DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	
	)	ISCR Case No. 09-06685
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Richard Stevens, Esquire, Department Counsel
For Applicant: *Pro Se*

September 27, 2011

Decision

CREAN, THOMAS M., Administrative Judge:

Based on a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Statement of the Case

On May 20, 2005, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to retain a security clearance he held while on active duty as part of his employment as a consultant to defense contractors. He was granted access to classified information. In August 2008, there was an allegation that Applicant in his role as a consultant to defense contractors possessed classified material in his home in violation of his consulting agreements. After a complete investigation, Applicant's defense contractor employer suspended his access to classified information in December 2008. His employer appropriately notified Department of Defense officials of its action. The Defense Office of Hearings and Appeals (DOHA) could not make the preliminary affirmative findings required to retain Applicant's security clearance. On January 31, 2011, DOHA issued Applicant a Statement of Reasons (SOR) detailing security concerns for improper handling of protected information (Guideline K). 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 in the Department of Defense on September 1, 2006. Applicant acknowledged receipt of the SOR on February 5, 2011.

On February 24, 2011, Applicant answered the SOR denying the six allegations under Guideline K. Department Counsel was prepared to proceed on April 19, 2011, and the case was assigned to me on May 19, 2011. DOHA issued a Notice of Hearing on June 9, 2011, scheduling a hearing for June 22, 2011. I convened the hearing as scheduled. The Government offered eight exhibits, which I marked as Government Exhibits (Gov. Ex.) 1 through 9 and admitted into the record without objection. Applicant testified, and introduced five documents which I marked as Applicant Exhibits (App. Ex.) A through E and admitted into the record without objection. DOHA received the transcript of the hearing (Tr.) on June 30, 2011.

Procedural Issues

Applicant received the Notice of Hearing on June 20, 2011. However, he discussed the hearing date with Department Counsel on April 27, 2011. He is entitled to 15 days advance notice of the hearing. (Directive E3.1.8.). Applicant was prepared and ready to proceed at the hearing on June 22, 2011. He waived the 15 days notice requirement. (Tr. 7-8)

Department Counsel requested that administrative notice be taken of certain provisions of the National Industrial Security Program (NISPOM) pertaining to consultants and facility clearances. I have included a discussion of the NISPOM provisions in my findings of fact below. (Hearing Exhibits I and II)

Findings of Fact

Applicant denied the factual allegations under Guideline K. After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact.

Applicant is 49 years old and served on active duty in the Army for 20 years retiring with an honorable discharge in 2004 as a lieutenant colonel. He is a college graduate and has a master's degree. He is married. He held a security clearance with high level access for his entire active duty career. He was wounded while on active duty and is now disabled. Applicant is an expert on a specific area of weapons systems that is a critical element in the war plan development, evaluation, and approval process for combatant commanders and high level government and coalition officials. (Tr. 11-12; Gov. Ex. 1, e-QIP, dated May 20, 2005**)**

Applicant presented at the hearing as a knowledgeable, hard charging, mission-oriented individual. He demeanor reflected an air of arrogance and he repeatedly invoked his relationship with the commanding general of a senior combatant command who accompanied him as he briefed the President of the United States, the Secretary of Defense, and elements of the Joint Staff on his area of expertise. He also noted that he was sent to brief on his area of expertise the Prime Minister of the major coalition partner for the invasion of Iraq. (Tr. 26-30, 41-42)

When Applicant retired in June 2004, he became a consultant for a number of defense contractors working in his area of expertise on assignments from various combatant commands. The six allegations of improper handling of protected information stem from him receiving, storing, and destroying classified information sent to him at his home office in violation of his consulting agreement and the NISPOM. Applicant's defense contractor employer notified the appropriate Government agency of the security violations. (Gov. Ex. 3, Report of Administrative Inquiry, dated November 26, 2008)

When Applicant retired in 2004, he purchased a home in his wife's home town so she would have family support while he was away on his consulting duties. Close to the house, but on the property, was a building that he renovated to serve as his office. The home office building had a different separate house number. When he received a safe in 2005 to store classified material, he modified the building so it had no windows but had a room that could be locked. The sides of the building were reinforced. He employed one person, his college graduate nephew, to serve as his administrative and business assistant. His nephew had access to the building and did not have a security clearance. Applicant traveled extensively as a consultant and his office assistant was always at the office during business hours. Applicant was never issued a facility security clearance for his office by the Defense Security Service (DSS). One of Applicant's defense contractor employers requested a facility security clearance for his office on June 22, 2007. On July 3, 2007, a DSS representative informed Applicant that a one-person facility does not qualify for a facility security clearance. Instead, the person is considered a "consultant" under the primary contractors account. On July 18, 2007, DSS notified Applicant that processing of the facility security request was discontinued. Applicant acknowledged that he received this notice. (Tr. 26-27, 31-33, 51-58, 71-74; Gov. Ex. 5, Request for Facility Security Clearance, dated June 22, 2007; Gov. Ex. 6, e-mail, dated July 3, 2007; Gov. Ex. 7, Notice, dated July 18, 2007; Gov. Ex. 8, e-mail, dated July 23, 2007)

