DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
---, ---- ------	)	ISCR Case No. 08-07693
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ray T. Blank, Jr., Esquire, Department Counsel
For Applicant: William Savarino, Esquire

March 30, 2011

Decision

HOWE, Philip S., Administrative Judge:

On February 1, 2007, Applicant submitted his Security Clearance Application (SF 86 or e-QIP). On March 24, 2010, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines M (Use of Information Technology Systems) and E (Personal Conduct). The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the Department of Defense on September 1, 2006.

Applicant acknowledged receipt of the SOR on March 31, 2010. He answered the SOR in writing through counsel on April 13, 2010, and requested a hearing before an administrative judge. DOHA received the request on April 15, 2010. Department Counsel was prepared to proceed on August 12, 2010, and I received the case assignment on September 18, 2010. DOHA issued a Notice of Hearing on September 8, 2010, and I convened the hearing as scheduled on October 6, 2010. The Government

offered Exhibits 1 through 4, which were received without objection. Applicant testified and submitted Exhibits A and B, without objection. DOHA received the transcript of the hearing (Tr.) on October 14, 2010. Based upon a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Findings of Fact

In his Answer, Applicant admitted the Guideline M allegations in ¶¶ 1.a and 1.b of the SOR. He denied ¶ 1.c, with explanation. Applicant admitted and denied parts of the Personal Conduct concerns alleged in ¶ 2.a through ¶ 2.c. He denied the allegations in ¶¶ 2d, 2.e, and 2.g. Applicant admitted the allegation in ¶¶ 2.f. He also provided additional information to support his request for eligibility for a security clearance.

Applicant is 51 years old and a graduate of the U.S. Naval Academy. He served seven years on active duty in the Navy. He is married and has two children. Since his separation from the Navy in 1998, Applicant has worked in the field of information technology (computers) for several defense contractors. Applicant is a database administrator for his present employer for whom he has worked since 2007. His current employer is a government contractor to the Navy. Applicant has held a top secret clearance since 1988. (Tr. 83-85, 91, 144, 150, 199; Exhibit 1)

As a database administrator, Applicant shared group passwords with other administrators. Applicant had 7 to 30 passwords to remember each day, and would guess his password or a group password if it were necessary. As an administrator, he could not research an existing password if someone in the user group forgot their password. Applicant could only assign a new password if the existing password was forgotten or lost. This practice of guessing passwords in such circumstances was commonplace in his company and his computer experience. There were no company policies on the sharing of passwords by database administrators, except the guessing of someone else's password when it is not a situation of helping the person remember their password or another administrator recollect the group password for work purposes is considered hacking in the computer business. (Tr. 95-106, 178, 181, 183; Exhibits 2, 3)

Applicant used outside disks and other media on company computers during his civilian work career since 1988. He did so only to improve the efficiency and effectiveness of the company's computer systems. Applicant made certain to scan all such outside disks and media using company issued anti-virus screening software prior to inserting such into his employer's computer system. In Applicant's 13 years of working as a government contractor, this practice of scanning outside media before using it on a company computer was common in the industry. The company's policy was that the person who brought in the outside media was initially responsible for screening it for viruses.

Applicant was never admonished by his supervisors for any of his actions involving the use of outside media on company computers. Applicant thought he was

following all standard Navy and company procedures. The computers Applicant managed were not connected to the internet or any computer outside of the company's network. The Government did not offer any evidence that the Navy or Applicant's company had policies, rules or procedures that prohibited this practice. Applicant introduced software patches into the computers to repair errors in software. That process was also routine in the industry and Applicant's experience. (Tr. 106-111, 166, 184-188; Exhibits 2, 3)

Applicant took company office supplies, e.g., staplers, pads, computer mice, paperclips, and paper home to do company work. Applicant's manager was aware he was taking office supplies home, and his supervisors did not object. Other employees also took office supplies home, with the understanding the items would be used for company business. (Tr. 111-116)

Applicant never had classified material in his workplace. He never took classified information home. Applicant did take home documents, which included company propriety data. When transporting this material, Applicant kept it locked in the trunk of his car or on his person. Applicant did not have his manager's authorization to take company information. (Tr. 117-125)

