DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 20-02990
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne Driskill, Esq., Department Counsel
For Applicant: Phillip Stackhouse, Esq.

September 30, 2021

_____

Decision

_____

GLENDON, John Bayard, Administrative Judge:

Applicant failed to mitigate security concerns regarding handling protected information, use of information technology, and personal conduct. Based upon a review of the pleadings, the documentary evidence, and Applicant's testimony, national security eligibility for access to classified information is denied.

Statement of the Case

On August 9, 2018, Applicant filed a security clearance application (SCA). On February 20, 2021, the Defense Counterintelligence and Security Agency, Consolidated Adjudications Facility (CAF), issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline K (Handling Protected Information), Guideline M (Use of Information Technology), and Guideline E (Personal Conduct). The CAF acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended (Exec. Or.); Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) promulgated in Security Executive Agent

Directive 4, *National Security Adjudicative Guidelines* (Dec. 10, 2016), effective within the DoD on June 8, 2017.

Applicant responded to the SOR (Answer). He denied the allegations under Guidelines K and E and "accepted" the allegation under Guideline M. In addition, he provided three pages of other comments and arguments. He requested a hearing before an administrative judge of the Defense Office of Hearings and Appeals (DOHA). On June 24, 2021, the case was assigned to me. On July 19, 2021, DOHA issued a notice scheduling the hearing for August 11, 2021.

I convened the hearing as scheduled. Department Counsel presented Government Exhibits (GE) 1 through 3, which were admitted without objection. Applicant offered four exhibits at the hearing, which I marked as Applicant Exhibits (AE) A through D. His exhibits were also admitted without objection. DOHA received the hearing transcript (Tr.) on August 18, 2021. (Tr. at 15-18.)

Findings of Fact

Applicant's personal information is extracted from his SCA unless otherwise indicated by a parenthetical citation to the record. After a thorough and careful review of the pleadings, Applicant's testimony, and the documentary evidence in the record, I make the following findings of fact.

Applicant is 36 years old and has worked for a major defense contractor as a cyber security engineer since September 2018. After graduating from high school, Applicant studied for one year (July 2003-June 2004) at the U.S. Military Academy Preparatory School, which is also known as West Point Prep. This education constituted active-duty service in the Army. He did not continue his education at West Point and was honorably discharged from the Army. He earned a bachelor's degree in August 2007 and began working for a major defense contractor (E1) in November 2007 as an information assurance engineer. He also continued his studies and earned two master's degrees, one in December 2013 and a second in April 2015, and a Ph.D. in March 2021. He was first granted a security clearance in about November 2007 and has continuously maintained his eligibility. He has lived with his girlfriend since 2017. They have no children. (Tr. at 20-21; GE 2 at 14; AE C.)

Applicant's last day of work at E1 was August 30, 2018. He had previously given notice of his intent to resign his position at that company and had accepted a position with his current employer (E2). In the afternoon of his last day of work, he downloaded over 15,000 files onto his personal USB external hard drive (USB Device), and when he left the employer's premises, he took the USB Device with him. On September 4, 2018, investigators at E1 were alerted to this unusual downloading activity by a departing employee and investigated the circumstances. (GE 3 at 1.)

The investigators found that the file path for the downloaded files was titled "Personaldocs\[E1]." They issued a memorandum to Applicant (the E1 Memorandum),

dated September 6, 2018, even though he no longer worked there. Applicant signed the E1 Memorandum the next day, acknowledging receipt, and returned it to the investigators. In the E1 Memorandum, the investigators advised Applicant that he had violated two company policies set forth in the E1 Corporate Information Protection Manual by connecting his USB Device to E1's information network and by downloading files from E1's network onto his personal USB Device without authorization. The two policies are described in the E1 Memorandum as follows:

1. Section 106.6.7(1) - titled Storage of Information on Personally Owned Information Technology Assets; and
2. Section 106.6.7(3) - titled Connectivity of Personally Owned Information Technology Assets to [E1] Infrastructure.

The investigators instructed Applicant to return his USB Device to E1, which he did. They advised him and sought his acknowledgment that E1 may delete E1 information from the device and in the process may also delete Applicant's information. In a separate internal E1 memorandum, dated December 10, 2018, which was not shared with Applicant at that time, the writer noted that the files recovered from his USB Device numbered 15,179 with a total amount of 8.7 gigabytes of data transferred from E1's network to the USB Device. The investigators compared that number of files with a full-year count of the number of files Applicant would transfer in the performance of his work duties, which was 22,599. This comparison highlighted the unusual nature of Applicant's actions on the day he left E1. (Tr. at 39, 66-68; GE 3 at 1-2.)

