DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-09192
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Francisco Mendez, Esquire, Department Counsel
For Applicant: Leslie McAdoo Gordon, Esquire

December 18, 2009

Decision

ANTHONY, Joan Caton, Administrative Judge:

After a thorough review of the case file, pleadings, testimony, and exhibits, I conclude that Applicant mitigated the Government's security concerns under Guideline M, Use of Information Technology Systems, Guideline K, Handling Protected Information, and Guideline E, Personal Conduct. His eligibility for a security clearance is granted.

Applicant completed and signed a security clearance application on June 27, 2002. On August 1, 2007, he completed and signed a Questionnaire for National Security Positions. On April 9, 2009, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR), detailing security concerns under Guideline M, Use of Information Technology Systems, Guideline K, Handling Protected Information, and Guideline 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 revised adjudicative guidelines (AG) promulgated by the President

on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

On May 6, 2009, Applicant answered the SOR in writing. He elected to have a hearing before an administrative judge. On July 27, 2009, Department Counsel, pursuant to ¶ E.3.1.13 of the Directive, amended the allegation at SOR ¶ 3.a. to read as follows: "That information set forth in paragraphs 1 and 2, above." Applicant answered the amended allegation in writing on August 7, 2009. The case was assigned to me on August 12, 2009. I convened a hearing on October 19, 2009, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant.

The Government called no witnesses and introduced six exhibits, which were marked Ex. 1 through 6 and admitted to the record without objection. The Government provided the following provisions from the National Industrial Security Program Operating Manual (NISPOM) for administrative notice: Chapter 5, Section 4, paragraphs 5-400, 5-401, 5-402, 5-403, and 5-404 and Chapter 5, Section 5, paragraphs 5-500, 5-501, 5-502, and 5-509. (January 1995). The Government's administrative notice documents were marked as Hearing Exhibit (HE) 1.

Applicant testified on his own behalf and called one witness. He introduced 13 exhibits, which were identified and marked as Ex. A through Ex. M. Applicant's exhibits were admitted without objection. DOHA received the transcript (Tr.) of the hearing on October 27, 2009.

Findings of Fact

The SOR contains four allegations of disqualifying conduct under Guideline M, Use of Information Technology Systems, five allegations of disqualifying conduct under Guideline K, Handling Protected Information, and three allegations of disqualifying conduct under Guideline E, Personal Conduct. Applicant admitted three of the Guideline M allegations and denied one; he admitted three of the Guideline K allegations and denied two; he admitted one Guideline E allegation and he denied one Guideline E allegation. In his answer to the amended Guideline E allegation, Applicant wrote: "Please refer to my Answer, dated May 6, 2009, which addresses the allegations in paragraphs 1 and 2." I interpret Applicant's answer as a denial of amended SOR allegation 3.a. Applicant's admissions are admitted herein as findings of fact. (Answer to SOR; Answer to Amended SOR.)

Applicant is 34 years old, married, and the father of five young children. He and his wife are expecting a sixth child. Applicant grew up in a military family but has no military service himself. (Ex. 1; Tr. 25-27.)

Applicant graduated from college in 1997, with a Bachelor of Arts degree in English Writing and a Bachelor of Arts degree in Theology. After graduating from college, he got a job writing technical manuals. That job led to employment in the

defense industry, and he was first granted a security clearance in 1997 or 1998. He was read into a special access program in 2004. He has worked for his present employer for almost five years. His current job title is Network Systems Specialist. In 2006, Applicant's security clearance and special access eligibility were revoked by another government agency. (Ex. 2; Ex. 4, at 5-8; Tr. 27-29, 83-84.)

Applicant did not have an academic background in computer and information technology. He acquired his knowledge of the Windows Operating System from on-the-job training and from coaching from more experienced co-workers. In 1998, he worked at a help desk and assisted other employees with their computer problems. In 1998 and 1999, he began to study on-line for certification as a systems engineer. His position title in March 1999 was Windows System Administrator. (Ex. 2 at 4; Tr. 55-58.)

