DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-00998
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Stephanie C. Hess, Esquire, Department Counsel
For Applicant: Robin L. Munson, Esquire

12/22/2014

Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant was fired from his previous defense contractor employment for violating security procedures involving an information system and for not being upfront about his conduct during his employer's investigation of the incident. Applicant has an otherwise unblemished record of handling classified information, but his claim of an accidental breach is not persuasive in light of his inconsistent accounts of the incident and other contradictory evidence. Clearance is denied.

Statement of the Case

On June 13, 2014, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K (Handling Protected Information), Guideline M (Use of Information Technology Systems), and Guideline E (Personal Conduct), and explaining why it was unable to find it clearly consistent with the national interest to grant or continue a security clearance for him. The DOD CAF took the action 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 adjudicative guidelines (AG) effective within the DOD on September 1, 2006.

Applicant responded to the SOR allegations on June 28, 2014. He requested a hearing before a Defense Office of Hearings and Appeals (DOHA) administrative judge. The case was assigned to me to conduct a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for him. On August 25, 2014, I scheduled a hearing for September 18, 2014. On September 5, 2014, counsel for Applicant entered her appearance.

I convened the hearing as scheduled. Four Government exhibits (GEs 1-4) and eight Applicant exhibits (AEs A-H) were admitted into evidence without objection. Applicant also testified, as reflected in a transcript (Tr.) received on September 30, 2014.

Summary of SOR Allegations

The SOR alleges under Guideline K (SOR 1.a and 1.b), and cross-alleges under Guideline M (SOR 2.a) and Guideline E (SOR 3.a), that Applicant knowingly and intentionally:

- Plugged a USB drive, which was classified Secret, into an unclassified laptop on January 24, 2011 (SOR 1.a); and

- Used a classified computer, logged in by a co-worker, to transfer classified files from the Secret USB drive (SOR 1.b).

Additionally, under Guideline E, Applicant allegedly refused to cooperate during his then employer's investigation into the security violations (SOR 3.b); was terminated by that employer on March 4, 2011 for the deliberate misconduct set forth in SOR 1.a and 1.b (SOR 3.c); and falsified material facts on his February 2013 Questionnaire for National Security Positions (QNSP) in that while he reported his employment termination for the incident involving the use of the classified USB drive in the unclassified laptop, he did not disclose the use of a then co-worker's classified computer to transfer classified files from the Secret USB drive (SOR 3.d).

When he answered the SOR allegations, Applicant indicated that due to fatigue, acute sinus pain, and the usual workplace distractions, he accidentally plugged the Secret USB drive into an unclassified computer. He denied any inference that his conduct was knowing or willful. Applicant denied that he used a co-worker's computer to transfer the classified information from the USB drive. A team member, who was appropriately logged in and held the requisite security clearance, made the physical transfer, which Applicant reviewed to ensure it had been done correctly, as was his responsibility. Applicant also strongly denied that he was uncooperative during his then

employer's investigation into the incident. He attended every meeting requested by security personnel or management and "[he] answered all questions honestly and thoroughly, to the best of [his] ability." Applicant also indicated that he had not acted to conceal his error in that he reported the incident immediately to the employee responsible for the security of the secure information technology system. Furthermore, Applicant opined that his termination was not justified, as evidenced by his receipt of unemployment compensation and the company's noncompliance with its published discipline procedures, which specified no more than a written reprimand for a first security incident. About his alleged failure to disclose on his QNSP the incident involving the transfer of classified material from the Secret USB drive, Applicant stated in part:

> I deny the accusation that I *deliberately* failed to disclose a second violation but may have unintentionally omitted it because of its relatively low importance. I always considered it to be part of the same incident, as it happened at the same time and location in an effort to complete the same task. What is being referred to as the second security incident was also addressed in a letter of 08.08.11 that my attorney sent to [name omitted], of the Defense Security Service, in a voluntary attempt to keep the Department of Defense informed.
>
> I also did not interpret the instructions to this particular question to mean that the entire event needed to be reiterated in detail as part of the reply, since it was clearly marked as an "optional" comment section.
>
> Furthermore, I chose to focus on the incident with the USB drive, because Raytheon security people told me that they considered the use of a classified computer logged on to by another employee to be minor in comparison.

Findings of Fact

After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is 64 years old and is currently employed as a senior principal design engineer with a defense contractor. He holds a master's degree in electrical engineering, which was awarded to him in June 1984. (GE 1.)

Applicant had ten or more years of employment in the defense industry with a DOD security clearance before June 1, 1999, when he was hired as a principal engineer by defense contractor X. (GE 2; AE G.) On June 3, 1999, Applicant executed a classified information nondisclosure agreement, agreeing not to divulge classified information to unauthorized persons with termination of any security clearance or employment as possible penalties for any breach. (GE 2; AE G.) Applicant's Secret security clearance eligibility was renewed on November 15, 2003. (GE 4.)

Around June 2005, Applicant was promoted to the position of senior principal electrical engineer. By late 2010, Applicant was earning a bi-weekly salary of $5,528. Applicant held security clearance eligibility to the Secret level throughout his tenure at company X, and he had been periodically briefed about his security responsibilities by his employer, which included briefings on the company's Classification Information Systems Security policy. (GE 2; AE G.)

On November 18, 2010, company X issued a security violation alert to employees after an engineer with 19 years of experience conducted an unauthorized and improper trusted download using a personal thumb drive, which resulted in a potential contamination of the company's unclassified network.[1] Employees were specifically advised to never use personal media on any company X system, classified or unclassified; to not rush in fulfilling their duties, and to be clear on the classification level of the systems in their laboratory. Furthermore, they were reminded that trusted downloads may be accomplished only by trained personnel with written authorization, and that those employees with clearances are responsible to understand and follow security procedures and to ask questions if unclear about proper security. The notification also stated:

> Classification markings on documents, media, and hardware serve to provide notice to all that the item is classified and requires approved safeguarding procedures. Regardless of the reason, failure to take notice of these markings and follow proper procedures puts National Security Information at risk.
>
> If you work in a hardware lab within a closed area, you need to be knowledgeable about the equipment in use, its classification, and permitted operations outlined in the System Security Plan (SSP). The SSP also identifies specific procedures related to the information system including the authority to perform a trusted download and the use of encrypted or unencrypted thumb drive. (GE 2.)