The December 10, 2018 internal memorandum references the allegation under investigation as follows:

> Allegation: Data Exfiltration with CI/CT nexus (SUBSTANTIATED) (emphasis in original)

The term CI/CT stands for Counterintelligence/Counter Terrorism. The USB Device was wiped in its entirety on September 17, 2018. The memorandum also states: "On October 9, 2018, Adverse information was filed against [Applicant]." (GE 3 at 1.)

In his August 2019 clearance reinvestigation background interview, Applicant initially denied any personal history of misuse of any information technology system, including any non-compliance with rules, procedures, guidelines, or regulations. He was then confronted by the background investigator with information from his E1 employment records regarding his actions on August 30, 2018. Applicant was advised that as a result of his actions on that date he was not eligible for rehire at E1. He testified at the hearing that he learned for the first time during his background interview that E1 regarded his actions as improper. Applicant admitted to the investigator that on his last day at E1, he accidentally downloaded E1 proprietary information (E1PI) onto his USB Device when he was hurriedly downloading his personal files onto his device that he wanted to take with him. He explained that this happened because he had used his company's laptop for both

work and personal purposes over his 11 years of working at E1. He said he downloaded onto the E1 network research articles that he read for his own education as well as information related to his doctoral studies when he was pursuing his Ph.D. as well as information related to his master's degrees prior to that. This information was downloaded onto the same drive on the E1 network that he used for work-related activities. He claimed that in his haste, he inadvertently downloaded E1PI along with his personal files. (Tr. at 39-40; GE 2 at 6-7.)

SOR Allegations

Paragraph 1, Guideline K - The SOR sets forth a single allegation under this guideline in which the Government alleges that Applicant deliberately downloaded E1PI onto his USB Device in August 2018 while employed by E1. In his Answer, Applicant wrote that his actions were not deliberate. He wrote that he only intended to download his educational materials related to his master's degree studies as well as over two years of his studies in his Ph.D. program. He explained that his E1 work laptop was limited to unclassified information. In mitigation, he commented that he immediately complied with the request of E1's security manager to deliver the USB Device to the manager. He also argued that his actions were infrequent and the result of inadequate training while he worked at E1.

Paragraph 2, Guideline M - This paragraph of the SOR cross-alleges under Guideline M the same facts alleged under Guideline K. In his Answer, Applicant admitted the disqualifying facts, using the words "I accept" rather than "I admit." In mitigation, he noted that this incident occurred nearly three years earlier and no similar action has occurred. He also commented that no classified information was copied onto his USB Device. He repeated that his actions were not intentional. He claimed that E1 permitted data to be transferred between computer systems using external hard drives, though he acknowledged that transferring E1PI to a personal mobile device was not authorized.

Paragraph 3, Guideline E – This paragraph also cross-alleges under Guideline E the facts set forth under Guideline K. In his Answer, Applicant denied the allegation. However, his denial was based upon his mistaken belief that the Guideline E allegation concerns a falsification in his SCA for his failure to disclose the August 30, 2018 security incident. In fact, the SCA predated August 30, 2018, by three weeks. Instead, the cross-allegation concerns the incident itself, as an independent personal conduct security concern.

At the hearing, Applicant testified at length about the circumstances surrounding the August 30, 2018 incident. He explained that E1 had two computer networks and that on occasion information had to be transferred from one network to the other. Certain files were so large that they could only be transferred by a USB external hard drive device. The administrative process to do this required the completion of a form by the employee transferring the files. The form must be approved to authorize the employee to perform transfers between networks. While performing his duties at E1, Applicant had submitted this form and had permission to transfer files on a USB drive between the two networks.

Without such an approval, the system would not deny him access to the company's network when he plugged in a USB hard drive. Applicant claimed that it was not necessary to use a company-issued USB device to transfer files. This testimony is inconsistent with the E1 Memorandum, which stated that Applicant had violated company policy prohibiting the connection of a personally owned device to E1's technology infrastructure. (Tr. at 22-26; GE 3 at 2.)

