DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-15190
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Julie R. Mendez, Esq., Department Counsel
For Applicant: Christopher Graham, Esq.

07/12/2013

Decision

LOUGHRAN, Edward W., Administrative Judge:

Applicant mitigated use of information technology systems security concerns, but he has not mitigated personal conduct security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On November 20, 2012, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines E (personal conduct) and M (use of information technology systems). The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) implemented by the DOD on September 1, 2006.

Applicant answered the SOR on December 20, 2012, and requested a hearing before an administrative judge. The case was assigned to me on April 19, 2013. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on May 1, 2013, scheduling the hearing for May 30, 2013. The hearing was convened as

scheduled. The Government called a witness and submitted Exhibits (GE) 1 through 6, which were admitted in evidence without objection. Applicant testified and called three witnesses, but he did not submit any documentary evidence. The record was held open for Applicant to submit additional information. He submitted documents that were marked Applicant's Exhibits (AE) A through C and admitted without objection. Correspondence about the additional exhibits is marked Hearing Exhibit (HE) I. DOHA received the hearing transcript (Tr.) on June 7, 2013.

Findings of Fact

Applicant is a 56-year-old employee of a defense contractor (contractor). He has worked for his current employer since 1998. He seeks to retain his security clearance, which he has held for at least ten years. He has a bachelor's degree and a number of post-graduate courses but no post-graduate degree. He is divorced with two children.[1]

In 2005, Applicant became the project manager at a government agency to modernize a telecommunications/information technology system. He left for another project for about 18 months before returning in 2009.[2] On August 17, 2011, the government agency forwarded the following information to the DOD regarding Applicant and another contract employee (Mr. CE-A):

> This memorandum summarizes seven (7) security incidents involving [contractor] employees providing task deliverables under contract number [---] which resulted in removal of two individuals from the contract and a subsequent temporary "Stop Work Order" issued by [government agency].
>
> Two [contractor] staffers, [Applicant] and [Mr. CE-A], were removed from contract tasking as a result of the following incidents:
>
> - March 24, 2011: Denial of Service; [Applicant] directs [Mr. CE-A] to modify account access and prevent [government agency] employees from accessing government-owned network equipment despite repeated direction from [government agency] manager to not access the device. This action resulted in a program lapse which compromised the physical safety of employees at [another office of the government agency].
>
> - March 24/25, 2011: Deletion of Files/Federal Records/Work Product; [Applicant] deletes approximately 1,800 emails and 14,000 files from a government issued laptop and a removable media device. At considerable cost, [government agency] staff was able to recover the emails and approximately one-third (1/3) of the 14,000 files.

[1] Tr. at 87-88; GE 1, 4.

[2] Tr. at 15-16, 71-73, 88-90; GE 4.

- March 24. 2011: Eavesdropping on telephone conversations; [Applicant] and [Mr. CE-A] conspire to afford [Applicant] the ability to eavesdrop on an ongoing conference call. [Mr. CE-A] subverts the system to ensure [government agency] staff is not aware Applicant is on the call and listening passively. Both [Applicant] and [Mr. CE-A] actively bypassed system safeguards designed to preclude such activity.

- March 23, 2011: Forced Government Off Call; [Mr. CE-A] and [Applicant] conspire to covertly force [government agency] employee [Mr. GE-1] off a telephone conference call.

- March 23, 2011: Unauthorized Access; [Mr. CE-A] improperly accesses a third party account by password guess to enable the ability to successfully complete the "Forced Government Off Call" action identified above. [Mr. CE-A] hacks the password of another [contractor] staff member who had administrative access to call functions.

- January 19/20, 2011: Unauthorized Recording of Phone Calls; [Applicant's] recovered files yielded three (3) recordings of conference telephone calls involving himself and [government agency] program managers. Interviews with [government agency] staff indicated that they were unaware any steps were being taken, systemic or other, to record the meeting sessions electronically. As the telephone system doesn't have a recording capability, a wiretap device would have been required to record the calls.