Applicant expanded administrative accounts when he was installing software on company computers. He used a particular command on the computer that allowed him to make the installation, but it also recorded an audit trail about what action was taken. Only super-users were to use this command. Applicant used it, and thought he had the authority to use it because the installation proceeded as planned. No one from his employer told Applicant his actions exceeded his authority. (Tr. 127-130)

Applicant removed an acronym for his company from the label on a media disk. Security banners on unclassified and/or For Official Use Only (FOUO) documents that he brought home to use in his home office did not have a sensitive material label on them. One time, in 2001, Applicant removed a label on a document because it contained the name of the machine and the acronym for the Navy command for which he worked. He shredded that label. Applicant did not verify the sensitivity level of the disk, nor whether he should have taken it from the facility, before he removed it. However, he did not see any label requiring that the document remain on the employer's premises. The document remains in his home safe with the tag excised. (Tr. 119-127, 130-133)

Applicant did not disclose on his February 2007 SF-86, the adverse security decision by another federal agency "disapproving" him access to sensitive compartment information (SCI) in 2004. Specifically, Question 26 B, asked Applicant:

> To your knowledge, have you ever had a clearance or access authorization denied, suspended, or revoked, or have you ever been debarred from government employment? [An administrative downgrade or termination of a security clearance is not a revocation.]

Applicant thought this adverse decision was an administrative determination instead of a denial. The language used in the agency decision was that it "disapproved you for access to classified information." In its February 13, 2004 decision, the other federal agency took this adverse action because of alleged security violations, misuse of information technology systems, and personal conduct. These allegations stem from an interview conducted by a polygraph examiner. The examiner questioned Applicant over the course of three days. He inquired as to Applicant's removal of items from his employer's offices, and "multiple attempts to enter classified and unclassified information technology systems without proper authorization." The agency also stated in its February 13, 2004 letter that Applicant "changed your access on other systems and broadened your area access, without authorization. You also knowingly circumvented security procedures." Furthermore, the agency stated Applicant admitted he removed disks and hard copy information from the workplace without authorization. "You advised taking home classified information with banner pages intact and then cutting them off and shredding them." (Exhibit 3)

When Applicant answered Question 26 B he "believed their action to be administrative and considered it a termination, because up to that point, I had been at (the agency) doing unclassified work." When this decision was made, Applicant was removed from that project (working for the other federal agency) and sent to work on another (unrelated) project. He considered himself terminated from the project with the other federal agency. In response to DOHA interrogatories, Applicant freely supplied a copy of the February 2004 letter from the other federal agency. He did not appeal the other agency's decision because he continued to maintain his Top Secret clearance, so in his estimation he did not lose anything by the decision. (Tr. 92, 133-139, 147, 152-157, 164; Exhibits 1, 3, 4)

Applicant did share group passwords while he worked at the other federal agency. He guessed his own passwords at that agency and expanded the authority of the group account. To his knowledge he did not violate any explicit instructions of that agency regarding computer use. (Tr. 139, 140)

Applicant's former supervisor testified on his behalf. They worked together for four years. She considered him thorough and careful in his work. They are peers now at their present employer. In her experience, the sharing of passwords is common for database administrators to do. She was not aware of any prohibition on the sharing of passwords. She would bring in outside disks and other media from her home, scan them with anti-virus software, and insert them into their employer's computer system. She, and other staff members, routinely took office supplies home to work on company business. This witness never saw any "FOUO" documents. She was not aware of any company policy about taking documents home to work on company issued laptops. She was also not aware of any restrictions on Applicant's authority to install software on their employer's computer system, and grant access privileges. This witness never saw any security banners on documents at their company. On occasion she would guess what her password was to enter her computer. (Tr. 25-51)

The president of Applicant's present employer also testified on Appellant's behalf. He explained his background in consulting on computers and the employment of Applicant. His company does not have a policy prohibiting the guessing of passwords. The company does not have restrictions on "FOUO" documents being taken home. His company does not have restrictions on broadening access. Where he works there are no security banners or sensitive material designations. He employs Applicant also as a data transfer agent in his capacity as a database administrator. Two weeks earlier the Navy changed its policy of bringing in outside media to prohibit or restrict it. Prior to this, no such prohibition existed at their workplace. (Tr. 52-80)

Applicant answered all questions directly and without hesitation. He explained the nature of his work and his background in computers. Applicant was credible and persuasive in his presentation.