Applicant further testified that he was required to use an external USB device only for work-related information. He admitted that one mistake he made on August 30, 2018, was that he used an external USB device to transfer his personal files. That required getting permission from "IT." He claimed he was unaware of that requirement at the time he left the company. The form he had previously prepared to obtain permission to use an external USB device required confirmation that the permission sought was to perform routine work-related activities. (Tr. at 26-28.)

A complication that increased the risk of Applicant's actions is that he did not separate his personal files from his work files on his section of the E2 shared drive used to store information. Under any single "parent folder," he would have subfolders containing both personal and work files. He referred in his testimony to "a nested tree" of parent folders and sub-folders with further sub-folders and even more sub-folders. He used a chronological approach to his filing system so that all of his activities in a given period, both work-related and personal, would be in that one main file, separated into sub-folders. As a result, when he copied over to his USB Device a parent folder that he thought had his academic literature as well as personal information, such as tax and pay information, the parent folder would also include sub-folders with E1PI. The Windows copying technology he used was simple "drag and drop," so he dragged and copied file folders that contained both work-related files and personal files. In that process, nothing was removed from the E1 system, it was just copied. He did not review each folder to see if it had only personal files. He was going through the process of copying hundreds of folders hastily over an hour or two at the end of his last workday at E1 before Labor Day weekend. He agreed he made a mistake in how he handled the copying. Nevertheless, he testified that it was only his intent to copy his academic and personal files. He purchased the USB Device about a week earlier. It was solely for the purpose of transferring his files in connection with his change of employment. (Tr. at 28-31, 47-55, 71-74.)

Applicant also transferred files from his emails that included both personal emails and work emails. He testified that E1 allowed personal use of its email system. Some of the email files he copied may have been work-related. He believes that a large number of the other files he transferred onto his USB Device were publicly available documents that he was required to download periodically for work purposes. Those files are large and numerous. (Tr. 31-34.)

Applicant contends that with the permission he had to use portable USB devices to transfer files for work-related purposes, he did not violate any company policies by his

actions on August 30, 2018. He does not believe he violated any policy by plugging his USB Device into the E1's network on that date. (Tr. at 76-77; GE 3 at 2.)

With hindsight, Applicant now realizes that he should have talked to E1's IT Department and explained what he wanted to do with his personal computer files, even though he already had "USB access" approval. The day he left the company, he had an exit interview in which he turned over all of his IT equipment. He had the opportunity then to talk about his use of the personal USB Device, but the subject never came up since his actions were only discovered in the following days. His job at E1 was related to information security in connection with a specific DoD project. His new job at E2 was also dealing with information security, but at the organization level. Nevertheless, he insisted at the hearing that the information he claims he copied inadvertently would not be helpful to him in his new position with E2. (Tr. at 61-65, 76-77.).

Other Mitigating Evidence

When Applicant was interviewed as part of his background investigation, he claims he learned for the first time the seriousness of his actions when he left E1. He decided to take actions to avoid future problems like this one, and he enrolled in a cyber awareness course provided by DoD in 2019 and again in 2021. He also teaches a course in cyber security at a local university. In connection with that experience, he further educated himself on such matters. (Tr. at 39-45; AE D at 1-2.)

Applicant testified that prior to the August 2018 incident, he had never been counseled or written up for being careless with information technology, nor has he had any security issues since the incident. He testified that since he was instructed by E1's investigators in September 2018 to return the USB Device, he has been transparent with everyone about the incident. (Tr. at 45-46.)

Applicant's exit from E1 in 2018 was the first time he had ever gone through this transition process. He had three weeks from the date of his new job offer from E2 to his last day at E1. He had much to do, including a geographic relocation. He deferred the copying process to his last day of work and performed it quickly in a limited amount of time. He did not take the time to see what sub-folders were included in each folder he copied and whether the folders he was copying contained any E1PI. He testified that throughout his 11 years at E1, he was aware of E1's rule that you cannot take E1PI when you terminate your employment with the company. (Tr. at 55-56.)

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants

eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865 § 2.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Adverse clearance determinations must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 15-01253 at 3 (App. Bd. Apr. 20, 2016).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531.

Analysis

Guideline K, Handling Protected Information, and Guideline M, Use of Information Technology

Due to the overlap in security concerns, disqualifying conditions, and mitigating conditions in the context of Applicant's conduct on August 30, 2018, these two guidelines are discussed together, below.

