DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-05543
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jeff Nagel, Esq., Department Counsel
For Applicant: Joseph Testan, Esq.

June 21, 2013

_____

Decision

_____

GOLDSTEIN, Jennifer I., Administrative Judge:

Without a need to know, Applicant downloaded proprietary information from his company computer and his company network onto a thumb drive after accepting an employment offer from a competing company. Security concerns under Guidelines M and E were not mitigated. Eligibility for access to classified information is denied.

Statement of the Case

On November 14, 2012, in accordance with DoD Directive 5220.6, as amended (Directive), the Department of Defense issued Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under Guidelines M, J, and E. The SOR further informed Applicant that based on information available to the government, DoD adjudicators could not make the preliminary affirmative finding that it is clearly consistent with the national interest to grant or continue Applicant's security clearance.

Applicant answered the SOR on December 5, 2012, and requested a hearing before an administrative judge. The case was assigned to me on March 29, 2013. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on April 9,

2013, scheduling the hearing for May 16, 2013. The hearing was convened as scheduled. The matter reconvened on May 22, 2013, and June 6, 2013, to allow the parties to complete their cases. The Government called three witnesses and offered Exhibits (GE) 1 and 2, which were admitted without objection. Applicant offered Exhibits (AE) A through D. AE A, AE B, and AE D were admitted without objection. AE C was excluded. (Tr. 335.) Applicant testified on his own behalf and called four witnesses. DOHA received the transcripts of the hearings (Tr.) on June 4, 2013, June 5, 2013, and June 18, 2013.

Amendment to the SOR

Pursuant to Additional Procedural Guidance ¶¶ E3.1.2, E3.1.3, E3.1.7, and E3.1.13 of the Directive, Department Counsel moved to amend SOR ¶ 1.b to conform to the evidence. This allegation originally read:

b. Security and management personnel from [company] seized the thumb drive prior to you leaving work and it was found to contain technical data (strategic development plans and two Digital Radio Frequency Memory (DRFM) designs) from projects [company] was working on or had worked on which would be useful to a competitor during any bidding process.

The Amendment proposed to change this allegation to read:

b. Management personnel from [company] seized the thumb drive prior to you leaving work and it was found to contain technical data (strategic development plans and two Digital Radio Frequency Memory (DRFM) designs) and other [company] proprietary, confidential, private, and non-disclosure files from projects [company] was working on which would be useful to a competitor during any bidding and project development process.

Further, Department Counsel moved to strike ¶1.c of the SOR in its entirety. Applicant had no objection to striking ¶1.c, but did object to the amendment of ¶1.b. I granted the motions for amendments. (Tr. 10, 243-245, 443-447.)

Findings of Fact

Applicant denied all of the SOR allegations. (Answer.) After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 49-year-old employee of a defense contractor. He is single and has no children. He earned a bachelor's degree in electrical engineering in 1985. (GE 1; Tr. 343-345, 425.)

Applicant was employed by a defense contractor (DC-A) from December 2002 to July 2010. Applicant became unhappy in his position with DC-A when a new business manager position was placed above him in their chain of command. He applied for a job

with a competing defense contractor (DC-B). DC-B was run, in part, by a former employee of DC-A, who testified on Applicant's behalf. On July 19, 2010, Applicant received a job offer from DC-B. He immediately gave DC-A two-week's notice of his intent to vacate his position. (Tr. 26-29, 102-105, 179-188, 541-544, 554.)

Unbeknownst to Applicant, his computer was under surveillance by DC-A as the result of an internal investigation beginning in early 2010. The information technology (IT) director at DC-A, who testified at the hearing on behalf of the Government, utilized two different monitoring software programs to track all of Applicant's key strokes and to take screen shots of his monitor every few seconds from early 2010 until after he resigned. (Tr. 34-40, 466-477, 497-498, 502-508.)

Suspicions were raised about Appellant's activities in May 2010. This was after a review of screen shots and key strokes disclosed that Applicant transferred a large amount of company proprietary and confidential material, including financial information that was outside the scope of Applicant's employment with DC-A, onto a removable drive (thumb drive) over the course of a single day. The President of DC-A testified that company policy stated downloads to thumb drives required permission from supervisors and required encryption. Applicant's former manager at DC-A testified Applicant had no need to know the information he copied and Applicant lacked permission to copy those files to a thumb drive. The transfer was discovered a few days after it was complete, when the IT director reviewed the output of the monitoring software. The President of DC-A testified that an attorney working with DC-A advised him against confronting Applicant without access to the thumb drive, but encouraged him to continue to monitor Applicant. The monitoring continued but did not disclose any suspicious activity again until July 20, 2010, shortly before Applicant gave his notice. (Tr. 41-50, 113-129, 225-226, 477-482, 512, 548-552, 568, 590, 594-596, 601-603.)

