DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-08119
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Borgstrom, Esquire, Department Counsel
For Applicant: Dennis J. Sysko, Esquire

March 18, 2010

Decision

CURRY, Marc E., Administrative Judge:

Between 1995 and 2004, Applicant mishandled classified and/or sensitive information on multiple occasions and downloaded an unclassified phone directory from a coworker's computer without his knowledge or permission. This conduct generates security concerns under Guidelines K, Handling Protected Information, M, Use of Information Technology, and E, Personal Conduct. Applicant has committed no security infractions in more than five years. In that time, his security awareness has been outstanding. Applicant has mitigated the security concerns. Clearance is granted.

Statement of the Case

On July 14, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns as outlined above. 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) effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant answered the SOR on August 4, 2009. He denied all of the allegations and requested a hearing. The case was assigned to me on October 2, 2009. On November 10, 2009, a notice of hearing was issued scheduling the case for December 2, 2009. The hearing was conducted as scheduled. I received nine government exhibits, seven Applicant exhibits, and the testimony of four witnesses for the Applicant. The transcript was received on December 10, 2009.

Preliminary Rulings of Procedure and Evidence

I. Applicant's Motion *in Limine*

Government Exhibit (GE) 2 is Applicant's Response to DOHA Interrogatories, signed on January 5, 2009. As originally proffered by Department Counsel, it consisted of among other things, records from another DoD agency including a 2004 clearance decision revoking Applicant's access to Sensitive Compartmented Information (SCI), and three investigative reports, on which the agency based its decision. The investigative reports were summaries of polygraph examinations. In total, GE 2, as originally proffered, was 166 pages long.

On November 30, 2009, Applicant's counsel filed a Motion *in Limine* seeking to exclude the investigative reports and the clearance decision. In doing so, he argued that the polygraph examinations are inadmissible hearsay and are inherently unreliable absent the opportunity to cross examine the investigator who conducted them. As for the clearance decision, he argued that it, too, was inadmissible hearsay.

In a response filed on December 1, 2009, Department Counsel withdrew sections of proposed GE 2 pertaining to polygraph examination reports (pages 137-141, and 144-152). Citing Appeal Board case law, he argued that the clearance decision was admissible because the Federal Rules of Evidence (FRE) are not strictly applied to such documents (ISCR Case No. 02-12199 (App. Bd. August 8, 2005)).

Department Counsel's analysis is correct. In ISCR litigation, the development of a full and complete record supersedes the technical application of the FRE (Directive ¶ E3.1.19). The admissibility of official records such as clearance decision statements are instead governed by Directive ¶ E3.1.20, which states that they are admissible without authenticating witnesses so long as they have "been furnished by an investigatory agency pursuant to its responsibility in connection with assisting the Secretary of Defense, or the Department or Agency head concerned, to safeguard classified information within industry under E.O. 10865."

Although the clearance decision was not furnished by an investigatory agency, as described in Directive ¶ E3.1.20, it was furnished by an authenticating witness - Applicant himself (*see* Applicant's testimony in response to Department Counsel's *voir*

dire questions regarding the clearance decision's authenticity (Tr. 44-59)). Consequently, I denied Applicant's Motion *in Limine* and admitted the clearance decision.

II. Motions Regarding SOR Subparagraph 2.b.

SOR subparagraph 2.b reads as follows:

> Between 1994 and 2004, you deliberately misused Government sponsored computers by inadvertently not write-protecting diskettes before using them on a higher security level system and then re-using them on a lower security level system.

At the hearing's conclusion, Department Counsel moved to amend the allegation by striking the words, "deliberately," and "inadvertently". Appellant's counsel opposed the motion, and moved to strike SOR subparagraph 2.b.

I denied both motions. However, I agree with Applicant's counsel's contention that SOR subparagraph 2.b is nonsensical because conduct cannot be both "deliberate" and "inadvertent." Consequently, I resolve SOR subparagraph 2.b in Applicant's favor.

Findings of Fact

Applicant is a 51-year-old single man with no children. He earned a bachelor of science degree in chemistry in 1980 (GE 1 at 1). After working for a few months as a chemist in the federal government shortly after graduation, he took a job with a defense contractor (*Id.*). He has been working for this employer ever since. According to a coworker who has shared an office with him since October 2007, he is "someone of high trust and reliability" (AE E at 18).