The security concern under Guideline K is set out in AG ¶ 33 as follows:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information-which includes classified and other sensitive government information, and proprietary information-raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The security concern under Guideline M is set out in AG ¶ 39 as follows:

> Failure to comply 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 includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

The following conditions under Guideline K, AG ¶ 34, are potentially disqualifying:

> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant copied and stored E1PI on his unauthorized USB Device. His actions violated Employer 1's rules for the protection of sensitive and proprietary information. The above disqualifying conditions have been established.

The following conditions under Guideline M, AG ¶ 40, are also potentially disqualifying:

> (a) unauthorized entry into any information technology system;
>
> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
>
> (e) unauthorized use of any information technology system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized.

Applicant's insertion of his USB Device was an unauthorized entry into E1's information technology system. He downloaded E1PI to an unauthorized USB Device. He had no authority to use E1's information technology system to copy files onto his USB Device. His actions of duplicating files from E1's information technology system for his personal use were not authorized by E1. The disqualifying conditions of AG ¶ 40 have also been established.

AG ¶ 35 of Guideline K contains three mitigating conditions that have possible applicability to the facts of this case:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
>
> (c) the security violations were due to improper or inadequate training or unclear instructions; and
>
> (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

AG ¶ 41 of Guideline M contains three mitigating conditions have possible applicability to the facts of this case:

> (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;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and

(d) the misuse was due to improper or inadequate training or unclear instructions.

AG ¶ 35(a) and AG ¶ 41(a) are not established. The passage of three years since Applicant's departure from E1 and his actions of copying a large number of files from the E1 information technology network onto his USB Device were not so long ago as to mitigate his actions. While his violations of the company's policies were infrequent and occurred under the unusual circumstances of Applicant resigning his position with the company, those facts do not mitigate serious security concerns arising under these guidelines. The fact that he was leaving E1 to begin working at another major DoD contractor suggests that Applicant's motives in copying E1 proprietary information were not innocent. This is exactly what the E1 investigators concluded when they determined that their counterintelligence and counter terrorism concerns were "substantiated." As discussed below, I did not find credibility in Applicant's testimony that his downloading of E1PI was "inadvertent." Moreover, his actions standing alone, without regard to his intent, cast doubt on his current reliability, trustworthiness, and judgment.

AG ¶ 35(c) and AG ¶ 41(d) are only partially established. Applicant has suggested that he did not receive proper training from E1 over his 11 years working there as an information assurance engineer regarding the procedures he should have used to copy personal files from the E1 network upon his departure from the company. The record is silent as to what training he did receive, though it is noted that his responsibilities were in the field of information security and it is likely that E1, as a major DoD contractor, would properly trained its information security professionals. Also, Applicant was highly educated and testified at length about his personal studies in this field. Even if he had insufficient training, he had the opportunity at his exit interview to discuss his actions and intentions, if they were indeed innocent, but he failed to do so.

AG ¶ 35(d) and AG ¶ 41(c) are not established. Applicant failed to carry his burden to prove that his conduct was unintentional or inadvertent. His demeanor and testimony lacked credibility, and the inconsistencies between his testimony and the other evidence in the record further undermined his credibility. He testified that he was unaware that E1 believed he had done anything wrong until his background interview a year later. This was inconsistent with the fact that he received a copy of the E1 Memorandum on September 7, 2018, advising him that he had violated company policies on August 30, 2018. He also testified that he has been fully transparent about the August 30, 2018 incident, yet he did not voluntarily answer a question during his background interview about any past misuse of information technology systems. At that point in time, he knew from the E1 Memorandum that his actions had raised a serious security concern. He had to be confronted by the investigator with information from his E1 employment records before he would discuss the incident. Also, Applicant is a highly educated information security specialist who fully understood the folder structure of his data on E1's computer

system. It is highly unlikely that he simply made a mistake while acting hastily on the day of his departure from the company. But even if Applicant's actions were inadvertent, he did not report them, let alone report them promptly. The fact that he returned the USB Device when instructed has some mitigating value, but not much. Once his actions were identified, he had no choice but to comply with the investigators' instruction. His return of the USB Device does not satisfy the good-faith requirement of AG ¶ 41(c).

Guideline E, Personal Conduct

The security concern under this guideline is set out in AG ¶ 15, which, in relevant part, provides, as follows:

> 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 or sensitive information.