- January 6, 2011: Improper Use of Government Resources; [Applicant] conducted a personal business enterprise using government systems and time while under contract task delivery paid for by the government. Furthermore, [Applicant] identifies his contract government affiliation during correspondence while conducting personal business.[3]

While Applicant was working on another contract for 18 months, his employer used another project manager (Mr. GE-2). Mr. GE-2 resigned from his job with the contractor and was hired directly by the government agency in a supervisory position as an assistant director under the chief information officer (CIO) of the agency. As the assistant director, Mr. GE-2 was Applicant's supervisor at the agency.[4] Applicant stated that Mr. GE-2 created a hostile work environment:

[3] GE 2.

[4] Tr. at 17, 76, 90-92.

> During both work periods, I was continually challenged by a persistent string of unreasonable requests and demands, inconsistent guidance and direction, unsubstantiated or exaggerated accusations of poor job performance, unfair terminations, disproportionate responses for on the job mistakes, and a management style including intolerance, intimidation, and personal ridicule.[5]

Applicant's employer verified that his company received several complaints about Mr. GE-2. The government representative who conducted the investigation into the allegations against Applicant testified that the agency requested that the contractor provide evidence of the hostile work environment for the agency to investigate. He stated that the contractor only provided information about Mr. GE-2's conduct on March 24, 2013. He stated that their investigation found that Mr. GE-2 was testy, loud, and yelling on that day. The agency reviewed the allegations with their general counsel and equal employment opportunity (EEO) assistant director and determined that the allegations of a hostile work environment were unsubstantiated.[6]

The allegations against Applicant will be discussed in chronological order, which is the reverse of how they were reported by the government agency and alleged on the SOR.

SOR ¶ 1.f (Improperly using U.S. Government resources)

Applicant inherited a property in another state that was held in a trust. He was in the process of selling the property to a neighbor of the property. In about January 2011, he sent a fax to the realtor handling the sale of the property from his work fax machine at the government agency. The fax contained a copy of an e-mail that Applicant sent to the realtor using his government e-mail account. The e-mail contained Applicant's name, title at the government agency, and contact information. The government agency permitted "de minimis" use of government resources for personal use. It prohibited all use of government resources for a private commercial enterprise.[7]

SOR ¶ 1.e (Recording government employees without their knowledge or consent)

In about January 2011, Applicant recorded meetings and telephone conference calls involving employees of the government agency and contract employees, without the employees' knowledge or consent. Applicant worked in a jurisdiction that did not make the recording of individuals without their consent a criminal offense as long as one party to the conversation consented to the recording.[8] The only party to the recording

[5] GE 4.

[6] Tr. at 53-54, 64, 73-78, 82, 85-86, 154-155, 175-177; GE 4.

[7] Tr. at 40-42, 63-64, 119-121, 151-154; GE 2, 4, 5.

[8] *See* http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations.

that was not located in the same jurisdiction was Mr. CE-A, who also worked in a jurisdiction that did not prohibit one-party consent recordings. Applicant testified that he did not believe he recorded any telephone conferences with anyone outside his jurisdiction, including Mr. CE-A. This is contradicted by the government agency representative who testified that Mr. CE-A's voice was on one of the tapes. The representative testified that the agency considers their work and meetings to be "sensitive, minimally official use." He stated that the people who were recorded "felt violated." Applicant admitted that his supervisor would have been mad if he discovered that Applicant was recording their meetings.[9] Applicant stated that he recorded his supervisor because it was not uncommon for his supervisor to:

- Make untrue and/or presumptive accusations against [Applicant], [contractor] and [its] employees.
- Hold [contractor] accountable for actions of other contractors or tasks clearly outside [its] scope of work.
- Make various statements that he might forget later.[10]

SOR ¶ 1.d (Applicant and co-worker forced a government employee off a telephone conference call)

On March 23, 2011, an office of the government agency in another state was having problems with its system. Applicant believes that a government employee (Mr. GE-1) caused the problem, but that Applicant's company was being held responsible for the problem. Applicant described Mr. GE-1 as a disgruntled former employee of Applicant's company:

> What is missing from [government agency's] report is that THE ONLY TWO government employees involved in these reported incidents – [Mr. GE-1] and [Mr. GE-2] – are both former [contractor] employees who resigned unhappily from [contractor] to become government employees. They are also good friends with one another. As an [contractor] employee [Mr. GE-1] had a history of internal disputes with other members of the [contractor] team prior to his resignation from [contractor]. Multiple [contractor] employees had come to me with suspicions that Mr. [GE-1] may have deliberately sabotaged their work or withheld critical information to provide Mr. [GE-1] the opportunity to "save the day" in the eyes of [government agency]. If smoke means fire, some serious games were being played by Mr. [GE-1]. In fact, while still an [contractor] employee, I had placed Mr. [GE-1] and another [contractor] employee on a written warning and Corrective Action Plans. Shortly thereafter, [Mr. GE-1] resigned from [contractor] and had only been an [government agency]

[9] Tr. at 20, 37-40, 117-119, 149-151, 155-157; GE 2, 4, 5.

[10] GE 4.

employee for 4-6 weeks (approximately) before the reported incidents involving him took place. (emphasis in original)[11]

A telephone conference call, known as a bridge, was initiated by an employee of Applicant's company (Mr. CE-B) to discuss the matter. As the initiator of the conference call, Mr. CE-B could control who had access to the call. The conference call went on for some time and parties entered and exited the call. Applicant and Mr. CE-A discovered that Mr. GE-1 was on the call. Applicant admits that Mr. GE-1 had authority to be on the call, but he stated that the "unethical behavior was when [Mr. GE-1] joined [contractor's] conference bridge (he knew the standard access numbers) and refused to acknowledge his presence when named and directly asked if he was present." During a period when Mr. CE-B was not on the call, Applicant and Mr. CE-A agreed that Mr. CE-A would access the system using Mr. CE-B's password and force Mr. GE-1 off the call. Mr. CE-A guessed Mr. CE-B's password, which was a simple numerical string and forced Mr. GE-1 off the call.[12]

SOR ¶ 1.a (Violated directives from his manager by directing a co-worker to modify network account access to prevent government employees from accessing the system.)

On March 23, 2011, an office of the government agency in a third state was also having problems with its system. On the morning of March 24, 2011, the problem had still not been resolved. Correcting the problem was a priority because the problem prevented security from monitoring the office, and it prevented the office from contacting security. Applicant admits that a contractor employee "accidently cancelled service" on the system. Mr. GE-2 told Applicant that the agency considered the problem to be the contractor's fault and that the government agency would correct the problem. Mr. GE-1 was assigned to work on the problem. By midday the problem was not resolved, and Mr. GE-2 tasked one of the contractor's engineers to work the problem.

The problem was still unresolved by late in the afternoon. Mr. GE-2 told Applicant to have Mr. CE-A work the problem with Mr. GE-1. Applicant stated that he "sent several messages to [Mr. GE-1] via Instant Messenger (IM) asking [Mr. GE-1] for the phone number of the conference bridge that was supporting the [location] issue," but he was unresponsive. He stated that Mr. GE-2 yelled at him several times using profanity and told him to "just have [Mr. CE-A] 'pick up the [expletive] phone' and call [Mr. GE-1] directly." Mr. GE-2 told Applicant that he was not to be involved in the process.

To correct the problem, an employee had to be on a telephone line to security. Mr. GE 1 was on the telephone line to security. Applicant believed that Mr. CE-A was more qualified than GE-1 to fix the problem. If two people access the system at once, the system can crash. At Applicant's direction, Mr. CE-A accessed the system and changed the password, which locked Mr. GE-1 out of the system and disconnected him from the telephone line to security. Applicant and Mr. CE-A both testified that they were

[11] GE 4.

[12] Tr. at 29, 32-37, 63, 68, 110-117, 144-149, 161-162, 166-167; GE 2, 4, 5.

unaware that Mr. GE-1 was in the system when the password was changed. Applicant admitted that he told Mr. CE-A not to give Mr. GE-1 the new password to access the system.[13]

SOR ¶ 1.c (Applicant and co-worker bypassed system safeguards to eavesdrop on a telephone conference call)

Shortly after the above incident, Mr. GE-2 held a telephone conference call with a number of key people. He specifically told Applicant that he was not to be on the call. Applicant testified that Mr. GE-2 "was out of control," and he thought Mr. GE-2 "was going to come in [his] office and start swinging." He testified that Mr. GE-2 "told me to keep my [expletive] butt off that call." Applicant later testified that Mr. GE-2 "did not explicitly tell me, you are not allowed on the call." Despite Mr. GE-2's directions, Applicant contacted Mr. CE-A and had him link him in to the call without the supervisor's or any of the other parties' knowledge.[14]

SOR ¶¶ 1.b and 2.a (Deleted 1,800 e-mails and 14,000 files from government-issued laptop and removable media device)

On March 24, 2011, it became clear to Applicant that he would no longer be working on the project at the government agency. He decided to copy files from the government agency's server. He borrowed a thumb drive that was issued by his company to a co-worker. He deleted files from the thumb drive to make room for the copied files.