On January 24, 2011, Applicant was the lead engineer directing the activities of two engineers involved in testing components and then verifying specifications of a classified system. (AE G.) The work required coordination with an integration group during third shift in a closed, secure area at a facility separate from Applicant's primary duty location. Applicant arrived at the testing site around 2:30 a.m. after working long hours the previous day. (AE B; Tr. 38-43, 51.) Applicant and his co-workers were in the final stage of a project and under time pressure. (Tr. 138.) A few hours later, Applicant needed to transfer classified information from a classified information systems network (source IS network) at the testing site to a classified IS network (destination IS network) at another company facility. The source IS network was accessed through a classified

[1] The engineer was re-briefed by company X security, but there is no evidence of other disciplinary action taken, even though the engineer initially denied that he had connected his personal thumb drive to an unclassified system. (GE 2.)

desktop computer (PC #1). Classified data had to pass through a classified gateway network (gateway IS network), which was accessed through a classified desktop computer (PC #2) at the test site. Applicant was authorized to access the source IS and destination IS networks but not the gateway IS network, although he had requested authorization, which he expected to be routine. (Tr. 54-56.) An engineer (engineer A) on his team at the test site was authorized to access the gateway IS network and PC #2. (Tr. 56.) Whereas the source and gateway networks were not linked, the data from the source IS network had to be transferred by copying the data onto a classified USB drive using PC #1 and then copying the data from the classified thumb drive to the gateway IS network using PC #2. (AE C.)

Audit logs of the source IS network and PC #1 show that PC #1 was logged in under the credentials of engineer A when, on January 24, 2011, classified files were transferred from the source IS network to a Secret USB thumb drive[2] via PC #1 (SOR 1.b). (GE 4.) Applicant claims he directed engineer A to transfer the data using PC #1. (Tr. 57.) Engineer A discrepantly told company X that he may have neglected to lock PC #1 while repeatedly entering and exiting the closed area to run tests, but he denied that he transferred any files for Applicant or that he worked side-by-side with Applicant on January 24, 2011. (GE 4.)

While awaiting authorization to access PC #2 and the gateway IS network, Applicant inserted the Secret thumb drive into his unclassified laptop computer, which was connected to the company's unclassified network (SOR 1.a). (GEs 1-4.) Company X engineers were authorized to bring employer-issued, unclassified laptops into the closed area to access email messages and work on documents. (Tr. 41.) However, the National Industrial Security Program Operating Manual (NISPOM) and company X's security procedures prohibit the introduction of a classified thumb drive into an unclassified laptop computer.[3]

---

[2] The thumb drive was classified Secret with the additional caveat of No Foreign Dissemination (NOFORN). (GE 3.)

[3] Under ¶ 8-105 of the NISPOM, all users of a classified information security system are required to comply with the IS security program requirements; be aware of and knowledgeable about their responsibilities in regard to IS security; be accountable for their actions on an IS; ensure that any authentication mechanisms, including passwords, issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access; and acknowledge, in writing, their responsibilities for the protection of the IS and classified information. Company X implemented the requirements of the NISPOM through published security standards. (*See* GE 2; AEs G, H.) Company security policy effective June 2, 2003, stated in part:

> Only an IS specifically approved by the local Information Systems Security Manager (ISSM) and, as required, the government Cognizant Security Authority (CSA), will be used to process classified information. It is a violation of [company X] policy and government security regulations to process classified information on an IS that has not been specifically approved for processing classified information. (GE 2.)

The classified USB drive was conspicuously marked as Secret by means of an attached 3" x 7" red tag.[4] An engineer with the integrations group (engineer B) noticed the Secret USB thumb drive in Applicant's unclassified laptop. Engineer B observed Applicant to be working on a document on his unclassified laptop while the Secret thumb drive was plugged in. Engineer B removed the classified thumb drive from Applicant's unclassified laptop and confronted Applicant about his reason for improperly inserting a classified drive in his unclassified laptop. Applicant stated to engineer B that he planned on copying a file from his computer onto the Secret USB thumb drive to transfer the file to a Secret PC on the classified source IS network. Engineer B took possession of the classified thumb drive and advised Applicant that he would be reporting the security incident to security. Engineer B notified the onsite Information Systems Security Officer (ISSO) of the incident as soon as he could find the ISSO. At the ISSO's direction, engineer B then unplugged Applicant's laptop from the unclassified network and secured the Secret USB thumb drive in a safe. (GE 4; AE D.) Applicant asserts that he notified the ISSO first ("I talked to him very briefly in the aisle, as I found him."), and that he and the ISSO then discussed the incident for 35 or 45 minutes in the ISSO's office. (Tr. 128.) The ISSO advised Applicant to stay off the IS network. (GE 4.)

Company X's Information Security Manager (ISSM) learned of the incident on January 24, 2011, from the ISSO. The ISSM asked Applicant to explain his conduct, and in a written statement given to the ISSM, he stated in part:

- With authorized assistance, I was using the [Secret USB] thumb drive to make a file transfer between the [source IS network] and the [gateway IS network] when I accidentally plugged the thumb drive into my laptop USB port.

- This was noticed simultaneously by myself and co-worker [engineer B].

- The USB thumb drive remained in the port for about 20 to 25 seconds before it was noticed and removed.

- No files on the thumb drive were accessed or opened, and no files were transferred in either direction.

(GE 4; AEs E, F.) Applicant also met with a company X Industrial Security Specialist (ISS) at the ISS' request on January 24, 2011, to discuss the incident. Applicant claims that the ISS thought there was no cause for alarm and that she was ready to close the investigation. (AE B; Tr. 81-82.)