In about 2000 or 2001, Applicant changed jobs and began working with the UNIX Operating System. His co-workers mentored him and provided him with on-the-job training. He also took on-line training courses to learn more about the UNIX system, and, in 2001 and 2002, he took information technology networking courses. From June 2002 to March 2003, he was assigned on an information technology contract overseas by his defense contractor employer. His position title in February 2003 was UNIX System Administrator. (Ex. 2 at 3-4; Ex. 3 at 3; Tr. 55-57, 60-61.)

From October 2003 to October 2004, Applicant was employed as a Systems Engineer. His job title from October 2004 to the present is Network Systems Specialist. (Ex. 2 at 3.)

In 1999, he received a security briefing for systems administrators. He recalled that as a systems administrator, he was required to have periodic security briefings. His last security briefing occurred in 2006 before he lost his security clearance and special access eligibility. (Tr. 58-60.)

The SOR alleges a number of incidents that raised security concerns under Guidelines M, K, and E. These events occurred between 1998 and 2006. Many of the SOR allegations are based on Applicant's self-reporting at the time the events occurred or during a polygraph interview conducted by another government agency in September 2005. Applicant acknowledged that he did not know all the rules for protecting classified information. During the polygraph interview, he made an effort to report every incident he could think of that could possibly be of security significance, even if he was unsure whether his actions violated information technology policy or reflected misuse of security systems. The facts alleged in the SOR were essentially the same facts relied upon by the other agency in revoking Applicant's security clearance and eligibility for special access in October 2006. (SOR; Ex. 4 at 5-6; Tr. 40-46, 90.)

SOR ¶ 1.a. alleged, under Guideline M, that Applicant deliberately or negligently failed to comply with rules and regulations for protecting classified or other protected information by placing an unclassified music disc in a classified computer. Applicant admitted putting the music disc in a classified computer. The incident occurred in 1998

or 1999, during the time that Applicant was a help desk employee. At the time, he worked with a group of more experienced information technology employees. His more experienced colleagues pointed out to Applicant that it was a security violation to insert an unclassified music disk into a classified computer. Applicant was caught by surprise; he did not realize that his action was a security violation. He initiated a discussion of the matter with his security officer, who confirmed that his action was a security violation and advised him not to do it again. Thereafter, Applicant never put an unclassified music disk in a classified computer. (Tr. 61-63.)

The SOR also alleged that in 1999, Applicant improperly transported classified hard drives, zip drives and zip discs from one Sensitive Compartmented Information Facility (SCIF) to another, in violation of Paragraph 5-400 of the National Industrial Security Program Operating Manual (NISPOM), dated January 1995. (SOR ¶ 2.a.) Applicant admitted the action. He explained that he knew how to remove classified materials from a SCIF and was also aware of the proper wrapping procedures required for taking classified material out of a building. However, on the day in question, he was charged with moving classified material on a cart across a lobby between two SCIFs. He did not wrap the materials and did not know that he was required to wrap the materials as he took them across the lobby from one SCIF to another. A security official walked with him as he pushed the cart carrying classified material. She told him that he was required to cover the classified material as he transported it across the lobby, which was an unclassified space between two SCIFs. Applicant, who was new to the classified environment and had not previously known about the requirement, complied with it thereafter. He also reported this incident during his polygraph interview. (SOR; Answer to SOR at 3; Tr. 63-65.)

Also in 1999, Applicant removed a password list from a computer and took it to his home, in violation of another government agency's security policy. This incident was alleged at SOR ¶ 2.b. Applicant was responsible for creating user accounts and passwords. After creating such a list, he put it in his back pocket, intending to take it back through a SCIF and to place it in a safe. He then went on to other administrative tasks. When he left his work site at the end of the day, he forgot that he had the list and inadvertently took it home with him. When he discovered the list, he burned it. The next day, he reported the incident to his security officer, who commended him for reporting the incident but did not brief Applicant on his security responsibilities. The security officer observed that the list was at low risk for compromise because it was not associated with the classified system. Thereafter, when Applicant acquired password lists in the course of his daily work, he put them in an envelope to remind himself that he had the lists in his possession and was responsible for placing them in a safe. When the three security incidents occurred in 1999, Applicant had not had any organized training in handling situations dealing with classified information that occurred during the course of his employment. (SOR; Answer to SOR, dated May 6, 2009, at 3-4; Tr. 65-66.)