Applicant began his career with the defense contractor as an associate software engineer tasked with coding hardware diagnostics and assisting with hardware debugging of custom signal processing systems (GE 2 at 61). By 1987, Applicant's employer had promoted him to senior software engineer (*Id.*).

In 1995, Applicant's employer re-assigned him to a different location where he remained through 2004 (Tr. 72). During this time, he held a Top Secret clearance with SCI access. In March 1996, his employer promoted him to the position of senior field engineer (GE 2 at 61). Applicant's duties included managing software upgrades, interfacing with factory engineers, and solving system anomalies (*Id.*). He performed these tasks on site at a Sensitive Compartmented Information Facility (SCIF) that used his company's information system. In 2001, Applicant's employer promoted him to the position of site engineer in charge (*Id.*). In this position, he supervised 12 employees and supported multiple operational systems (*Id.*). He remained in this position through October 2004 (GE 1 at 1; Tr. 81).

Applicant's home office communicated with him through e-mail sent from an unclassified system. The only accessible information system at the SCIF was classified, and the program host prohibited Applicant and his team members from using it to correspond with their home office (GE 2 at 119 - Affidavit of Coworker X, dated November 3, 2004; Tr 74). Consequently, the only method of sharing unclassified correspondence between the SCIF contractors and the home office was through home e-mails[1] (GE 2 at 122 - Affidavit of Coworker Y, dated November 3, 2004).

Applicant's home office required him, among other things, to prepare a weekly unclassified report summarizing the status of the upkeep of the information systems for which he was responsible (GE 3 at 11). This involved maintaining daily logs, then compiling them into one report at the end of each week, and e-mailing them to the home office. Applicant prepared and maintained the unclassified logs on the program host's computer diskettes.[2]

Because Applicant could not use the program host's e-mail system to send his weekly reports to the home office, he had to print all of the daily program logs from the program host's diskettes, take them home, retype them onto his company-issued home computer, then prepare and e-mail the reports to his supervisor (*Id.;* Tr. 77, 173). Printing the information from the diskettes and taking this information home posed no problem; however, the program host's security regulations forbid taking any diskettes from the facility (GE 3 at 11).

Because of the labor-intensive nature of this task, Applicant began to fall behind on his weekly reports. Once in 1998, he skipped the step of printing the daily program logs and taking them home. Instead, he took home a diskette containing the daily program logs, inserted it into his company-issued home computer, copied the file containing the daily program logs, and used it to prepare his weekly report (Tr. 88). He did so because he was tired of having to retype the program logs onto his home computer each time he prepared a weekly report (Tr. 135, 171; GE 2 at 29). He knew that the program host's security regulations prohibited him from taking any magnetic media from the SCIF (GE 2 at 28). Also, he knew that the SCIF security guards would have made him return the diskette if he had attempted to check it out of the SCIF (Tr. 132). Applicant, therefore, concealed the diskette from the SCIF security guards by concealing it in his pants pocket when he exited the SCIF (*Id.;* Tr. 132). He returned it the next day (Tr. 132; GE 2 at 29).

This was not the first time Applicant improperly removed a diskette from a classified facility (Tr. 173). In 1995, his employer tasked him with writing an operations manual for an unclassified program (GE 2 at 29; Tr. 86). This work was to occur during a temporary duty assignment (TDY) at another satellite location (GE 3 at 8). While

[1]As time progressed, this discrepancy was fixed (AE G).

[2]All of the diskettes at the SCIF were labelled 'SECRET" (*Id.*).

working on the assignment, Applicant downloaded two files from a classified computer system onto two diskettes, removed the diskettes from the facility, and referred to the information on the diskettes, using his company-issued computer, to help him prepare the manual (*Id.*). While preparing the manual, Applicant discovered that one of the programs he had downloaded was classified (GE 3 at 9). He acknowledged that he did not check the document thoroughly before downloading it (*Id.*). After discovering that one of the programs was classified, Applicant deleted it from his computer (GE 2 at 30). He does not recall whether he deleted it from the diskette (*Id.*). No record evidence indicates that he knew one of the diskettes contained classified information before he took it from the facility, or that he surreptitiously removed them from the facility knowing that one contained classified information.