On January 26, 2011, a company engineer with a Top Secret clearance cleared files from all classified USB drives used by the program to transfer data between IS networks. (GE 4.) On January 27, 2011, engineer B provided a written statement to

[4] Applicant testified at his security clearance hearing that the tag was on a long string. (Tr. 70.)

company X, reporting that Applicant "was working on a document on his work laptop" while the classified USB drive was plugged into Applicant's unclassified laptop computer. (GE 2; AE D.) Company X security investigators understood engineer B to mean that Applicant had been typing on his laptop at the time. (GE 4.) On January 28, 2011, Applicant met with the facility security officer (FSO) to discuss engineer B's statement. (AE B.) When asked about the discrepancy between his and engineer B's versions, Applicant stated that engineer B was lying if his account differed. Due to the conflicting versions provided by Applicant and engineer B about the incident, company X's facility security officer (FSO) confiscated Applicant's unclassified laptop. A forensic search of the laptop did not reveal any suspicious activity. The ISSM took the USB thumb drive involved in the incident and stored it in the ISSO's container. Recovery software was used on a classified laptop to recover the files that had been deleted on January 26 in accord with standard practice, but analysis of the data was inconclusive about the files on the USB drive when it was plugged into Applicant's unclassified laptop. (GE 4.)

During a February 9, 2011 meeting with company X's ISS, Applicant explained that he was "very groggy" and in an "extreme fog" on January 24, 2011, and that he had taken a double dose of over-the-counter allergy medication before reporting to the testing site that day. He denied that he had entered any keystrokes on his laptop while the classified thumb drive was inserted. Applicant indicated that he was not thinking when he inserted the classified thumb drive in his laptop, and he did not know why he did it. (GE 4.)

Applicant met with the ISS and the ISSM on February 10, 2011, to explain the factors (fatigue, a "severe and painful sinus attack") that he believed contributed to the incident. Additionally, he indicated that while waiting for assistance to access the gateway IS network, he wanted to check unclassified work on his laptop. He again denied that any computer keys were struck while the classified USB drive was connected to his laptop. Applicant stated in part, "Although [engineer B] and I realized the situation virtually simultaneously, [engineer B] removed the USB drive as I was simultaneously reaching to remove it as well." (GE 4; AE F.)

On February 14, 2011, Applicant accompanied company X security personnel to the closed area and demonstrated that he accessed the source IS network via PC #1 on January 24, 2011 before going to his unclassified laptop. Applicant was asked directly if he intentionally inserted the classified USB drive in his unclassified laptop, and he stated that he had not. The ISSM then checked the audit logs for PC #1 on January 24, 2011, which indicated that the computer had been logged in under the credentials of engineer A during the time the incident occurred. (GE 4.)

Applicant met with company X security personnel on February 21, 2011. Applicant indicated that he had inserted the classified USB drive into his laptop after he had moved files from the classified source IS network via PC #1. On being told that audit logs showed that he had not logged onto PC #1, Applicant responded that he thought he had accessed PC #1, but it was possible that he used engineer A's account

on the source IS network to move the classified files to the USB drive for transfer to the gateway IS network.[5] (GE 4.)

On February 22, 2011, engineer A indicated to company X security personnel that he did not transfer files for Applicant on January 24, 2011, although he may have neglected to lock PC #1 on that date while running tests. (GE 4.) On February 24, 2011, the company removed Applicant's access to the source IS network. (GE 4; AE B.)

On March 2, 2011, company X reported its findings about the incident to the Defense Security Service (DSS). The company concluded that Applicant knowingly plugged the classified USB drive into his unclassified laptop to transfer files to a classified network and that his action placed the classified files contained on the USB drive at risk for compromise. Applicant's laptop was connected to the company's network when the classified USB drive was inserted, so classified information was not adequately protected from approximately 4:00 a.m. on January 24, 2011, until clean-up actions were completed by the ISSM on January 25, 2011. A loss of classified information was presumed as files were stored and handled improperly when the Secret USB drive was plugged into Applicant's unclassified computer system, which was connected to an unclassified network. The company also expressed its belief that Applicant committed a second security violation by using PC #1 while it was logged onto by engineer A. Furthermore, the company concluded that misleading statements by Applicant at the beginning of the investigation into the incident caused the deletion of evidence during the cleanup process. Company X informed the DSS it was contemplating terminating Applicant from his employment "for knowingly committing a security violation and repeatedly covering up his actions."[6] (GE 4.)

On March 16, 2011, Applicant was terminated for cause from company X. (GE 3; AE G; Tr. 37.) The company's decision to terminate Applicant cited his experience as an engineer with many years in the industry; that "he knew full well what he was doing when he violated the security rules, and when caught, repeatedly lied about his actions."

Applicant filed for unemployment compensation on March 21, 2011. To support his claim, he provided a statement on May 9, 2011, claiming that his security infraction

[5] Applicant testified at his hearing that there were times that "in the generic sense," he said he transferred the information from source IS network to the classified USB drive when he meant that he directed or caused the information to be transferred by engineer A. (Tr. 57.)

[6] In accord with ¶ 1-304 of the NISPOM, which requires government contractors to establish and apply a graduated scale of disciplinary actions in the event of employee violations or negligence of NISPOM requirements, company X established an enterprise-wide Security Standard on August 7, 2006. Under the Security Standard, "processing classified information on computer systems not authorized and approved for classified processing," is expressly cited as a deliberate breach of security. For a first non-deliberate breach of security, the recommended minimum disciplinary action is a written reprimand. For cases of deliberate breaches of security, the Security Standard specifies at a minimum a five-day suspension without pay but also indicates, "circumstances may warrant recommendation of termination." (GE 2; AE H.)

was minor; that the incident was blown out of proportion by the company; and that the company did not investigate anything. He explained his conduct, as follows:

> BEFORE ANY DATA FOR INFORMATION WAS TRANSFERRED, I TOOK IT OUT WHEN I REALIZED IT. THEY CHECKED MY LAPTOP TWICE AND DID NOT FIND ANY DATA. THE FIRST COUPLE OF MEETINGS THEY WANTED TO DROP IT. THEN SOMEONE WANTED TO PRESS THE POINT. IN THE MEANTIME, THEY SAID I LOGGED INTO SOMEONE ELSE'S COMPUTER BUT I NEVER DID AND THERE IS NO PROOF. (GE 2.)