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 useful in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's 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." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "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 Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

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

AG ¶ 40 describes eight conditions that could raise a security concern and may be disqualifying:

> (a) illegal or unauthorized entry into any information technology system or component thereof;
>
> (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;
>
> (d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(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;

(g) negligence or lax security habits in handling information technology that persist despite counseling by management; and

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

Four disqualifying conditions may apply. AG ¶ 40 (a) and (c) apply to any illegal or unauthorized entry into an information technology system or component thereof, and the use of any such system to gain unauthorized access to another system or a compartmented area within the same system. Applicant was guessing passwords to gain entry into computer systems. He installed software in computer systems to which he was not authorized access. His entry of code that mimicked a "super-user" allowed him access for his installation work. Appellant testified no one ever told him his work was not authorized. It did exceed his authority.

The third condition is the unauthorized use of a government or other information technology system. Applicant was the database manager for his employers. He admitted he guessed his own computer password when he could not remember it amongst the 30 he had within his control. He admitted he shared group passwords with other contractors and other authorized personnel to access his employer's computers for work purposes. AG ¶ 40 (e) applies.

The fourth condition involves the introduction of media into his company's information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations. Applicant admitted he engaged in the introduction of media from his home laptop computer into the company's computers for work purposes only. Also, he always screened any media with anti-virus software. He added software to the company computers while appearing to be a "super-user," which status he did not have. No rules, regulations, procedures, or guidelines that prohibited this conduct were submitted as exhibits. Applicant denied there were any such rules or procedures. He acted in accordance with what he knew or thought he knew to be the company procedures. However, AG ¶ 40 (f) applies because he did not have the authority to be a "super-user" and introduce software and media into a computer system.

AG ¶ 41 provides three conditions that could mitigate security concerns:

> (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.

All of these mitigating conditions apply based upon the evidence in the record. The first mitigating condition provides that the behavior happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on Applicant's integrity. The testimony of Applicant and his two witnesses showed the SOR allegations were commonplace practice within the last two companies for whom Applicant worked. He is the database administrator and had to take these actions to help keep the company operating on a daily basis. AG ¶ 41 (a) applies.

The misuse, if any, by Applicant was minor and done only to make the organization's computers operate more efficiently and effectively. Applicant only guessed at his own password or group passwords that he was authorized to use as the database administrator. AG ¶ 41 (b) applies.

Over the past 13 years Applicant has followed his employer's information technology rules and procedures. His actions were in conformity with the rules and procedures as he understood them to be. Therefore, he did not act intentionally in a malicious or criminal manner. He never compromised national security. Applicant's supervisor at his previous company and the president of his current employer both testified that they had no concerns or problems with Applicant's work. To Applicant there was no situation to correct because he was always following the correct procedures all the time. No supervisor admonished or counseled him. AG ¶ 41 (c) applies because any action that might have been contrary to a policy was inadvertent or unintentional, designed only to promote his employer's work for the client, and his supervisors knew he was introducing the media as part of his standard actions. They knew and did nothing to stop Applicant, so they acquiesced in his actions.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern pertaining to personal conduct:

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

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

> (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation; and,
>
> (b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

AG ¶ 16 describes seven conditions that could raise a security concern and may be disqualifying:

> (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;
>
> (b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;
>
> (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; 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, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group;

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

(g) association with persons involved in criminal activity.

The seven allegations in Paragraph 2 of the SOR fall within three disqualifying conditions. First, Applicant did not make full disclosure about a denial of a security clearance by another agency in 2004. Question 26 B on the SF-86 of February 2007 asked if Applicant had ever been denied. He answered “no.” The agency’s letter uses the word “disapproved.” AG ¶ 16 (a) applies.