Applicant reported neither security violation to his facility security officer until approximately nine years later, in February 2004, after a routine polygraph examination that another DoD agency conducted (GE 3 at 9; *see also* GE 3 at 50 - Security Violation Report, dated February 9, 2004). He did not immediately report these security violations because he was afraid of losing his security clearance (Tr. 135).

Over the years, Applicant took other materials from the SCIF to assist him in his work at home (Tr. 125-127). The program host prohibited removing material that referenced the program regardless of whether the material was classified (Tr. 126). Applicant acknowledged that a few of the materials he took home "were ones that if somebody was familiar with the program [he or she] could read that piece of paper and figure out it was about that program" (Tr. 127). On some occasions through February 2004, he concealed unauthorized information from the SCIF security (GE 3 at 27). He knew this was against SCIF regulations, but considered that adhering to these particular SCIF regulations impeded his job responsibilities, and disclosing his violations would be "time-consuming and embarrassing (Tr. 135).

Twice in 2003, and once or twice between 1994 and 2003, Applicant accidentally removed e-mails with classified banners to his home (GE 2 at 27). He did not know whether the body of the e-mails contained classified data or if the messages were accidentally marked classified (*Id.*). Each time this happened, he returned them to the SCIF and shredded them (*Id.*). He did not report this activity to the requisite security authorities. He never intentionally removed classified e-mails (Tr. 89).

In 1997, Applicant copied an unclassified phone directory from a coworker's computer without his knowledge or permission (Tr. 107). The coworker's work station was located in the same room as Applicant's work station (Tr. 107). One day, Applicant noticed that his coworker left his computer unattended and unsecured, with a phone directory on the screen. He perused it, and concluded that he needed some of the contacts in the phone directory for "operational support" (Tr. 108). He then copied the file onto one of his floppy disks, then copied it onto his computer (Tr. 108). The disk used was classified at the same level as the coworker's computer (Tr. 142). The phone directory was not classified (GE 3 at 11). After copying the information, Applicant did not tell his coworker (Tr. 108). Applicant did not report the 1997 misuse of the information

system until seven years later, in February 2004, after his second meeting with the SCIF's facility security officer (GE 3 at 57).

In 2003, Applicant prepared a presentation on a Secret-level laptop (Tr. 93). The presentation was unclassified (Tr. 94). Shortly before making the presentation, Applicant decided to spell check it; however, the laptop lacked a spell-checker program (Tr. 93). Applicant then saved the presentation on a 3.5 inch floppy disk and inserted it into a computer system, classified at a higher level, that had the spell-checker program (Tr. 94). He then spell-checked the presentation and made the necessary corrections. He failed to write-protect the floppy disk before inserting it into the higher level-classified computer, as required by security regulations (Tr. 95).

In the nine years Applicant worked at the SCIF, he ran programs saved on disks containing lower-level classified information on higher-level systems between one and two hundred times (Tr. 179). He may have failed to write-protect the disks on two other occasions (Tr. 179).

In February 2004, an investigative agent subjected Applicant to three polygraph examinations. In April 2004, the investigative agent interviewed Applicant. In June 2004, the agency that conducted the investigation issued a clearance decision revoking Applicant's access to SCI (GE 3 at 25).

After Applicant's access to SCI was revoked, his employer transferred him to another facility. He continued to maintain a Top Secret clearance (Tr. 84). According to the Information Systems Security Officer (ISSO) of the facility where Applicant worked between 2004 and 2007:

> Applicant conducted himself in a professional and security conscious manner. He was proactive in his security responsibilities and even helped to secure the proper marking of media, as required in a classified area (AE A at 13).

Since losing his access to SCI in 2004, Applicant has received counseling regarding security procedures (GE 3 at 14). The current facility where he works is governed by "very very clear" security procedures, unlike the facility where he worked between 1995 and 2004 (Tr. 160).

Other than a 19-month period between March 2006 and October 2007, Applicant has continuously held a security clearance since 1980.[3] He had only committed one security violation in the 15 years before he was assigned to the satellite facility in 1995 (Tr. 116).