In response, company X indicated that Applicant "violated security rules and when caught, repeatedly lied about his actions [emphasis in original]." Applicant's claim for unemployment benefits was denied. Applicant appealed the denial on May 12, 2011.

Testimony was taken on Applicant's appeal of the unemployment benefit denial over two sessions in June 2011. On June 22, 2011, a company X human resources (HR) generalist testified that Applicant deliberately took classified information and placed it on an unclassified computer, and that his deliberate action led to a possible breach. The HR representative was unaware of any actual compromise of classified information and testified that Applicant had no previous security infractions at the company. The defining factor for the company in deciding to terminate Applicant's employment was that he lied and failed to cooperate with the company's investigation into the security infraction. Company X's FSO testified that the ISSM did an "overwrite" of the hard drive based on Applicant's initial account that it was an accident he had not used the keyboard while the classified thumb drive was plugged into his laptop. About the company's findings that Applicant had not been fully candid, the FSO testified that Applicant claimed his conduct was inadvertent until February 24, 2011, when Applicant admitted that he put the classified USB drive into his unclassified laptop after he had moved files from a classified system to the classified thumb drive. The FSO admitted that Applicant refused to sign a statement of admission that he had deliberately inserted the classified thumb drive in his unclassified laptop. The FSO further testified that compromise of classified information could not be ruled out because of Applicant's actions, although he also explained that data transfer from a USB drive requires manipulation of the computer. (AE G.)

Applicant maintained at his unemployment compensation hearing that he "made an accidental mistake, nothing more." He testified that engineer A was sitting at the PC to access the source IS network when Applicant went to take possession of the thumb drive from someone in the integration group.[7] Applicant related that he did not have the proper log on information for the gateway IS network, so he had previously asked engineer A to transfer the information for him. About the incidents alleged in SOR 1.b, Applicant provided the following account:

[7] The name of the co-worker was not audible to the transcriber of the proceedings. (AE G.) Given the other evidence of record, it is reasonably presumed that Applicant named engineer A.

So, [engineer A] basically received the thumb drive and he was already logged in at that time. And so, uh, and he actually said to me, "You know, why don't I go ahead and do this anyway because I'm already logged on?" And I did say to him, "Well, you know, if you would like, you, maybe you should log off so that I could log on."

He said, "No, I'm already logged on so I'll just do this. Just tell me what you wanted; what files do you want to transfer." So basically, I–then I actually went up to the, uh, to the workstation there and I pointed to him. I said, "Well, just take this folder because this, this has, uh, I think, the files that I said that I would want." So, he copied those files out to the thumb drive and then we both watched [sic] over to the [gateway IS network] workstation where he could then access the thumb–He could then access the [gateway IS network] and he logged on to that. And then he took that thumb drive and he took that file from the thumb drive and used the [gateway IS network] to place [a downloaded file] on a location in [the destination IS network]. And I basically watched them as he did this.

So, after he was done with that task, he basically gave the thumb drive to me and I said, "Well, okay, I'll hold onto this and I'll, I'll, I will find someone who is responsible for this." And, uh, uh, and, and, and talk to someone how to get this back to the file cabinet where it was stored. So, I walked back to my, uh, my desk and then I started to–I just basically kind of put some drive on my desk, uh, immediate and after about ten minutes or so, uh, after I was looking at some files and, and looking at my agenda. I was actually taking [sic] on my laptop at that time looking at my agenda. Uhm, then it just kind of occurred to me and basically that I think, uh, the effects of the tiredness and the medication was really starting to hit me at that time and it just kind of popped in my head that I was wanted [sic] to check what was in that file because, in that folder, because I really didn't know the individual files in the folder, and I wanted to be sure that the team had the individual files that were actually needed to be worked on.

So, what I was thinking about the security implications and my clouded state, I basically plugged the thumb drive in there so I could see what files were, were in the folder. Uhm, and after, uh, like that was–that was the motivation basically for plugging in the, uh, thumb drive into the laptop. I completely forgot about the security, you, know, implications because of my state. Uh, there were a couple of other things that went through my mind as they, uh, and during this time, as a senior principal engineer, I'd like to think that one of my, uh, one of my activities is to think about how to do things more efficiently. And one of the things and just the split second, it took less than five seconds, where this thumb drive, probably five seconds or so, where this thumb drive was plugged in, in that split second, one of the things that I was, running through my mind was would it be nice

> if we could use a thumb drive to, to move information between, uh, networks like this?
>
> Uhm, and, and then I realized that–that's when I started to realize when I went through the series of logic that but, you know, you can't use a, uhm, a secured thumb drive on an unsecured laptop. And that realization just hit me. I started to reach for the, uh, for the thumb drive but [engineer B] was sitting right next to me and he pulled it out basically about the same that I was reaching for it. And then, uh, then [engineer B], uh–Then I–I was–I was now– At that point, I was not only tired and I was not only medicated but I was also pretty rattled by what just happened and then I started to try to explain to [engineer B], "Well, you know, we, we, I was using this to move information from one network to the other network."

Applicant denied that he had typed on the laptop while the thumb drive was inserted. About him telling the FSO on January 28, 2011, that engineer B had to be lying about the incident, Applicant stated:

> As far as when, uh, [the FSO] asked me the question, uh, that it was [engineer B] lying that I gave, the way he asked me that question, it kind of implied to me that maybe he was saying that [engineer B] claimed that I robbed the bank or something, something totally unrelated. And that's why I said, "Well, if he said something like that, he'd be lying."