On July 26, 2005, Applicant signed a consulting agreement with a defense contractor that restricted Applicant's possession of classified information. The agreement provided that Applicant shall not possess classified information away from the premises of the contractor's facility; that the contractor shall not furnish classified information to Applicant at any location other than on the premises of the company or at the supported military agency; and that performance of the consulting services by Applicant shall be accomplished only on the premises of the contractor facility or the supported military agency. His consulting agreements with approximately six other defense contractors had the same provisions on handling classified materials. After signing the agreement, Applicant would go to the location of the supported agency or

the defense contractor employer about two weeks a month to perform his consulting function. The tempo for his visits did not change after he received a safe to hold classified material. The number and frequency of his visits was changed because of the operational necessity of the combatant command. (Tr. 45-49, 63-66; Gov. Ex 3, Report of Administrative Inquiry, dated November 26, 2008, at 46)

On October 27, 2005, the supported military agency provided Applicant a safe which was certified for storing classified information. Applicant personally transported the safe to his home office which was located in a state hundreds of miles from the supported military agency and the defense contractor's office. Applicant did not bill the contractor or the supported government agency for the cost of the rental truck to transport the safe. Prior to that time, the government agency had also provided Applicant with a secure communication device which was capable of encrypting telephone conversations. (Tr. 26-31, 66-71, 74-77; Gov. Ex. 2, Applicant's statement, dated March 9, 2010; Gov. Ex. 4, Formal Report of Security Incident, dated December 5, 2008, at 72; App. Ex. A, OMNI Secure Terminal User Agreement, dated October 7, 2005; App. Ex. B, Shipping documents, dated October 7, 2005)

Classified information was sent to Applicant at his home office beginning in 2007. Classified documents and CDs were sent to Applicant by the government agency at his home office on May 22, 2007, June 1, 2007, February 19, 2008, March 27, 2008, April 8, 2008, and June 11, 2008. Applicant viewed classified material on the CDs sent by the supporting government agency on his personal laptop computer. After working with the classified material on his laptop, Applicant used a computer program to wipe all information from his computer. His personal laptop was not an authorized computer to view classified information. Another package of classified information was prepared to be mailed to Applicant on August 12, 2008. The person who was instructed to mail the material questioned the authority to mail classified material to a home address. Her concerns started the inquiry into Applicant's authority to receive and store classified information at his home office. A preliminary inquiry was directed by the senior military command over the supported government agency. Prior to this time, Applicant's defense contractor employer did not know he was receiving classified information at his home in violation of his consulting agreement. The preliminary inquiry recommended a formal investigation. A formal investigation was opened on October 2, 2008, and completed in December 2008.

The formal investigation reported that Applicant destroyed all classified information in his possession by August 14, 2008. The safe was returned to the supported government agency on October 17, 2008. On November 10, 2008, DSS conducted a site survey of Applicant's office. Applicant's laptop computer was seized and sent for analysis. A DSS investigator questioned the capability of Applicant's shredder to destroy CDs, as well as his authorization to destroy classified material. A security damage assessment concluded that the laptop did not contain classified information which was consistent with Applicant having used a computer program to clean all material from the hard drive. However, the report concluded that it must be assumed that a compromise of classified information may have occurred. However, it

also concluded that damage to national security is unlikely. (Gov. Ex. 4, Formal Report, at 76-78)

The formal investigation found that procedures and processes were not in place in the supported government agency to prevent classified material from being sent to an unauthorized address. No individual in the agency checked the validity of the address to receive classified material until the seventh package was being mailed. The government personnel did not have an understanding of the relationship between a government contractor and a consultant. The government personnel at the government agency developed a close working relationship and familiarity with Applicant thus facilitating the unauthorized sending of classified information to him. (Gov. Ex. 4, at 79)