According to a coworker who Applicant supervised between 2002 and 2004, Applicant displayed no irresponsibility in his attitude toward the discharge of his security

[3]The record is unclear as to why Applicant did not hold a security clearance during this period.

responsibilities, even though the security rules at the SCIF often added additional work (AE A at Tab I). According to Applicant's supervisor from 1993 to 1996, Applicant "always seemed security conscious . . . [and] maintained a positive attitude about security" (AE E at 10). Applicant's supervisor from 2001 through 2002 "directly observed nothing but sheer dedication on [Applicant's] part regarding program security and functionality" (GE 3 at 18). When Applicant sought a new position within the company in 2007, his ex-supervisor "had no hesitations in recommending him . . . given [his] past dealings with him" (*Id.*).

The ISSO at Applicant's current assignment both testified and provided a reference letter. He has held this position since Applicant began working at the program in October 2007 (AE E at 9). Of the 40 to 50 people who work at the facility he oversees, Applicant is the most diligent in adhering to security practices (Tr. 222). Also, the ISSO noted the following:

> [Applicant] often has had to handle and create classified media in the form of CDs. He has played a key role in ensuring that this form of media is being properly tracked and secured in designated security containers . . . [Applicant] often has been responsible for opening and closing our classified lab . . . During this time, [Applicant] has made it a point to be security conscious and demonstrated his willingness to follow security guidelines (*Id.*).

Since receiving the new assignment in 2007, Applicant has been proactive in clarifying ambiguous security procedures (*Id.*). For example, when tasked with an assignment that involved, among other things, the transfer of classified packages, he identified an ambiguity regarding the company's procedures for transporting such materials, and did not begin the task until the company developed a more precise procedure, which he helped to define and implement (*Id.;* Tr. 217).

The assistant ISSO (AISSO) also provided a reference letter (AE E at 11). His duties include "follow[ing] behind the people that work late to make sure the lab and office areas are secure" (*Id.*). He shared the following observations about Applicant's security awareness:

> Whenever I've come behind [Applicant] I have never seen anything out of order and he has even called me on occasion to clarify procedures when something in the lab fell into a gray area. Several of his questions have caused me to add detail to my security briefing so everyone will know how to react to similar situations. (*Id.*).

The program's advisory engineer has often performed security monitoring of applicant's desk and local safe (*Id.* at 21). They have both always been properly secured (*Id.*).

A licensed, clinical psychologist testified for Applicant (Tr. 182-200). The witness served in the U.S. Army as a military psychologist from 1985 to 1991 (AE G at 3). Since leaving the Army, he has periodically served as a consultant as to the psychological aspects of military-related issues such as administrative discharges, eligibility for specialized schooling, and security clearances (Tr. 184; AE G at 2). He has provided "low-intensity" counseling to Applicant on a monthly basis since approximately 2006 (Tr. 199). They discussed a number of issues including those leading to the revocation of Applicant's SCI in 2004. According to the psychologist, Applicant is now so sensitized to security matters that "when he would give [him] copies of awards that he had received . . . he would blacken out some of the names and some of the locations" (Tr. 201). The psychologist had "never had this happen with any other candidate or subject" with whom he had worked (Tr. 200).

Policies

When evaluating an applicant's suitability for a security clearance, the 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.

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. 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, Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." Applicant has the ultimate burden of persuasion as to obtaining a favorable security decision.

Analysis

Guideline K, Handling Protected Information

Under this guideline, "[d]eliberate 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, and is a serious security concern" (AG ¶ 33). Applicant never knowingly concealed classified copies of e-mails in his pants pocket in order to

circumvent security checkpoints upon exiting a classified facility, as the SOR alleged. Nevertheless, the multiple episodes of mishandling classified and/or sensitive information over the years render the following disqualifying conditions under AG ¶ 34 potentially applicable:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, 'palm' or pocket device or other adjunct equipment; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

Over the years, Applicant negligently removed classified e-mail, and intentionally removed unauthorized information from the SCIF. However, in these instances, he returned the materials to the office the next day, and shredded them. Although Applicant's conduct represents a significant security concern, he had no intent to collect or store it at his home. AG ¶ 34(b) does not apply.

Applicant's negligent downloading of a classified file in 1995 and use of it to prepare an unclassified operations manual triggers the application of 34(c). All of Applicant's security violations trigger the application of 34(g).