About his failure to tell the ISSM during their first meeting on January 24, 2011, about his sinus medication, Applicant claimed it did not occur to him until the following day, when he noticed the wrapper while taking out the garbage. Applicant maintained that he had been as "completely cooperative and, and, and forthcoming [with the company's investigation] as [he] possibly could." He also asserted that training was "very poor" about secured thumb drives in that he was unaware of the functional parameters for their use or who was the proper custodian of the Secret/NOFORN USB thumb drive. (AE G.)

The decision denying unemployment to Applicant was overturned. While evidence was presented showing that Applicant's insertion of a classified thumb drive into his unclassified laptop was a breach of security, fatigue was a mitigating factor that led the judge to conclude his action was an accident and not willful. Company X established that it had a reasonable expectation, although not a policy, that its employees cooperate with investigations into security breaches. However, company X did not establish that Applicant had engaged in deliberate misconduct, or that he had admitted his guilt. Applicant's explanations were accepted as credible in the absence of testimony from other witnesses with firsthand knowledge or other substantial evidence to corroborate his alleged admission. (GE 2.)

Applicant was unemployed until June 2011, when he began working as an engineering product manager for another defense contractor.[8] (GE 1.) On August 8, 2011, Applicant provided a written account of his conduct on January 24, 2011, to the Defense Security Service (DSS). He indicated in part that he was not only authorized to view the classified information on the thumb drive, but also had "personally created a substantial portion of it." During routine security and team meetings, he was told, "an approved method of transferring data such as the Classified Information was through the use of a classified thumb drive." He also indicated to his knowledge the information on the secured thumb drive was encrypted, so plugging it into an unclassified laptop would have caused an authentication screen to appear. Yet, no dialog box appeared when he plugged the thumb drive into his machine, presumably because the drive was inserted "for a very short time, somewhere in the range of five to twenty-five (5-25) seconds." He asserted that he had not typed a single character on the unclassified laptop while the thumb drive was plugged in. Applicant also claimed that just before he plugged the classified thumb drive into his laptop, he observed engineer B (who had contradicted Applicant's claim of no keystroking) to be checking his vacation plans online. In addition, he testified that engineer B had expressed concern to him earlier that evening about a possible poor performance appraisal. Applicant asserted that he had done his best to cooperate during what he characterized as "a series of interrogations of increasing strenuousness," during which questions were asked with the intent of trapping him into giving an incorrect answer. He expressed his belief that a marginal security rating received by company X caused the security team to make an example of him, and that the actions of management were influenced by recent layoffs. (GE 2.)

On February 5, 2013, Applicant completed and certified to the accuracy of an Electronic Questionnaire for Investigations Processing (e-QIP). He disclosed in response to inquiry concerning whether he had left any employment under negative circumstances in the last seven years that he had been fired by company X in March 2010 [sic]. He gave the following reason for his termination:

> [Company X] claims lack of cooperation during the investigation of a minor security incident. This was subsequently proven to be false. The decision to terminate was driven largely by poor company security lapses including a marginal security audit rating at the time. These combined circumstances caused the travesty of a grossly overly punitive reaction without proper management oversight or deliberation.

Applicant also responded "Yes" to the question concerning whether he had ever had a security clearance eligibility/access authorization denied, suspended, or revoked. He explained in part that in January 2011 he was using a classified USB drive to transfer files from one classified network to another classified network and that after completing the task, he "accidentally connected the classified USB drive to [his] unclassified laptop while turning attention to other work." (GE 1.) Applicant did not know whether his

[8] On his February 2013 Electronic Questionnaire for Investigations Processing (e-QIP) (GE 1), Applicant mistakenly listed the end date for his employment with company X as March 2010 and the start date for his next job as June 2010 instead of March 2011 and June 2011 respectively.

clearance was officially suspended or revoked. He was advised by his then employer's FSO to answer "Yes" to the clearance question because the company was unable to verify his situation. (Tr. 106.) Applicant explained that he did not mention separately that he had allegedly accessed PC #1 when the computer was logged under engineer A's credentials because it happened at the same time as the USB thumb drive incident and involved the same people for the same task. To him, it was a single event. (Tr. 109.)

On March 14, 2013, Applicant was interviewed by an authorized investigator for the Office of Personnel Management (OPM). Applicant claimed that he erred on his e-QIP because the incident involving the classified USB thumb drive occurred in January 2010 [sic], when he "accidentally" connected the classified thumb drive to his unclassified laptop. He asserted that he immediately realized his mistake and removed the classified USB drive. Applicant confirmed he had received the proper security training but he was tired, on a new schedule, and on a new sinus medication at the time. He added that he self-reported the incident to the ISSO on duty, whose name he did not recall. (GE 2.)

In response to DOD CAF interrogatories, Applicant confirmed that the information previously provided during his March 2013 interview was accurate. About any additional information that he believed might assist the DOD CAF to determine whether it is clearly consistent to grant him security clearance eligibility, Applicant indicated that he had over 20 years of unblemished compliance with security clearance responsibilities and that company X had provided no advance training in the use, features, or functions of the USB drive at issue. (GE 2.)

By late June 2014, Applicant had a new job with another defense contractor.[9] His work has been of an unclassified nature, although the company is sponsoring him for security clearance eligibility. (Tr. 115.)

At his security clearance hearing in September 2014, Applicant testified that he had received no security training specific to the testing site. When he asked about training, he was advised to rely on the integration group for direction and assistance in security matters. (Tr. 59.) About engineer A's involvement in the security incident, Applicant testified that engineer A took the classified USB drive from the integration employee, and offered to Applicant that he would load the files onto the USB from the classified source IS network. Engineer A then moved over to PC #2 and loaded the data from the USB to the gateway IS network. (Tr. 123-124.) Applicant denied that he ever used engineer A's login session to move files from one network to another. (Tr. 150.) Applicant testified that he possessed the classified thumb drive from engineer A for "probably under five minutes" when he inserted it into his unclassified laptop. (Tr. 128.) "I just absentmindedly just [sic] did it by accident, because I was kind of tired at the time, and some of–and my other conditions, I just really didn't think of the security at that split second." (Tr. 61.) He testified on direct examination that he was reading specifications on his computer and not typing into it. (Tr. 69.) He later testified on cross examination that the combination of his impaired cognition and "being used to using this laptop to