The remaining six allegations fall within the purview of both AG ¶ 16 (c) and (d). The allegations under Guidelines E and M when considered as a whole support a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules, or other characteristics indicating Applicant may not properly safeguard protected information. They also contain credible adverse information not explicitly covered under any other guideline and may not be sufficient individually for an adverse determination, but when combined with all available

information would support 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.

Applicant admitted he took office supplies from empty office cubicles to use at home when doing company work. He denied he took multiple documents home without authorization that had "FOUO" or sensitive designations on them. He admitted he broadened administrative accounts without authority and to accomplish the company's work.

Next, the allegation was made that Applicant was told his access was denied by another agency in February 2004. The denial was based on security violations, misuse of information technology and personal conduct.

Finally, the three allegations in SOR Paragraph 1 were incorporated into Paragraph 2 under personal conduct. Those allegations concern access to computer systems, introduction of media into computer systems, and guessing passwords.

AG ¶ 17 provides seven conditions that could mitigate security concerns:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully.
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;
>
> (f) the information was unsubstantiated or from a source of questionable reliability; and

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

The falsification issue is a matter of semantics and Applicant's understanding of the agency's action six years ago in 2004. The agency stated he was "disapproved." The government alleges it was a denial and should have been disclosed. Applicant knew he had no security clearance at that agency so he assumed it was an administrative determination that did not have to be disclosed in response to Question 26 B. His understanding of the action is not a reasonable interpretation of the agency's action. He did not disclose an adverse action by the other agency concerning his SCI and security clearance application on his SF-86. That denial is an important fact to be considered by the government in deciding whether to grant Applicant another security clearance for five years. Applicant graduated from the U.S. Naval Academy and served seven years on active naval duty. He knows what a falsification is and his duty to disclose based on his experience as an officer and a corporate employee. He did not take any action to correct his omission before being confronted with the facts.

The other allegations are not mitigated under AG ¶ 17 (c) because Applicant admitted freely he did them and he continued to do them over several years. Taking corporate property merely because someone else did is not justification for that action. Removing sensitive material from the workplace, exceeding his authority on computer operations, and removing security banners are actions under the Personal Conduct Guideline that are not minor in their totality nor were they infrequent. These actions Applicant performed over several years and are likely to continue based on that precedent.

No other mitigating conditions apply. No evidence concerning improper or inadequate advice from authorized personnel or legal counsel concerning the security clearance process was submitted by Applicant, so AG ¶ 17 (b) does not apply. Applicant has not changed any of his behaviors to allow AG ¶ 17 (d) to apply. No positive steps to reduce or eliminate vulnerability to exploitation or duress were taken. AG ¶ 17 (e) does not apply. The information was substantiated and admitted by Applicant. AG ¶ 17 (f) does not apply. Finally, there was no evidence or admission of any association with criminals, so AG ¶ 17 (g) does not apply.

Whole-Person Concept

Under the "whole-person concept," the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of an applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

AG ¶ 2(c) requires each case must be judged on its own merits. 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. Regarding information technology systems, Applicant is an experienced former naval officer and database administrator. He acted in his employment the way he thought was proper to accomplish the work for which he was hired. No employer or supervisor every counseled or disciplined him for his actions. His witnesses showed his actions were within the industry norm and they had no concerns about Applicant. Any conduct was motivated by a desire to keep his company's computers operating and to improve his work performance.

However, Applicant did not make a full disclosure about his denial of a security clearance and SCI by another agency. The total number and type of actions Applicant took regarding sensitive information and the computer systems under his control show personal conduct that was done by an experienced and professional adult which was serious. It was also undertaken voluntarily and done frequently. There were no changes in the behavior over the past several years, the continuation of the actions is likely, and there is the potential for pressure, coercion, exploitation, or duress. These are not actions of an experienced professional, particularly the falsification of his questionnaire concerning the denial of an earlier application for SCI and security clearance by another agency.

Overall, the record evidence leaves me with questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising from his use of information technology systems. He did not mitigate the security concerns under personal conduct. I conclude the "whole-person" concept against Applicant.

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:	FOR APPLICANT
Subparagraph 1.a to 1.c:	For Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a to 2.g:	Against 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.

_____
PHILIP S. HOWE
Administrative Judge