AG ¶ 35 sets forth the potentially applicable mitigating conditions. They are as follows:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

The applicability of AG ¶ 35(c) is predicated on an unintentional security breach. Applicant, however, knew that he was violating security regulations when he committed his most significant security breach, the 1998 diskette-removal episode. Consequently, the level of training he received before the security breach occurred is neither relevant nor mitigating. AG ¶ 35(c) does not apply.

Three of Applicant's coworker's submitted affidavits supporting his assertion that the SCIF where he worked from 1995 to 2004 was governed by unusual security rules that, at times, impeded communication with their employer. This does not mitigate Applicant's history of circumventing security regulations. AG ¶ 35(a), as it relates to unusual circumstances, is inapplicable.

Conversely, AG ¶ 35(a), as it relates to the passage of time without recurrence, is applicable. Excluding a 19-month period between March 2006 and October 2007, Applicant has continued to work with classified information. He has not committed any security violations since 2004. The ISSO at his current job assignment characterizes him as one of the most security-conscious employees at their facility.

Applicant completed remedial counseling regarding handling classified information. He is vigilantly committed to adhering to security regulations. His vigilance in identifying potential gaps and ambiguities in his company's security policies has led to the revision of both its security briefings and policies. AG ¶ 35(b) applies.

Guideline M, Use of Information Technology Systems

The security concern under this guideline is set forth in AG ¶ 39 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.

In 1997, Applicant deliberately obtained unauthorized access to a coworker's desktop computer and downloaded an unclassified phone directory onto a floppy disk, then copied it onto his desktop computer. Also, he negligently downloaded classified information in 1995, intentionally removed a classified diskette from a SCIF in 1998, and failed to write-protect a diskette before inserting it onto an information system classified at a higher level in 2003. AG ¶¶ 40(a), "illegal or unauthorized entry into any information technology system or component thereof," and 40(e), "unauthorized use of a government or other information technology system," apply

Applicant has not misused any information technology since 2004. Since then, he has handled information technology in an exemplary manner. AG ¶ 41(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," applies.

Guideline E, Personal Conduct

Under this guideline, "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's conduct triggers the application of AG ¶ 16(d)(1) "untrustworthy or unreliable behavior . . .," and 16(d)3), "a pattern of dishonesty or rule violations." The applicability of these disqualifying conditions is predicated on Applicant's conduct not being "explicitly covered under any other guideline" (AG ¶ 16(d)). Applicant's conduct is covered under both Guidelines M, Use of Information Technology Systems (AG ¶¶ 39-41), and K, Handling Protected Information, (AG ¶¶ 33-35), rendering their discussion under these particular disqualifying conditions superfluous. The mitigating conditions set forth in AG ¶¶ 17(d), "the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur," and 17(e), "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress," apply for the reasons discussed in the previous sections.

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.

Applicant's misconduct reflected a tendency to elevate expedience over security consciousness when performing his tasks. Particularly troubling was the intentional and surreptitious nature of some of his misconduct. Consequently, Applicant's security violations and misuse of information technology generate significant security concerns.

Applicant has not committed any security violations or engaged in any episodes of information systems misuse in more than five years. The remoteness of Applicant's conduct alone, however, is not mitigating, given the seriousness of the conduct.

Since 2004, Applicant has not only avoided committing any additional security violations; he has attended remedial security counseling and demonstrated an enthusiastic, vigilant attitude toward the discharge of his security responsibilities. Specifically, he assisted in the revision of company security policy to eliminate gaps and ambiguities that he had identified. Consequently, Applicant's vigilance has led to an improved security posture of an entire division within his company.

Applicant has worked for his employer for nearly 30 years. He has maintained a security clearance for nearly his entire tenure at the company. He is well respected by his coworkers. One coworker, who supervised him between 2001 and 2002, complimented his dedication to security awareness, which Applicant demonstrated while working for him, and strongly endorsed his application to maintain his security clearance.

As the psychologist who counseled Applicant noted, he is now extraordinarily sensitized to security matters. Under these circumstances, the seriousness of the conduct is outweighed by the presence of rehabilitation and the minimal likelihood of recurrence. Applicant has mitigated the 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 K:	FOR APPLICANT
Subparagraphs 1.a - 1.c:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraphs 2.a - 2.b:	For Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraphs 3.a - 3.b:	For Applicant

Conclusion

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

MARC E. CURRY
Administrative Judge