[9] Applicant was working for his current employer as of his June 28, 2014 answer to the SOR.

plug in [his] own personal thumb drive" led to him plugging in the classified USB drive "without thinking." (Tr. 121.) He noticed that nothing was happening on his computer, so he looked down and saw that the classified USB thumb drive was plugged into his laptop. (Tr. 127.) Applicant explained that his intent was to hold onto the thumb drive until he could identify someone who had access to a classified storage container. Engineer B was busy at the time. (Tr. 120.) When asked by me why he failed to notice the classified marking on the USB thumb drive, Applicant testified as follows:

> Well, part of it was that when the thumb drive was on the table, all I could really see was the thumb drive, the tag was hanging down on the bottom. So, it was very easy for me to absentmindedly think, well, here is a thumb drive. It's not like the tag is right on top of the thumb drive and you have to move it to get to it. So, it was very easy just to take that thumb drive, move it half an inch and plug it into the laptop. (Tr. 154.)

Concerning whether Applicant had any other removable media on his desk at the time, he claimed he could not recall exactly "because the table was very cluttered." (Tr. 156.)

Applicant described engineer B's reaction as "very agitated" to see the classified USB thumb drive in Applicant's unclassified laptop. (Tr. 62, 130.) He denies telling engineer B that he planned on copying files from his computer onto the Secret USB drive and then transferring it to a Secret PC on the source IS network. (Tr. 74.) Applicant went on that he was so unfamiliar with the details of the networks that he did not know what to call them at that time. (Tr. 75, 140.) He tried to explain to engineer B that he planned to use the thumb drive to transfer information between classified networks, but engineer B did not understand what he was trying to tell him. (Tr. 63.)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered in evaluating an applicant's eligibility for access to classified information. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to 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. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K, Handling Protected Information

The security concern for Handling Protected Information is articulated in AG ¶ 33:

> 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.

Applicant acknowledges that on January 24, 2011, he plugged a USB thumb drive classified Secret/NOFORN into an unclassified laptop issued to him by his then employer (company X). As an authorized user of a classified information system, Applicant was required to comply with all security requirements under the NISPOM (*see* ¶ 8-105) and his then employer's security standards implementing the NISPOM requirements. The NISPOM and his employer's security procedures prohibited the processing of classified information on non-classified systems. Applicant has consistently denied that he intended to insert the classified USB thumb drive into his laptop. He also denies that any classified information on the thumb drive could have been compromised because he did not process any information or type any keystrokes

during the short time that the classified thumb drive was plugged into his unclassified laptop.

As a threshold matter, the burden is on the Government of establishing disputed facts. A reasonable inference of deliberate conduct arises because of the nature of the conduct involved. Applicant physically inserted a conspicuously marked Secret thumb drive into his unclassified work laptop, which he knew was not approved for the processing of classified information. Even assuming some level of fatigue and impaired cognition from him taking a double dose of generic sinus medication before reporting to work, these factors apparently did not cloud his judgment only minutes before he inserted the thumb drive in his laptop, when according to him, he oversaw engineer A's authorized downloading of a file from the classified source IS network to the classified USB drive. When asked to explain how he could have inserted the classified thumb drive by accident, Applicant testified on direct examination at his September 18, 2014 security clearance hearing that he was not thinking about the security implications of his conduct. On cross-examination, he testified in part that he inserted the classified thumb drive without thinking because he was used to plugging in his personal thumb drive into his employer-issued laptop.[10] In response to my inquiry into how he could have failed to note the conspicuous tag marking the USB thumb drive as Secret, he indicated that the tag had a long string that somehow hung off his desk. The inference to be drawn is that he picked up the drive without noticing that it was classified.

Yet, there is no evidence showing that he had an unclassified thumb drive at his workstation that he intended to insert into his unclassified laptop instead. Furthermore, engineer B's contemporaneous account of the incident supports a finding of a deliberate violation on Applicant's part. When engineer B asked Applicant to explain why he had the Secret thumb drive plugged into his unclassified laptop, Applicant stated that he "planned on copying a file from his computer onto the Secret USB" and then transferring it to a Secret PC on the source IS network. When confronted with engineer B's account in January 2011, Applicant claimed engineer B had to be lying. Applicant now asserts that engineer B misunderstood him; that he meant to convey that he was transferring information between classified networks; and that when he referred to his "computer" in his verbal exchange with engineer B, he meant classified PC #1. However, if Applicant intended to transfer information between classified networks, there would have been no reason to insert the classified thumb drive in his unclassified laptop. Employees were reminded in a security violation alert on November 18, 2010, of their responsibilities to note the markings on classified documents, media, and hardware. Under the circumstances, it is difficult to conclude that Applicant inserted the classified thumb drive by mistake. Disqualifying condition AG ¶ 34(g), "any failure to comply with rules for the protection of classified or other sensitive information," applies.

The Government also alleges that Applicant knowingly violated the security regulations covering the authorized use and protection of classified IS systems by using a classified computer logged in under the credentials of another company X employee

[10] Employees were reminded in a security violation alert in November 2010 that personal drives were not to be used on any company IS system. (GE 2.)

