DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 09-05899
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Caroline Jefferies, Esquire, Department Counsel
For Applicant: *Pro se*

March 30, 2011

Decision

WESLEY, Roger C., Administrative Judge:

Based upon a review of the pleadings, exhibits, and testimony, I conclude that Applicant failed to mitigate the security concerns regarding his use of information technology systems and his personal conduct. Eligibility for access to classified information is denied.

Statement of Case

On July 21, 2010, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing reasons why DOHA could not make the preliminary affirmative determination of eligibility for granting a security clearance, and DOHA recommended referral to an administrative judge to determine whether a security clearance should be granted, continued, denied, or revoked. 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 (AGs) implemented by the Department of Defense on September 1, 2006.

Applicant responded to the SOR on August 16, 2010, and requested a hearing. The case was assigned to me on October 18, 2010. It was scheduled for hearing on November 18, 2010. A hearing was held on the scheduled date for the purpose of considering whether it would be clearly consistent with the national interest to grant, continue, or deny Applicant's application for a security clearance. At hearing, the Government's case consisted of four exhibits; Applicant relied on three witnesses (including himself) and eight exhibits (AE A-H). The transcript (Tr.) was received on December 6, 2010.

Summary of Pleadings

Under Guideline M, Applicant is alleged to have copied computer files relating to parts that had passed inspection and used them to falsify non-destructive test record results for classified parts in 2009, while employed by a defense contractor, in violation of company rules, procedures, and guidelines. Allegedly, he was terminated by his employer as a result of his actions.

Under Guideline E, the allegations made under Guideline M are incorporated. Applicant is also alleged under this Guideline to have denied falsifying non-destructive test record results when questioned by company personnel in March 2009 about the earlier incident.

In his response to the SOR, Applicant admitted most of the allegations: He admitted the specific allegations covered by subparagraphs 1.a and 2.b. But he denied that his actions reflect current unreliability and trustworthiness, or call into question his willingness or ability to properly protect classified information, sensitive systems, networks, and other protected information.

Findings of Fact

Applicant is a 31-year-old-mechanic for a defense contractor who seeks a security clearance. The allegations covered in the SOR and admitted to by Applicant are incorporated herein and adopted as relevant and material findings. Additional findings follow.

Applicant served in the Air Force (USAF) between 2001 and 2008. (GE 1) He was honorably discharged in September 2008. (GE 1 and AE A) Applicant attended college between January 2003 and August 2005 at an accredited college and earned an associate's diploma from an AF community college in December 2005. (GE 1 He married in October 2002, and has one child from this marriage (age 7)

Following his USAF discharge, Applicant went to work for a defense contractor (Company A) as an engineer technician and obtained the proper certifications. (GE 1; Tr.54-55) As an engineer technician, he was responsible for inspecting aircraft engine housings and testing classified parts and entering the results on a ledger form. (GE 2)

Inspections involved tracking ultra sound waves to create images on a computer screen to ensure no separation in the glue bonding of the main assemblies. (Tr. 56-58)

Upon joining Company A, Applicant was fully briefed on the company's standards, policies, and procedures, and in September 2008, he acknowledged his receipt of his company's current edition of its standards of business ethics and conduct. (GE 4) Still, he proceeded to knowingly and intentionally copy computer files from previously tested parts on 12 to 17 different occasions in January 2009, and he applied the copied results of those tests to the new parts being tested. (GEs 3 and 4; Tr. 55-59, 72) The serial numbers of these tested parts were isolated by the company's investigators and corrective measures were taken to ensure the quality of these parts. (GE 3) When copying the results of these prior tests, Applicant never considered whether anyone else would notice his actions. (Tr. 64) Nor did he give any thought to what flight risks he might be exposing aircraft by his actions. (Tr. 65-69). In reflection, he acknowledged risks of the non-inspected bonds separating internally and weakening the reinforcements of the overall bonded parts. (Tr. 69-71)

A company investigator discovered the incidents covered by subparagraph 1.a when reviewing tested files ready for transfer to a CD disk. (GE 3) He found some of the copied files were clustered with the original files and had the same modified date and time notations. He proceeded to inform the company's facility supervisor and Applicant's supervisors of his findings.

Several days later, the facility security officer (FSO) questioned Applicant about the suspected falsification incident. (GE 3; Tr. 61) When initially questioned, Applicant denied that he had copied records. (GEs 2 and 3) Pending the results of the company's investigation of the incident, Applicant was placed on unpaid suspended leave and sent home. (GE 2) Several days later, he was called back to work for a follow-up interview with a company investigator. (GE 2) Once Applicant admitted to the investigator that he falsified the computer records (GEs 2 and 3; Tr. 61-62), termination procedures were initiated by his company. Shortly after his admission, he was terminated from Company A. (GEs 2 and 3)

Applicant claims he has paid a heavy price for his actions in the falsification incident. (GE 2) He was forced to split-up his family and start over in another state. (GE 2; Tr. 52-53) He considers himself conscientious and is determined to restore his honor and character. For his past indiscretions, Applicant expressed deep remorse and assures that his falsifications will never be repeated. (Tr. 51-52) In his interview with an investigator of the Office of Personnel Management (OPM) in December 2009, he attributed his initial denial of falsifying his company's test results to fears of losing his job. (GE 2)

