclassified computer through the internet to a recipient that he never verified prior to sending the document, was authorized access to classified information. Applicant was a mature and experienced senior official at the time these more recent security violations occurred and when he was officially disciplined for his actions regarding his government-issued computer.

Applicant was interviewed by an OPM investigator as part of his security clearance update and was asked about any prior disciplinary actions he may have had. He knowingly and intentionally failed to fully divulge the extent of his prior conduct or the official disciplinary actions and punishment he received. His testimony at his hearing was untruthful, repeatedly evasive, and lacked candor. He claimed he could not recall many of the specific and pertinent facts regarding incidents he was personally involved in. I have carefully considered all of the evidence and testimony presented at the hearing. I have considered the candor and directness of each witness, as well as their specific testimony. I have considered the nine adjudicative factors when analyzing the whole person and how they specifically related to Applicant. Based on all of the evidence and my analysis above, the record leaves me with serious questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the security concerns arising from handing protected information, use of information technology and personal conduct. Applicant has mitigated the security concerns arising from foreign preference.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	Against Applicant
Subparagraph 2.c:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant
Subparagraph 3.b:	Against Applicant

Paragraph 4, Guideline C:

FOR APPLICANT

Subparagraph 4.a:

For Applicant

Subparagraph 4.b:

For Applicant

Conclusion

In light of all of the circumstances it is not clearly consistent with national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

Carol G. Ricciardello
Administrative Judge