to transfer classified files using the Secret USB drive (SOR 1.b). The evidence shows that on January 24, 2011, Applicant sought to transfer classified information from a source IS network at the testing site to a destination IS network at another location. The source IS network was not linked to the gateway IS network, so transfer was via a PC # 1 trusted download onto a classified thumb drive that would then be plugged into classified PC #2 for upload onto the gateway IS network. Applicant now maintains that the download was accomplished by engineer A, who took possession of the thumb drive from an integration engineer and volunteered to transfer the files because he was already logged onto PC #1. However, other evidence raises doubts about whether engineer A performed the trusted download and transferred the information through the use of the Secret thumb drive. On January 24, 2011, Applicant provided a written statement to the ISSM in which he stated in part: "With authorized assistance, I was using the thumb drive to make a file transfer between the [source IS network] and the [gateway IS network] when I accidentally plugged the thumb drive into my laptop USB port. On February 14, 2014, Applicant demonstrated to security personnel that he had accessed the source IS network via PC #1, before going to his unclassified laptop. The ISSM then checked the January 24, 2011 audit logs for PC #1, which showed that PC #1 was logged in under the credentials of engineer A when the Secret USB thumb drive was used. Engineer A told company X security personnel that he had not worked alongside Applicant on January 24, 2011, nor had he transferred any files for him on that date.[11] It is possible that engineer A did not recall the events of January 24, 2011, when he was interviewed by company X security personnel on February 22, 2011. On the other hand, one has to question why Applicant did not clearly detail engineer A's involvement from the outset, if engineer A performed the download and transfer. Additionally, Applicant apparently demonstrated to security personnel on February 14, 2011 that he accessed the source IS network on PC #1 before going to his laptop and plugging in the Secret USB thumb drive. Again, it is inexplicable that Applicant would fail to mention that engineer A accessed PC #1 instead of him. Furthermore, Applicant's version has changed over time, from he was using the classified thumb drive with authorized assistance, to engineer B performed the download and transfer at his request, to engineer B volunteered to transfer the information for him.

Engineer A and Applicant were authorized users of PC #1 and the source IS network at issue, although access by Applicant to the classified source IS network when the computer was logged in under engineer A's identifiers would violate identification and authorization controls established to ensure that users have the appropriate security clearances and need-to-know for the information on the classified system. *See* NISPOM ¶ 8-303.[12] The weight of the evidence implicates Applicant in a violation of IS authentication requirements. AG ¶ 34(g) applies.

[11] The only evidence of engineer A's denial of any involvement is in company X's report of its investigation into the incident involving the Secret thumb drive. Hearsay evidence is entitled to less weight than a signed affidavit or statement. At the same time, company X had no apparent motive to misrepresent the interview of engineer A or its findings during the investigation. Applicant's assertion that company X was looking for a way to terminate his employment to reduce personnel costs is speculative.

[12] ¶ 8-303 of the NISPOM provides as follows:

Mitigating condition AG ¶ 35(a), "so much time has passed 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's current reliability, trustworthiness, or good judgment," applies in part. The security violations were committed almost five years ago, and Applicant had no previous security violations or infractions. Nonetheless, it is difficult to conclude that the conduct is not likely to recur in light of Applicant's failure to accept any responsibility and his failure to be fully forthcoming about his actions, as detailed in the findings of fact. For example, Applicant indicated that he had moved files from the classified source IS network until he was advised about the audit logs. His first response was that it was possible that he used engineer A's account to download the classified files. When informed that engineer A denied any involvement in the downloading and transfer, Applicant claimed the transfer was accomplished by engineer A at his direction. Applicant has also imputed base motives to engineer B and company X in an effort to minimize his own culpability. On August 8, 2011, Applicant provided a statement to the Defense Security Service in which he claimed that engineer B was checking his vacation plans online and had related concerns about possibly receiving a poor performance appraisal just before engineer B observed the classified thumb drive in Applicant's laptop. On his e-QIP, Applicant asserted that the decision of company X to terminate his employment was driven "largely by poor company security lapses including a marginal security audit rating at the time." During Applicant's unemployment hearing, company X admitted the marginal rating and job layoffs in the fall of 2010. However, the evidence before me does not establish that his employment termination was related to those events.

AG ¶ 35(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities," is not implicated. Company X terminated Applicant's employment in March 2011 for his security violations, but also because of his failure to acknowledge responsibility. There is no evidence that Applicant has accessed classified information since then, so he has no subsequent record of compliance with security procedures.

As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.

a. Unique identification. Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.

b. Authentication at Logon. Users shall be required to authenticate their identities at "logon" time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of any application or utility on the system.

Applicant claims he was not adequately trained about security procedures at the testing site, but the evidence is to the contrary. He was told to ask the onsite integration engineers if he had any security questions or concerns. Furthermore, the security violations committed did not involve a security procedure specific to the testing facility or the particular classified project. Furthermore, Applicant had received refresher security briefings by his employer. All employees with clearances were reminded in the security violation alert of November 2010 of their responsibilities concerning taking proper notice of classification markings and to comply with security procedures when using classified hardware. Applicant's violations of the security procedures involving classified information systems whether deliberate or due to gross negligence, are not mitigated under AG ¶ 35(c), "the security violations were due to improper or inadequate training."

Guideline M, Use of Information Technology Systems

The security concern for Use of Information Technology Systems is set out in AG ¶ 39:

> 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 use for the communication, transmission, processing, manipulation, storage, or protection of information.

Applicant's insertion of the Secret USB thumb drive into his unclassified laptop computer on January 24, 2011, establishes Guideline M concerns under AG ¶ 40(f):

> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

Based largely on engineer B's statement that he observed Applicant working on his computer while the Secret thumb drive was plugged in, company X concluded that the possibility of compromise could not be ruled out. Applicant has consistently denied that he engaged in any keystroking or otherwise manipulated the computer while the Secret thumb drive was in his laptop. While any processing of classified information on an unclassified computer or IS network would implicate AG ¶ 40(e), "unauthorized use of a government or other information technology system," and perhaps also AG ¶ 40(h), "any misuse of information technology, whether deliberate or negligent, that results in damage to the national security," the evidence falls short of establishing that Applicant manipulated the computer. However, AG ¶ 40(e) applies in that Applicant's use of the IS source network through PC #1 when the computer was logged onto under engineer A's identifier would be an unauthorized use of an IS system, notwithstanding Applicant could have properly accessed the system under his own logon identifier. Even so, the

primary concern is with his knowing entry of a classified thumb drive into his unclassified computer when it was connected to an unclassified IS network.

As with Guideline K, the failure to comply with the rules and regulations pertaining to information technology systems may be mitigated if so much time has elapsed since the misuse to where it no longer casts doubt on judgment, reliability, and trustworthiness. For the reasons addressed above, Applicant has not demonstrated the reform necessary to apply 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."