The IT director testified that the screen shots and keystroke programs showed that on Friday, July 16, 2010, Applicant received an email from the head of DC-B. Applicant's manager at DC-A testified that screenshots and key logs showed on Monday, July 19, 2010, Applicant printed his resignation letter. Approximately one minute after Applicant sent the resignation letter to a printer, he started to download information to a thumb drive. First, he copied proprietary systems files that set out "how [DC-A]'s systems department worked, procedures, manpower plans, that sort of thing." (Tr. 555-556.) Then Applicant copied personal information to the thumb drive in a separate download. Next, Applicant sent his timecard to a printer. Applicant's manager at DC-A testified that nine minutes later the screen shots showed Applicant downloaded "technical form files" to the thumb drive. Those files contained, "hiring plans, some technical detail on some of the things we were doing and how we were doing them." (Tr. 558.)The files not only came from Applicant's hard drive, but also from DC-A's company network. Applicant's manager testified that Applicant had been working on the files, but should not have taken them with him when leaving to work for a competitor. The screen shots showed Applicant's manager that Applicant then deleted select portions of the technical details from a folder on the thumb drive but retained other portions. After Applicant's downloads were complete, Applicant served the resignation letter to his

employer, giving two-weeks' notice. (Tr. 50-79, 482-487, 553-566, 569-571, 581, 586-589, 592.)

After Applicant tendered his resignation letter to DC-A, the management decided to check the screenshot and keystroke logs. The logs showed the activity noted above. It was near the end of the workday, and the President of DC-A decided that they should try to retrieve the thumb drive from Applicant. The President of DC-A headed out to the parking lot, where he found Applicant. Two other managers were also present. The President of DC-A requested the thumb drive from Applicant. Applicant reached in his pocket and surrendered it. Applicant told the President of DC-A that he had only downloaded personal information to the thumb drive. (Tr. 55-58, 133-136, 173, 423, 567, 573-574.)

The President of DC-A testified the thumb drive was sent to a forensic lab for them to document and recover the files contained on the drive. The thumb drive was ultimately found to contain both deleted and undeleted proprietary files downloaded in May 2010, as well as those files copied on July 19, 2010.[1] Both the President of DC-A and Applicant's manager testified that the files contained on the thumb drive would be useful to a competitor during any bidding and project development process. (Tr. 58-65, 158-160, 549.)

Applicant appeared for work on July 20, 2010, but was told the thumb drive had not yet been reviewed. He was given the option of remaining at work or going home. Applicant chose to go home. Later, he was notified his position had been terminated and he was given an "Employee Departure Notice" that shows Applicant voluntarily resigned. (GE 1; GE 2; AE A; Tr. 365, 939-395.)

The President of DC-A testified he reported the incident to the Defense Security Service (DSS). DSS recommended he report the incident to the FBI. He did so. Applicant acknowledged that he was contacted by the FBI. He never spoke with the FBI agent, but she left a message on his phone. No one from the FBI followed up and he never spoke to anyone from the FBI. Applicant was never cited for any criminal or security violation. There is no evidence that the FBI conducted a full investigation of these allegations. (GE 2; Tr. 66-79, 367.)

Applicant contends that he did nothing wrong. He testified that he was not required to obtain permission every time he used the thumb drive. He called three former DC-A employees that testified thumb drives were often used at DC-A.[2] Applicant asserted that he was using the information downloaded in May 2010 to try to do forecasting of manpower needs for employees he managed who did work on the files in question.[3] Further, he testified he was not aware that when files are deleted, they

[1] Witnesses testified that deleted files could be recovered. (Tr. 58-65, 516-517.)
[2] However, Applicant's witnesses had all terminated their employment with DC-A by 2006. (Tr. 252-256, 257-261, 281-287.)
[3] This assertion was later rebutted by testimony from the IT director, who testified they had a computer program that was designed to complete the forecasting function for them. (Tr. 492-496, 512-514, 523-526, 530-535, 596-599.)

remain on a thumb drive and can be restored until overwritten. Regarding his July 19, 2010 download, he testified that his intent was to copy only his personal files, but:

> Well it was another day for me. I wasn't that careful on what I was copying to the thumb drive. I was looking for personal folders but I didn't look inside the folders and look at subfolders or every single file in every folder so it is possible that there were [DC-A] proprietary files there yes. (Tr. 361.)

Applicant reported he though he copied only personal music files, his resume, and his closing papers from the condo he had purchased. He testified that at the time of the download on July 19, 2010, he was still an employee of DC-A, and intended to continue to work at DC-A for the remaining two weeks. He acknowledged that there probably was proprietary information in the files that he copied that day, but denied copying it intentionally. Neither Applicant nor his witnesses believed that information from DC-A would have been useful to DC-B, due to the unique designs involved. (GE 2; Tr. 346-365, 390-392, 397-398, 402-422, 427-440.)