Applicant testified that he was extremely busy as a consultant working with soldiers and combatant commands on issues concerning his area of expertise. The joint staff had also contacted him about rewriting their methodology in his area of expertise. He was approached by senior personnel from the supported government agency about issuing him a safe for storage of classified material. He did not question their authority but assumed they had authority to issue the safe and had coordinated with the contractor. He stated the documents on the safe seemed in order and he knew the safe had been inspected and had previously contained classified material. He had little contact or interaction with his defense contractor employer. The first set of material sent in May 2007 was sent by an employee of his contractor employer who was working full time at the supported agency. He indicated he had no reason to question the transfer of the safe or the receipt of classified material. (Tr. 29-31)

Applicant kept meticulous records and accountability of all classified documents sent to him. He was able to account for documents that the government agency did not know that they had sent to him. He provided the proper documents to show that material had been destroyed. He received destruction documents and instruction from the government agency. He destroyed the documents and CDs rather than take the risk of transporting them again through the mail. He destroyed the documents in front of his administrative assistant. His administrative assistant was not cleared to view classified material. The assistant did not view the documents but did view the destruction and signed the destruction certificate. The administrative assistant could not read the data on the discs but could read the paper documents. He informed the assistant of the subject matter of the document being destroyed but did not show the documents to him. (Tr. 32-36; App. Ex. C, Classified Document Control Record, dated August 14, 2008; App. Ex. D, Activity Security Checklist, various dates; App. Ex. E, Security Container Check Sheets, various dates)

Applicant testified that when he was questioned about a facility security clearance by his employer, it was his belief the clearance was needed to be able to transmit his security access information for his consulting travels. He did not know it pertained to the physical location of his office. He thought that the supported command and his contractor employer would provide the physical facility clearance. He had no idea of a link between a contractor's cage code and a facility clearance. In all the conversations he had with facility security officers of the defense contractors he had

consulting agreement with, his understanding was they needed a facility security clearance to manage his security clearance requirements. His focus was on the operational mission and not learning the requirements of security for a consultant. He thought his years of active duty experience in that area provided him with the knowledge he needed. He believes he did due diligence in managing and maintaining the security of the classified material sent to him. (Tr. 36-42, 49-51, 58-63)

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 over-arching 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, 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 burden of persuasion 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.

Analysis

Guideline K, Handling Protected Information

The 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, and is a serious security concern. (AG ¶ 33)

Applicant received, stored, and worked with classified material at his home office in violation of his consulting agreement. His consulting agreement required him to possess classified material only on the premises of the contractor or at the supported government agency. Applicant's home office and the safe containing the classified material were not certified for storage of classified material by the appropriate Government agency as required by the NISPOM. Applicant also viewed classified material on his personal laptop computer which had not been certified for use with classified material. Applicant was informed prior to receiving some of the classified material that he did not have a facility security clearance for his home office. He also permitted a person not cleared for access to classified information to witness the destruction of classified material. His administrative assistant could also read paper documents and was advised of the subject matter on CDs.

These facts raise Handling Protected Information Disqualifying Conditions. AG ¶ 34 (b) (collecting or storing classified or other protected information at home or in any other unauthorized location); AG ¶ 33(c) (loading, drafting, editing, modifying, sorting, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, work processor, or computer hardware, software, drive, system, game board, handheld, "palm" or pocket device or other adjunct equipment); and AG ¶ 33(g) (any failure to comply with rules for the protection of classified or other sensitive information). It does not appear that Applicant deliberately violated the security requirements for his home office. However, he failed to learn, understand, and follow the procedures and requirements for a facility clearance. This failure was more than simple negligence. Based upon the communication he received from DSS before and after he received classified material, he knew there was an issue with the facility clearance. He failed to pursue the issue citing that he was too busy. He took no actions to learn the rules even though he was new to the consulting and contracting business. He assumed he knew the rules, assumed government personnel were knowledgeable on security matters, and he assumed he followed all requirements. Applicant testified extensively about his unique expertise and his prestigious briefings with high ranking officials. He spent a considerable portion of his career working with classified material. He was in a position to question the lack of procedures and the unorthodox ways things were being conducted. He chose not to question them because it was convenient for him. At a minimum, he knew or should have known that his nephew was not cleared to receive or handle classified information even for a short time or witness its destruction. His failure to inquire and act is gross negligence.

I also considered AG ¶ 33(i) (failure to comply with rules and regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent). The formal investigation and damage assessment concluded that a possibility of compromise of classified data could have occurred but that damage to national security is unlikely. I conclude this disqualifying condition is not raised.