AG ¶ 41(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," could reasonably apply to Applicant's access to the IS network via PC #1 under engineer A's logon identifier. Applicant was apparently not only an authorized user of PC #1 and the classified IS source network. He created some of the information on the system. Applicant testified during his unemployment hearing that he watched as engineer A downloaded the files onto the Secret thumb drive and then loaded the files onto the gateway IS network. Applicant demonstrated during the February 14, 2011 walkthrough with security personnel that he accessed the IS source network before going to his laptop. Applicant did not indicate that he personally uploaded files to the classified gateway IS network for which he was waiting access authorization. AG ¶ 41(b) would not mitigate his intentional insertion of classified removable media on an unclassified laptop connected to an unclassified IS network. AG ¶ 41(b) also would not apply to any unauthorized access by Applicant to the classified IS gateway network, but the evidence does not prove culpability in that regard.

Applicant's evidence to establish AG ¶ 41(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," is not persuasive. The denial of unemployment benefits to Applicant was overturned because a review examiner on appeal concluded that company X failed to present a statement from Applicant or the testimony of a witness to substantiate its report that Applicant admitted moving files from the source IS network to the Secret thumb drive. That decision is not binding on the security clearance adjudication process. Due to the need to protect classified information, any doubts about an individual's security clearance eligibility are to be resolved in favor of national security. As discussed under Guideline K, it is difficult to believe that Applicant would have failed to notice the large marking tag on the Secret thumb drive. While Applicant explained that he had impaired cognition, no co-worker interviewed during the investigation mentioned concern about Applicant's ability to perform on January 24, 2011. Engineer B reported, with no apparent motive to misrepresent, that Applicant told him he planned to copy a file from his laptop onto the Secret USB thumb drive and then transfer it to the classified source IS network. Engineer B's swift removal of the Secret thumb drive from Applicant's unclassified laptop prevented Applicant from acting on his

stated intent. Whether it was Applicant or engineer B who first notified the ISSO of Applicant's misuse of the IS system, AG ¶ 41(c) does not mitigate deliberate conduct.

Guideline E, Personal Conduct

> The security concerns about Personal Conduct are set forth in AG ¶ 15:
>
> 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.
>
> The following will normally result in an unfavorable clearance action or administrative termination of further processing for security clearance eligibility:
>
> (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation; or
>
> (b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

By using PC #1 without properly logging on with his own credentials, and then inserting the Secret thumb drive in his unclassified computer (SOR 3.a), Applicant raised significant doubts about his judgment and willingness to comply with the rules and regulations for the proper use and protection of a classified information system. During company X's security investigation, Applicant provided discrepant accounts about whether he accessed PC #1 and downloaded information onto the Secret thumb drive before inserting it in his unclassified computer. Applicant's then employer viewed these conflicting accounts as a failure to cooperate and terminated Applicant's employment as a result. The Government alleged Applicant's employment termination as a separate concern under Guideline E (SOR 3.c). Applicant had an obligation to provide full, frank and truthful answers to company X security officials from the outset, and he failed to do so. His initial account led the ISSM to perform an overwrite of the system on January 24, 2011. At the same time, his employment termination is a consequence of his security violations and lack of candor. It does establish a separate issue of poor judgment, unreliability, or untrustworthiness. A favorable finding is warranted as to SOR 3.c. Disqualifying condition AG ¶ 16(b) applies to the personal conduct concerns covered under SOR 3.a and 3.b:

> (b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative.

Applicant's violations of security procedures through misuse of an information system are explicitly covered under Guidelines K and M, so his misconduct does not trigger AG ¶ 16(d):

> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:
>
> (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information;
>
> (2) disruptive, violent, or other inappropriate behavior in the workplace;
>
> (3) a pattern of dishonesty or rule violations;
>
> (4) evidence of significant misuse of Government or other employer's time or resources.

Nevertheless, Applicant engaged in unreliable behavior and demonstrated a pattern of dishonesty that would implicate AG ¶ 16(d) were his actions not otherwise covered under other guidelines.

The Government alleged that Applicant was also not candid when he completed his e-QIP and did not mention that he had violated computer logon authentication procedures when he accessed PC #1 when it was logged on under engineer A. Applicant could reasonably consider his access to PC #1 as part of the same incident involving the insertion of the Secret thumb drive in his unclassified laptop. The Government did not establish that Applicant deliberately falsified by not mentioning the violation committed by accessing PC #1 under engineer A's logon information. However, Applicant displayed minimization and denial of responsibility when describing the insertion of the Secret thumb drive on his unclassified laptop. Applicant cooperated with company X's investigation in that he attended all meetings about the incident. However, Applicant's documented record of inconsistent statements about his role in the events of January 24, 2011, and his unacceptable tendency to discredit the

motivations of his then employer as well as engineer B, are inconsistent with reform. Not one of the personal conduct mitigating conditions is fully satisfied.[13]

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 his conduct and all relevant circumstances in light of the nine adjudicative process factors listed at AG ¶ 2(a).[14]

Applicant and his team were under some time pressures on January 24, 2011, which may well have been the primary motivator in him circumventing security regulations involving the download of classified information from an IS network and then inserting a Secret USB drive in his unclassified laptop. Applicant maintains that security

---

[13] Conditions that could mitigate security concerns under AG ¶ 17 include:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment as caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (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 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;
>
> (f) the information was unsubstantiated or from a source of questionable reliability;
>
> (g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

[14] The factors under AG ¶ 2(a) are as follows:

> (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.

training was inadequate. He had held a security clearance for approximately 20 years, so he is reasonably expected to have known and complied with the security procedures established for the security of a classified IS system, especially the source IS network for which he had access authorization. It is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or renewal of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990). Based on the facts and circumstances before me, for the reasons noted above, I do not find it clearly consistent with the national interest to reinstate Applicant's security clearance eligibility at this time.

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

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

Elizabeth M. Matchinski
Administrative Judge