Applicant, through his attorney, argued that the Government's witnesses are not credible because they had significant reasons to be biased.[4] I do not find the argument to be material in determining Applicant's credibility. I find that Applicant behaved wrongly on the day in question. (AE D; Tr. 73-85, 108-113, 148-153, 160-169, 174, 178, 234, 281-317.)

Applicant is well respected by his friends and colleagues, many of which are employed by his current employer. His four witnesses testified that they find Applicant reliable and trustworthy. Additionally, seven friends and colleagues wrote letters on Applicant's behalf. Each attested to the high morals and trustworthiness of Applicant. (AE B; Tr. 14-18, 245-256, 257-280.)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used 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, administrative judges apply the guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching 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

[4] Applicant, through his attorney, alleged the witnesses testifying on behalf of the Government are biased against Applicant because he is a key player with their current competitor. Applicant also presented a lawsuit between DC-A and DC-B, and offered testimony concerning alleged questionable acts conducted by the former President of DC-A, and possibly DC-A itself, in the past.

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 the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance 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 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.

Section 7 of EO 10865 provides that adverse 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 M, Use of Information Technology Systems

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

> Noncompliance with rules, procedure, 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 a security concern and may be disqualifying. The following disqualifying condition is potentially applicable:

> (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.

The President and Applicant's manager at DC-A credibly testified that by 2010 their company had a policy restricting the use of thumb drives to "need to know" information with the permission of a direct supervisor. Applicant duplicated information (media) that he had no need to know, and no permission to download to a thumb drive, in direct violation of this policy. Specifically, on July 19, 2010, after receiving an employment offer from a competitor, he downloaded company proprietary information from his hard drive and from the company network. That thumb drive was seized by DC-A management and it was found to contain proprietary information. Applicant acknowledged he may have downloaded proprietary information on that date, but suggested he did it inadvertently. I decided that Applicant's credibility on this point was lacking due to the sequence of events, established the Government witnesses, on his last day of employment. He has the burden to rebut the evidence against him, and he failed to do so. The above disqualifying condition has been established.

AG ¶ 41 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (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 failed to acknowledge wrong-doing. He has not established that similar circumstances are unlikely to recur. Further, his conduct casts doubt on his current reliability, trustworthiness, and good judgment. The misuse was a serious event and Applicant failed to correct the situation in any manner. None of the above mitigating conditions apply.

Guideline E, Personal Conduct

The security concern for the Personal Conduct guideline is set out 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying condition is potentially applicable:

> (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; and
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources.

Appellant's inappropriate behavior in copying proprietary files belonging to his employer, for which he had no need to know, shows that he has a lack of candor and exercised questionable judgment. His behavior indicates that he may not properly safeguard classified information. AG¶ 16 (d) applies. However, due to the lack of evidence on an alleged FBI investigation, I find no disqualifying conditions can be applied to SOR ¶ 2.b.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (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; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

None of the above mitigating conditions apply. Applicant failed to produce sufficient evidence that he acknowledges his misconduct. His violations of IT policy and misappropriation of proprietary information were not minor matters, and he has done little to show similar inappropriate behavior would not occur. Thus, he continues to demonstrate questionable judgment and has left himself open to potential coercion.

Guideline J, Criminal Conduct

The security concern relating to the guideline for Criminal Conduct is set out in AG ¶ 30:

> Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

AG ¶ 31 describes conditions that could raise a security concern and may be disqualifying. The following is potentially applicable:

> (c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted.

Applicant copied company proprietary material without authorization onto a thumb drive. An agent from the FBI called Applicant after the incident was reported, but no further action was taken. The Government failed to present evidence of a substantiated allegation or admission of criminal conduct. It presented no criminal statutes that were alleged to have been violated, no records from the FBI, and no court records. As a result, I cannot find this disqualifying condition applies.

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 relevant 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 commonsense 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 pertinent facts and circumstances surrounding this case. I have incorporated my comments under Guidelines M, E, and J in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant has a long history of working in the defense industry, and is respected by his colleagues and friends. He performs well at his job. Those are facts that weigh in favor of reinstating his security clearance. However, his conduct demonstrated a lack of honesty, reliability, and trustworthiness. He failed to provide evidence of sufficient remedial action that could assure the Government that similar conduct will not occur in the future, or that the potential for coercion or duress is insubstantial.

Overall, the record evidence 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 Use of Information Technology Systems, and Personal Conduct security concerns.

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 M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	For Applicant
Paragraph 3, Guideline J:	FOR APPLICANT
Subparagraph 3.a:	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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Jennifer I. Goldstein
Administrative Judge