The SOR alleged at ¶ 2.c. that from October 2003 to October 2004, Applicant violated the need-to-know policy by discussing classified launch information with a co-worker without first determining the co-worker's access and level of clearance, in

violation of Paragraph 5-500 of the NISPOM. Because he believed that dates were not correct, Applicant denied the allegation at his hearing. (*See* Tr. 37-39.) Applicant admitted he and the co-worker had a five-minute conversation on one day, and he denied that he had held unauthorized communications with the individual for a 12-month period. Applicant provided the following additional information:

> We were actually cleared at the same level but I didn't know his level- - - I didn't know what programs he had been read into. So, this was again like I said a five-minute conversation and I made an illusion or I alluded to a particular launch that had something to do with a site that we both had supported. No classified information was discussed. But at that time I realized that we hadn't had a third party introduction so I didn't know whether or not he had been read into the particular program so we stopped talking about it and never discussed it since.

(Tr. 38.)

Applicant further stated: "Though no classified information was communicated, I learned the importance of not alluding to programs at the risk of revealing need-to-know information. I have never disclosed classified information to anyone without first determining his or her level of access before or after this incident." (Answer to SOR, dated May 6, 2009, at 4.)

The SOR alleged at ¶ 2.d. that each day, from February to May 2005, Applicant carried an unclassified floppy disc in and out of secure areas and facilities, which was a violation of another government agency's security policies. In his answer to the SOR, Applicant denied the allegation and stated that it did not constitute a failure to properly handle protected information or to comply with another agency's security policy. He explained that he self-reported the incident and also may have discussed it in a polygraph interview in September 2005, but he learned later from his security officer that he was permitted to carry discs in and out of a SCIF as long as they were virus scanned and labeled "unclassified." The person who issued him the floppy disc assured him that the disc had been labeled and scanned to comply with another government agency's security policy. (Answer to SOR, dated May 6, 2009, at 4; Tr. 39-42.)

In February 2005, Applicant reported for work in a SCIF. He hung up his coat and forgot that he had left his cell phone in his coat pocket. At the end of the day, he put on his coat, put his hand in his coat pocket, and discovered his cell phone. This incident was alleged at SOR ¶ 2.e. (Tr. 66-67.)

Because he had heard that it was a security violation to have a cell phone in a SCIF, Applicant immediately went to his security officer and reported the incident. The security officer asked Applicant to provide an e-mail incident report, which he did. Applicant did not receive a security briefing or remedial training from his employer as a result of reporting the incident. In his answer to the SOR Applicant stated: "I discussed this issue with my [personnel security officer] who explained it's a very common

occurrence for people to inadvertently carry their cell phone into the SCIF. I have only done this once unintentionally, and have since then refrained from removing my cell phone from my vehicle during SCIF work days." (Answer to SOR, dated May 6, 2009, at 4; Ex. 6; Tr. 67.)

From about November 2004 to September 2005, while working as a system administrator, Applicant was tasked with updating operating system patches on a classified computer system. The SOR alleged at ¶ 1.b. that Applicant "routinely transferred patches for certain operational systems from an unclassified computer to a classified computer system, downloading a majority of these patches from the Internet and placing them on . . . read/writable discs and downloading them onto a classified system." In order to accomplish this task, Applicant would copy the patches from the unclassified computer to a CD. After copying the patches to the CD, and before putting the CD in a classified computer system, it was necessary to apply a read-only software lock on the CD so that nothing further could be copied to it. (Answer to SOR, dated May 6, 2009, at 2; Tr. 68-69.)

Applicant did not know he was required to apply the lock to the CD before putting it into the classified computer system. Additionally, on one or two occasions, he removed an unlocked CD from a classified computer, returned it to the unclassified computer, added additional patches, and added it to the classified computer again. One of Applicant's more experienced co-workers explained to him that it would be an improper use of government equipment not to lock an unclassified CD before putting it in a classified computer. Applicant went to his security officer to verify his co-worker's advice. Applicant received no remedial security training after this event. (Answer to SOR, dated May 6, 2009, at 2; Tr. 70-72.)