Applicant realized that he could not copy everything onto the thumb drive. From his home, he accessed the agency's server from his government-issued laptop computer. He copied a large amount of files from the server onto the laptop and then a DVD. After the files were copied onto the DVD, Applicant deleted the files from the laptop.

The government agency representative testified that the agency has a process that an exiting employee must follow to obtain copies of files that are on the server. Applicant did not follow that process. The representative testified that the bulk of the files were deleted from the thumb drive and that copies of the deleted files were not on the server. He testified that the agency was able to recover the e-mails and about one third of the files that were deleted at a cost of about $32,000. The agency was reimbursed for that cost by the contractor. Applicant stated that the only files that were deleted from the server were personal files and files that had the contractor's personnel materials. The co-worker who loaned Applicant the thumb drive testified that all the files on the thumb drive were back-up copies of files that were on the server.

Applicant stated that he gave the thumb drive and the DVD to his employer. In April 2011, Applicant's employer reported to the government agency that Applicant

[13] Tr. at 22-29, 60-62, 66-68, 92-106, 140-144, 159-165; GE 2, 4, 5.

[14] Tr. at 29-32, 106-109, 161, 165-166; GE 2, 5.

deleted files from the thumb drive because he "sought an expedient way to download [contractor] proprietary and personal materials from his [government agency] laptop to the thumb drive." His employer offered to provide the thumb drive and a DVD containing a copy of the files deleted from Applicant's laptop computer to the government agency. The agency representative testified that the agency received a thumb drive, but it was a different thumb drive. To his knowledge, the agency never received a DVD. Applicant stated post-hearing that his company's general counsel had not responded to him as to whether the DVD had been returned to the government agency.[15]

SOR ¶ 1.g (Questionnaire for National Security Positions)

Applicant submitted a Questionnaire for National Security Positions (SF 86) on May 9, 2011. Applicant answered "No" to Section 27b, which asked: "In the last 7 years, have you illegally or without authorization modified, destroyed, manipulated, or denied others access to information residing on an information technology system." He testified that he thought he answered the question truthfully.[16]

Applicant was interviewed for his background investigation by an Office of Personnel Management (OPM) investigator on July 18, 2011. A signed statement was not taken, but the interview was summarized in a report of investigation (ROI). He was not asked about, and he did not discuss, the problems at the government agency. He made a general statement that he had never removed restricted material or information from a federal or approved contractor facility without authorization.[17]

Character Evidence

Applicant was described by his company's chief operating officer (COO) as an extremely hard worker, a good manager of people, and a solid engineer.[18]

Policies

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 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

[15] Tr. at 42-51, 63-66 121-143, 154, 170-174; GE 2; AE A.

[16] Tr. at 168-169; GE 1.

[17] GE 3.

[18] Tr. at 85.

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 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."

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." 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 the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of 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 E, Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, 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 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 conditions are potentially applicable:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other 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 person may not properly safeguard protected 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 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; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as . . . engaging in activities which, if known, may affect the person's personal, professional, or community standing.

Applicant used his government fax machine to send a fax to the realtor handling the sale of his inherited property. He sent an e-mail to the realtor using his government e-mail account. The e-mail contained Applicant's name, title at the government agency, and contact information. I find that Applicant's "de minimis" use of government resources for personal use does not rise to the level of a security concern. SOR ¶ 1.f is concluded for Applicant.

There is insufficient evidence for a determination that Applicant intentionally provided false information on his SF 86. AG ¶ 16(a) is not applicable. SOR ¶ 1.g is concluded for Applicant.