The Government produced sufficient evidence to establish the disqualifying conditions in AG ¶¶ 35(b), 35(c), and 35 (g). The burden shifted to Applicant to produce evidence to rebut, explain, extenuate, or mitigate the security concerns under handling protected information. An applicant has the burden to refute an established allegation or prove a mitigating condition, and the burden to prove or disprove it never shifts to the Government.

I considered Handling of Protected Information Mitigating Conditions AG ¶ 35(a) (so much time has elapsed since the behavior, or it 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) (the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude towards the discharge of security responsibilities); and AG ¶ 35(c) (the security violations were due to improper or inadequate training). None of these mitigating conditions apply. The security violations happened only four to six years ago. In the area of security violations, this is a short time ago. The circumstances were not unusual even though the violations were partially attributed to the security failures of personnel from the government agency. While Applicant states he has learned a lot during this process about security requirements for consulting and contractor personnel, he has not presented sufficient information to establish that the violations would not recur. Applicant has not presented any information concerning additional training on security procedures. In fact, he states he is very aware of security requirements from his experience on active duty.

Applicant's position is that after he retired and started working as a consultant for the government agency, he was so busy with work and travel he did not have sufficient time to learn the security requirements for consultants. He intimated he relied on the government and contractor employees to have the authorization to provide the safe and send classified materials to him at his office. They had provided him with a secure telephone previously and he assumed they acted correctly. After receiving the classified material, he followed all rules and regulations to properly account for, manage, safeguard, and ultimately destroy the material.

Applicant has not presented sufficient information to rebut, explain, refute, or mitigate the government's security concern for his failure to properly receive, manage, handle, and safeguard classified material. The requirement in the consulting agreement was clear that Applicant's work with classified material was to be performed at either the contractor's facility or at the government agency. This same requirement was in every consulting agreement signed by Applicant. He moved the safe himself and did not charge his contractor employer for the cost. He then modified his office building to be more secure. Applicant never checked with any official to determine if he had authority

to possess classified material in this office near his home. Classified material was not sent to Applicant until May and June 2007, over two years later. In the same time frame, Applicant learned that a request for him to have a facility security clearance was discontinued since his was a single person office. While he stated he believed the facility security clearance was only needed to permit him to transmit his security clearance when traveling, he never checked to insure that it did not concern his ability to received and store classified material in his home office. He was negligent in not inquiring into his authority to receive and work with classified material at his home office which did not have a facility security clearance.

Only Applicant benefitted from the ability to have classified material sent to his home office. If he could work at home, he did not have to travel to another state to perform work as required by the consulting agreement. The government supported agency and his contractor employer did not gain from this arrangement. Applicant's dominant, hard charging, assertive personality cannot be discounted in determining if he had a major influence on the government employees' decision to provide him a safe and send classified material. Applicant has not provided sufficient information to discount that he was not the driving and major force in having the classified materials sent to his home office. In addition, Applicant did not inform his contractor employer that he was receiving and working with classified material at home and not at their facility or the required government facility. Since Applicant was not working with classified material at the locations required under the consulting agreement, Applicant had a duty to inform his contractor employer of the location where he was working with classified material. It should be note that after receiving the classified material, Applicant followed the rules and regulations for accounting for, managing, and destroying classified material. He kept meticulous records that established he followed all rules and regulations concerning the management of classified material.

Applicant's receipt, storage, and work with classified material outside the places authorized in the consulting agreement and the NISPOM is a serious security concern. Applicant has not met his burden to refute, explain or mitigate the concern. Accordingly, I find against him on SOR allegations 1.a through 1.e. Even though he followed the rules and regulations concerning destruction of classified material, his office assistant did not have a security clearance when he witnessed the destruction of the classified material, I find against Applicant on SOR allegation 1.f.

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. I considered that Applicant served 20 years on active duty, was wounded, and is disabled from service to the United States. I considered that Applicant is the subject matter expert in the U.S. military in his area of expertise and is sought after for his knowledge and ability in this area.

I also considered that Applicant was negligent in not verifying that he could possess classified material at his home office in direct violation of his consulting agreement and the NISPOM. Applicant followed the rules and regulations for managing classified material after he received it at an unauthorized location. This is akin to locking the barn door after the horse has bolted. Applicant has not met his burden to show that his failure to properly handle protected information does not reflect adversely on his reliability, honesty, trustworthiness, and good judgment. The serious security concerns raised by his conduct and lack of good judgment are not mitigated. Overall, the record evidence leaves me with questions and doubts as to Applicant's judgment, reliability, and trustworthiness. Access to classified information is denied.

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:	AGAINST APPLICANT
Subparagraphs 1.a - 1.f:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

THOMAS M. CREAN
Administrative Judge