The SOR alleged in ¶ 1.c. that in about June 2006, Applicant granted himself elevated domain access without prior authorization or permission. Applicant admitted granting himself elevated domain access, without following the regular procedure of requesting permission from the relevant system administrator, in order to carry out classified duties that mirrored unclassified duties for which he held elevated domain access. Applicant admitted that he did this once. He stated that while he had not been briefed on the issue, his common sense told him that "[i]f you want to get higher access and you're another system administrator, go talk to the guy who administers that system and he'll give it to you." (Tr. 73-74.)

Applicant further explained that in his effort to get the job done, he did not reflect on the need to seek permission. He noted that he was responsible for performing the same work on the classified system as on the unclassified system, and to perform the work on the classified system, he required elevated domain access. In his answer to the SOR, he stated: "I admit making this decision was [imprudent], but that it occurred only once and I now frequently consult management and security before performing any action that may be questionable." (Answer to SOR, dated May 6, 2009, at 2-3; Tr. 74.)

The SOR alleged at SOR ¶ 1.d. that in about 2006, Applicant left his user account open and unattended without password protection. Applicant denied the allegation and asserted that it overstated the vulnerability of his account to unauthorized access. He explained that he was troubleshooting password and authentication issues on a classified system, and to complete his testing of the system, he had "to blank-out my account password which would enable login without typing a password." (Answer to SOR, dated May 6, 2009.)

Applicant further explained that he worked on the troubleshooting and password issues for about a week and logged out of this account daily. He then moved to other assignments and forgot about the account. He remembered the account about six months later. When he accessed the account, he realized that it was still without a password. He disabled the account immediately and verbally reported the incident to responsible security personnel. The security officer to whom Applicant gave his verbal report advised him to be more careful in the future, and requested that he provide a written report of the incident. Applicant provided his security office with an e-mail that discussed the incident in greater detail. He stated that he had checked the server and found no evidence that anyone had used his user name to enter the classified system during the time when his account had no password. Applicant received neither a formal notice of a security violation nor remedial training following his report of the incident, and his access was not revoked. (Answer to SOR, dated May 6, 2009; Ex. 5; Tr. 31-37, 73-77.)

The SOR alleged that the security concerns alleged under Guidelines M and K also raised security concerns under Guideline E, Personal Conduct (SOR ¶ 3.a.). When Applicant was interviewed by a polygrapher in September 2005, he tried to think of any possible issues that might affect his veracity or security worthiness. He told the polygrapher that between mid-2004 and May 2005, he drove his vehicle while intoxicated on at least five occasions. This behavior was alleged at SOR ¶ 3.b. In his answer to the SOR, Applicant denied the allegation and asserted that he had no way to determine if his conduct demonstrated intoxication as defined by the law of his state. Applicant has never been arrested for driving under the influence of alcohol. He stated that he has not driven his vehicle when he has thought he might be intoxicated for about 3 ½ years. (Answer to SOR, dated May 6, 2009, at 5; Tr. 43-49.)

The SOR alleged at ¶ 3.c. that Applicant's security clearance and program access were revoked in October 2006 by another government agency "as a result of a series of security violations that raised questions concerning [his] ability to protect sensitive and classified information." The allegation also recited in SOR ¶ 3.c. that Applicant's appeal of the revocation was denied by another government agency in May 2007. The 2006 revocation by another government agency was based on the same adverse facts alleged in the SOR. (Tr. 53-54.)

Applicant stated that in the three years since losing his security clearance, he had grown greatly in technical competence and awareness of his security responsibilities. He stated that his increased competence had led his employer to

entrust him with greater responsibilities, which, in turn, had led him to increase his technical skills. In 2007 and 2008, he took additional courses in hardware and software storage architecture in order to be better able to serve the information technology needs of his employer. (Tr. 51-53, 57.)

Applicant also reported maturity in his personal life. As the father of a large family, he is aware of his responsibility to lead by example. He reported that his alcohol intake had diminished as he assumed more familial responsibilities. He resolved never to drive a vehicle if he felt intoxicated. Applicant's witness, a friend from his college years, praised Applicant's moral character and integrity. The witness holds Applicant up as a model to his own children and tells them: "[Y]ou need to behave as this man does. He does the right thing even when he's in bad circumstances. Even to the detriment of himself, he does what he considers right and what is truthful." (Tr. 44-49, 52-53, 100.)