The other incidents reported by the government agency merit greater scrutiny. Applicant recorded meetings and telephone conference calls involving employees of the government agency and contract employees without the employees' knowledge or consent. Applicant worked in a jurisdiction that did not prohibit one-party consent recordings. He admitted that his supervisor would have been mad if he found out that Applicant was recording their meetings. Applicant's statement that he did not believe he recorded any telephone conferences with anyone outside his jurisdiction was contradicted by the government representative who testified that Mr. CE-A's voice was on one of the tapes. Mr. CE-A also worked in a jurisdiction that did not prohibit one-party consent recordings.

On March 23, 2011, Applicant and Mr. CE-A agreed that Mr. CE-A would access the system using another contractor's password and force a government employee off a conference call. Applicant admits that the government employee had authority to be on the call, but he stated that the employee's behavior was "unethical" because he "refused to acknowledge his presence when named and directly asked if he was present."

On March 24, 2011, a government employee was attempting to correct a malfunctioning system. Mr. GE-2 told Applicant that he was not to be involved in the process. At Applicant's direction, Mr. CE-A accessed the system and changed the password, which locked the government employee out of the system.

Shortly after the above incident, Mr. GE-2 held a telephone conference call with a number of key people. He specifically told Applicant that he was not to be on the call. Despite Mr. GE-2's directions, Applicant contacted Mr. CE-A and had him link him in to the call without his supervisor's or any of the other parties' knowledge.

Applicant realized that his time at the government agency was coming to an end. He borrowed a co-worker's thumb drive and deleted many of the files on the thumb drive to copy files from the government agency's server. He took his government-agency-issued laptop home and copied files from the agency's server onto the laptop and then onto a DVD. He then deleted files from the laptop. He did not follow the agency's protocol for retrieving files when an employee is leaving the agency.

I find that the above actions showed poor judgment and an unwillingness to comply with rules and regulations. It also created a vulnerability to exploitation, manipulation, and duress. AG ¶¶ 16(c), 16(d), and 16(e) are applicable.

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;

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

(f) the information was unsubstantiated or from a source of questionable reliability.

Any one of Applicant's actions, standing alone, likely would not be enough to establish a security concern. It is the pattern of questionable decisions and disregard for authority that is troubling. Applicant may not have liked or respected Mr. GE 2, but he was an assistant director at the government agency, and Applicant was obligated to follow his directions. He repeatedly failed to do so.

I also was unable to accept all of Applicant's explanations at face value. For example, Applicant testified that Mr. GE-2 "told me to keep my [expletive] butt off that [conference] call." A short time later, Applicant testified that Mr. GE-2 "did not explicitly tell me, you are not allowed on the call." In April 2011, Applicant's employer reported to the government agency that Applicant deleted files from the thumb drive because he "sought an expedient way to download [contractor's] proprietary and personal materials from his [government agency] laptop to the thumb drive." Applicant clearly copied more than just his company's "proprietary and personal materials." Applicant testified that other than personal information and his company's personnel materials, he did not delete any files from the agency's server. Even if true, the copying of the agency's files and the failure to follow the agency's exit protocol are problematic. There are no mitigating conditions applicable to SOR ¶¶ 1.a, 1.b, 1.c, 1.d, and 1.e.

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 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 are potentially applicable:

> (a) illegal or unauthorized entry into any information technology system or component thereof;
> (b)
> (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;
>
> (e) unauthorized use of a government or other information technology system; and
>
> (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.

Applicant's copying and deletion of files would establish several of the above disqualifying conditions. However, as discussed above, it is the pattern of questionable conduct that is the true concern. That concern is appropriately and adequately addressed under Guideline E. SOR ¶ 2.a is concluded for Applicant.

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 the facts and circumstances surrounding this case. I have incorporated my comments

under Guidelines E and M in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

I considered Applicant's favorable character evidence and his long and positive work record with his employer. However, I have concerns about Applicant's judgment, trustworthiness, and willingness to comply with rules and regulations.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant mitigated use of information technology systems security concerns, but he has not mitigated 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 E:	Against Applicant
Subparagraphs 1.a-1.e:	Against Applicant
Subparagraphs 1.f-1.g:	For Applicant
Paragraph 2, Guideline M:	For Applicant
Subparagraph 2.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 continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Edward W. Loughran
Administrative Judge