The following conditions under AG ¶ 16 have possible applicability to the facts of this case and may be disqualifying:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any single guideline, but which, when considered as a whole, 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 individual may not properly safeguard classified or sensitive information;
>
> (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 individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:
>
> > (3) a pattern of dishonesty or rule violations; and
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources;
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

(1) engaging in activities which, if known, could affect the person's personal, professional, or community standing; and

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

Assuming *arguendo* that Applicant's actions on August 30, 2018, are not sufficient for an adverse determination under any other single guideline or that his actions are not explicitly covered under any other guideline sufficiently to support an adverse determination, then AG ¶ 16(c) and (d) have been established. The record evidence contains credible adverse information, which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, and unwillingness to comply with rules and regulations indicating that Applicant may not properly safeguard classified or sensitive information. Applicant's actions of violating two policies of E1 and his downloading of over 15,000 files on the last day of his employment with E1 before commencing work for E2 constitute "a pattern . . . of rules violations" and a "significant misuse of. . . [his] employer's time and resources."

Furthermore, the evidence established the applicability of AG ¶¶ 16(e) and (f). Applicant's conduct could affect his personal and professional standing if it became known by his current or future employers and that fact creates a vulnerability to exploitation, manipulation, or duress by others. His violation of E1's information protection policies violated the commitment he made when he became employed by E1 that he would comply with its policies. Such a commitment was a condition of his employment.

The guideline in AG ¶ 17 contains seven conditions that could mitigate security concerns arising from personal conduct. Three of these mitigating conditions have possible applicability to the facts of this case:

(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 contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and

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

AG ¶ 17(c) is not established. Applicant's violations of E1's policies are not minor and cast doubt on his reliability, trustworthiness, and judgment. Without general authorization or his employer's explicit prior approval, Applicant copied files from the company's network that contained E1PI. That conduct casts doubt on his reliability, trustworthiness, and judgment.

AG ¶ 17(d) is only partially established. Applicant has acknowledged his actions required the prior approval of his employer. He has taken steps to educate himself further on DoD information security procedures. There is a serious question, however, whether such additional education was necessary because Applicant's area of education and professional expertise is information security. Even a non-expert employee would readily understand the security risks presented by plugging a privately purchased USB device into the employer's computer network and copying files without the employer's permission.

AG ¶ 17(e) is not established. Applicant offered no evidence that he has advised his current employer and others about his actions on August 30, 2018, and E1's response charging him with violating E1's policies. As long as this is information is not disclosed to Applicant's current employer, he has not mitigated the potential vulnerability he faces to exploitation, manipulation, or duress.

Whole-Person Analysis

Under AG ¶ 2(c), the ultimate determination of whether to grant or continue national security eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. In applying the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct, all relevant circumstances, and the adjudicative factors in AG ¶ 2(d); specifically:

> (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.

I have incorporated my comments under Guidelines K, M, and E in my whole-person analysis and considered the adjudicative factors in AG ¶ 2(d). Additional comments are warranted. Applicant is a mature and highly educated cyber security engineer. The nature, extent, and seriousness of his conduct speaks for itself. The fact that he did not seek his employer's prior approval to copy files onto his USB Device strongly suggests that he knew that such approval would be denied or highly supervised. I also found Applicant's testimony and demeanor while testifying to lack credibility on the

issue of whether his actions of copying thousands of files from his employer's computer network, some of which contained E1PI, was inadvertent. I conclude Applicant knew better and was seeking to do something without his employer's approval while hoping he was acting "under the radar" of his employer in the afternoon of his very last day of work there. Unfortunately for Applicant, E1's computer system detected his unusual activity of downloading of large numbers of files, and an investigation ensued. E1 investigators found that their counterintelligence and counterterrorism concerns were substantiated. Applicant's evidence in mitigation fell far short of satisfying his burden to establish mitigation of the security concerns raised by his conduct.

Overall, the record evidence as described above leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. After weighing the applicable disqualifying and mitigating conditions and evaluating all of the evidence in the context of the whole person, I conclude Applicant has failed to mitigate the security concerns raised by his handling protected information, use of information technology, and personal conduct.

Formal Findings

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

Conclusion

I conclude that it is not clearly consistent with the national interests of the United States to grant Applicant national security eligibility for a security clearance. Eligibility for access to classified information is denied.

John Bayard Glendon
Administrative Judge