Applicant's current manager, who has known him for 10 years, provided a letter of character reference on his behalf. In her letter, the manager praised Applicant's strong technical skills, ability to mentor other employees, dependability, and reliability. She observed that Applicant "has always been the technical backbone of the team" and "encourages the team to document technical processes once they have been figured out so that it doesn't have to be figured out in the future." The manager also provided the following observation:

> I understand the concerns you have listed regarding [Applicant's] past actions while he had a security clearance but I do not believe there will be any more issues of poor judgment. I believe that some of the non-compliance with rules regarding information technology may have occurred while [Applicant] was coming up to speed with working in this environment. Too often the system administrators are so busy with putting out fires that they forget the password list is in their pocket or folder and mistakenly go home with it still there. Sometimes in a rush to get a system going, they forget that carrying a classified hard drive or CD from one building to another is not acceptable. I do not feel that any of the issues that have come up in the past were done by [Applicant] with any malicious intent behind them. I know [Applicant] is truly dedicated to the mission of the work we do here and maybe he was so focused on getting the users back up and working so the mission could be accomplished that he wasn't as careful with the smaller, yet important, security steps.

(Ex. C.)

Additional co-workers, supervisors, and personal friends also provided letters of character reference on Applicant's behalf. They praised him as technically proficient, diligent, conscientious, truthful, dedicated, and a hard worker. They identified him as productive and dedicated to the mission of his office. One co-worker, who has worked with Applicant for seven years, praised Applicant's security awareness and respect for the rules and procedures that ensure data integrity. He observed that Applicant's

heightened conscience and desire to protect classified information led him to focus on past small mistakes. Another manager observed that "the overwhelming share of [Applicant's] actions were proper and positive in ensuring that information was properly handled---only a few problems were self-reported by [Applicant], who is very diligent in that regard." (Ex. A; Ex. B; Ex. D; Ex. E; Ex. F; Ex. G.)

Applicant's performance evaluations from 2006, 2007, and 2008 praised Applicant as "conscientious and dependable." The quality of his work was identified as "excellent," "superb," and "critical to the success of the team." He received individual or small team spot awards in 2005, 2006, and 2008. (Ex. H; Ex. I; Ex. J; Ex. K; Ex. L; Ex. M.)

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, and it has emphasized that "no 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 Applicant's 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, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

When evaluating an applicant's suitability for a security clearance, an administrative judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are 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, the administrative judge applies these guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's over-arching adjudicative goal is a fair, impartial and common sense 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, the Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The Applicant has the ultimate burden of persuasion as to obtaining 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 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

Use of Information Technology Systems

AG ¶ 39 describes the Guideline M security concern as follows:

> 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.

Between 1998 and 2006, Applicant was involved in four incidents of noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems. The first incident occurred in 1998 or 1999, when he inserted an unclassified music disc in a classified computer. The second incident occurred in 2004 and 2005, when he failed to put a read-only software lock on a CD before inserting it into a classified computer and transferring operating system patches copied from an unclassified source. The third incident occurred in June 2006, when he granted himself elevated domain status without prior authorization or permission in order to carry out his assigned duties. The fourth incident occurred in 2006, when

Applicant left his user account without password protection for approximately six months. These incidents raise security concerns under AG ¶¶ 40(a), 40(e), and 40(f). AG ¶ 40(a) reads: "illegal or unauthorized entry into any information technology system or component thereof." AG ¶ 40(e) reads: "unauthorized use of a government or other information technology system." AG ¶ 40(f) reads: "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."

There are three conditions that could mitigate Guideline M security concerns. If "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," then AG ¶ 41(a) might apply. If "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," then AG ¶ 41(b) might apply. Finally, if "the conduct was unintentional or inadvertent and was followed by a prompt good-faith effort to correct the situation and by notification of supervisor," then AG ¶ 41(c) might apply.

Applicant's insertion of an unclassified music disc into a classified computer occurred in 1998 or 1999, soon after he began working in information technology. He did not know that putting an unclassified music disc in a classified computer was an unauthorized use of a government information technology system. When he questioned a security officer and learned that his action was not authorized, he never did it again.

In 2004 and 2005, Applicant carried out an assignment to update operating system patches on a classified computer. He did not know that he was required to use a read only lock on the CD containing the materials to be transferred to a classified computer system. When he learned from a co-worker that this was a requirement, he verified it with a program security officer and thereafter complied.

In 2006, he granted himself elevated domain status without prior authorization or permission. While Applicant had not received specific training on the subject, he suspected that he should request permission for elevated domain status from a system administrator. At the same time he was aware that his on-going duties required that he use and exercise the elevated domain status. In the interest of getting the job done, he granted himself the elevated domain status. Upon reflection, he concluded that his decision was imprudent. He never repeated the action, and when similar issues arise, he consults his security officer before initiating action.

In 2006, Applicant used his account to troubleshoot password and authentication issues. He blanked out his password, which enabled him to logon without typing a password. After working on the password and authentication issues, he signed out of his account and went on to another project. The account was not password protected for six months. No entries were made on the account and no security breaches occurred. When Applicant discovered the status of his account, he disabled it

immediately and reported the situation to his security officer. He filed a report. His security officer advised him to be more careful in the future. He received neither a notice of security violation nor remedial training. His access was not revoked by his employer.

Three years have passed since the security concerns alleged in SOR ¶¶ 1.c. and 1.d. Nearly five years have passed since the security concern alleged at SOR ¶ 1.b., and ten years have passed since the security concern alleged at SOR ¶ 1.a. At his hearing, Applicant provided testimonial and documentary evidence to establish that the Guideline M conduct alleged in the SOR is not likely to recur and does not cast doubt on his present reliability, trustworthiness, or good judgment. He also established that the alleged actions were either of a minor nature or done in the interest of organizational efficiency. Moreover, he established that the alleged conduct was unintentional or inadvertent, and it was followed by notification of a supervisor or security official and a good-faith effort to correct the situation. Accordingly, I conclude that AG ¶ 41(a), AG ¶ 41(b), and AG ¶ 41(c) apply to the facts of Applicant's case.

Guideline K, Handling Protected Information

AG ¶ 33 describes the Guideline K security concern as follows: "Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information. . . ."

Applicant credibly established that the facts alleged in SOR ¶ 2.d. did not constitute a violation of another government agency's security policy. Accordingly, that allegation is concluded for Applicant.

In 1999, Applicant learned that he was improperly transporting classified hard drives, zip drives, and zip discs from one SCIF to another on the same floor and in the same building. Also in 1999, Applicant removed a password list from a computer, put it in his pocket, forgot he had it in his pocket, and discovered it when he arrived home. In about 2003 or 2004, he had a brief conversation with a co-worker in which a reference was made to a launch. Applicant realized he did not know the co-worker's level of access and he discontinued the conversation as inappropriate. In 2005, Applicant left his cell phone in his coat pocket in a SCIF during one work day. These actions raise security concerns under AG ¶ 34 (g), which reads: "any failure to comply with rules for the protection of classified or other sensitive information."

Under Guideline K, there are three mitigating conditions. AG ¶ 35 (a) reads: "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." AG ¶ 35 (b) reads: "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities." AG ¶ 35(c) reads: "the security violations were due to improper or inadequate training."

The incidents that gave rise to security concerns occurred in 1999, 2003 or 2004, and 2005, and they are therefore not recent. Applicant's security incidents happened under unusual circumstances; he reported them and sought clarification from supervisors or security officers about how to handle them properly in order to avoid security problems in the future.

Applicant appears to have had general periodic security briefings, but he was not formally trained or made aware of many day-to-day details in protecting classified information. In his concern to protect classified information, he remembered every infraction, real or suspected. However, he also took it upon himself to seek answers from his supervisors and security officers when he had questions about security issues and how to protect classified information. He responded favorably to their suggestions, and he now demonstrates a very positive attitude toward the discharge of his security responsibilities. I conclude that, when viewed in light of Applicant's present reputation for care and diligence, it is not likely that similar incidents will occur in the future, and these incidents do not cast doubt on Applicant's current reliability, trustworthiness, or good judgment. None of the alleged security concerns resulted in the compromise of classified information. I conclude that AG ¶¶ 35(a), 35(b), and 35(c) apply to the facts of Applicant's case.

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." AG ¶15.

Applicant argued that the allegation at SOR ¶ 3.c. was inconsistent with the adjudicative process specified at ¶ 2(b) in the Directive because it relied not on Applicant's own conduct but on an adjudication of his security worthiness arrived at by another government agency. Further, Applicant argued that Appeal Board precedent required that an administrative judge not defer to a previous adjudication based on the same underlying facts unless it could be established that the other agency's revocation had a security significant independent of the underlying reasons for the revocation. *See* ISCR Case No. 03-09212 at 5 (App. Bd. May 10, 2006). (Tr. 53-54, 123-124.)

Applicant argued persuasively that the SOR allegation at ¶ 3.c. did not identify a disqualifying condition under the Directive and Appeal Board precedent. I conclude that the other government agency's 2006 revocation of Applicant's security clearance did not have security significance independent of the underlying reasons for the revocation. Accordingly, I conclude the allegation at SOR ¶ 3.c. for Applicant.

The amended SOR alleged that Applicant's failure to comply with rules and regulations pertaining to information technology systems and his deliberate or negligent failure to comply with rules and regulations for protecting classified information also raised security concerns under Guideline E, Personal Conduct. Specifically, allegations

of Appellant's alleged personal conduct related to allegations in SOR ¶¶ 1.a. through 1.d, and ¶¶ 2.a. through 2.e. The amended SOR alleged at ¶ 3.a. that Applicant's conduct under Guidelines M and K raised doubts about his judgment, reliability, and ability to comply with laws, rules, and regulations.

Additionally, the SOR alleged, under Guideline E, that Applicant's self-reported statement that for about a year, during 2004 and 2005, he drove his vehicle five times while intoxicated raised security concerns. Applicant denied this allegation, pointing out that he had no way of knowing if he was legally intoxicated when he drove his vehicle at those times.

Applicant identified ten incidents, occurring during the period from 1998 to 2006, which he believed violated security regulations. He reported these incidents when he had an interview with a polygrapher. The allegations at SOR ¶¶ 3.a. and 3.b. raise security concerns under AG ¶ 16(c), which reads:

> Credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other since 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.

I have considered all of the Personal Conduct disqualifying conditions, several of which appear to have applicability in this case. If "the offense is so minor, or so much time has passed, or the behavior is so infrequent, or if 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," then AG ¶ 17(c) might apply. If "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," then AG ¶ 17(d) might apply.

None of the nine Guideline M and Guideline K incidents that Applicant reported gave rise to a written or formal security violation or to remedial training. When he reported these incidents to his manager or to a security officer, Applicant was advised to be more careful in the future. Applicant diligently sought direction from his managers and security officers so that he could improve his security awareness.

Applicant reported that he drove while intoxicated five times in 2004 and 2005, and this behavior was alleged at SOR ¶ 3.b. The record reflects that Applicant has never been arrested for driving under the influence of alcohol. At his hearing he credibly stated that he no longer drinks as much as he once did, and he does not drive if he has been drinking. In his personal life, Applicant has taken positive steps to avoid any untrustworthy, unreliable, or inappropriate behavior related to alcohol use and driving. In

his personal and his professional life, Applicant consciously sought to avoid repeating behavior that he knew raised security concerns. I conclude that the mitigating conditions at AG ¶¶ 17(c) and 17(d) apply to the facts of Applicant's case.

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 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.

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. Applicant is a mature adult. He holds himself to a very high standard of rectitude. Several of the security incidents attributed to him resulted from a lack of training and information. He has learned from his mistakes, and he now does not hesitate to seek timely and sufficient information to protect the information he is entrusted with.

I observed Applicant carefully at his security clearance hearing. I found him to be a serious and responsible person. I believe it is highly unlikely that in the future he will fail to carry out any of the responsibilities of a person entrusted with a security clearance and the protection of classified information. I conclude that he is not a security risk.

Overall, the record evidence leaves me with no questions or doubts as to Applicant's judgment and eligibility and suitability for a security clearance, and I conclude Applicant rebutted and mitigated all security concerns arising under Guideline M, Guideline K, and Guideline E.

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
Subparagraphs 1.a. through 1.d:	For Applicant
Paragraph 2, Guideline K:	FOR APPLICANT
Subparagraphs 2.a through 2.e.:	For Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraphs 3.a. through 3.c.:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Joan Caton Anthony
Administrative Judge