Since joining his new employer, Applicant has earned considerable praise from his supervisor for his performance as an engine mechanic responsible for documenting analysis of oil samples. (GE 2, AEs B through D, F, and G; Tr. 31-32) Applicant has completed all of his lab analysis assignments and is credited by his supervisor with

providing consistently honest recovery documentation. *See* AEs E and F; Tr. 33-37. A quarterly report covering the period of July through September 2010 documents Applicant's sample and analysis statistics for the quarter. (AE E) Aware of the Government's SOR concerns through Applicant's own acknowledgments, his supervisor remained impressed with Applicant's overall honesty and judgment. (Tr. 38) His supervisor noted, too, that Applicant's current oil analysis work does not require a security clearance. (Tr. 39-40). With a clearance, Applicant will be able to access aircraft to provide inspection work without an escort, and thereby increase his value to the company. (Tr. 40)

Coworkers and former USAF non-commissioned officers (NCOs) who have worked with Applicant and are familiar with the Government's concerns describe him as honest and reliable. *See* AE H; Tr. 46-47 They extol his strong work ethic, the demonstrated quality of his work, and his aptitude for non-destructive testing programs. (AE H; Tr. 46-47)

Policies

The AGs list guidelines to be used by administrative judges in deciding DOHA cases. These guidelines take into account factors that could create a potential conflict of interest for the individual applicant, as well as considerations that could affect the individual's reliability, trustworthiness, and ability to protect classified information. These guidelines include "[c]onditions that could raise a security concern and may be disqualifying" (disqualifying conditions), if any, and any of the "[c]onditions that could mitigate security concerns." They must be considered before deciding whether or not a security clearance should be granted, continued, revoked, or denied. The guidelines do not require administrative judges to place exclusive reliance on the enumerated disqualifying and mitigating conditions in the guidelines in arriving at a decision. Each of the guidelines is to be evaluated in the context of the whole person in accordance with AG ¶ 2(c).

In addition to the relevant AGs, administrative judges must take into account the pertinent considerations for assessing extenuation and mitigation set forth in AG ¶ 2(a) of the revised AGs, which are intended to assist the judges in reaching a fair and impartial commonsense decision based upon a careful consideration of the pertinent guidelines within the context of the whole person. The adjudicative process is designed to examine a sufficient period of an applicant's life to enable predictive judgments to be made about whether the applicant is an acceptable security risk.

When evaluating an applicant's conduct, the relevant guidelines are to be considered together with the following AG ¶ 2(c) factors:

> (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 chances; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Viewing the issues raised and evidence as a whole, the following adjudication policy factors are pertinent herein:

Use of Information Technology Systems

The Concern: 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, manipulation, storage, or protection of information. AG ¶ 39.

Personal Conduct

The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process. AG ¶ 15.

Burden of Proof

A decision to grant or continue an applicant's security clearance may be made only upon a threshold finding that to do so is clearly consistent with the national interest. Because the Directive requires administrative judges to make a common-sense appraisal of the evidence accumulated in the record, the ultimate determination of an applicant's eligibility for a security clearance depends, in large part, on the relevance and materiality of that evidence. As with all adversary proceedings, the judge may draw only those inferences which have a reasonable and logical basis from the evidence of record.

The Government's initial burden is twofold: (1) It must prove any controverted fact[s] alleged in the Statement of Reasons, and (2) it must demonstrate that the facts proven have a material bearing to the applicant's eligibility to obtain or maintain a security clearance. The required showing of material bearing, however, does not require the Government to affirmatively demonstrate that the applicant has actually mishandled

or abused classified information before it can deny or revoke a security clearance. Rather, consideration must take account of cognizable risks that an applicant may deliberately or inadvertently fail to safeguard classified information.

Once the Government meets its initial burden of establishing admitted or controverted facts, the burden of persuasion shifts to the applicant for the purpose of establishing his or her security worthiness through evidence of refutation, extenuation or mitigation of the Government's case.

Analysis

Applicant is a well-regarded mechanic for a defense contractor who in 2009 knowingly and wilfully copied a former employer's computer files relating to parts that had passed inspection and then used them to falsify non-destructive test record results for classified parts. Applicant had been thoroughly briefed on his company's standards of business ethics and conduct and was clearly aware that his intended actions violated company rules, procedures, and guidelines.

Applicant's computer-based transgressions raise considerable security concerns under both the use of information technology systems and personal conduct guidelines. DC ¶ 40(a), "illegal or unauthorized entry into any information technology system or component thereof," DC ¶ 40(c), "use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system," and DC ¶ 40(e), "unauthorized use of a government or other information technology system," all apply to Applicant's multiple incidents (12 to 17) of falsification of non-destructive test record results for classified parts. DC ¶ 16(a) of Guideline E, "a pattern of dishonesty," and DC ¶ 16(e), "personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing . . ." are applicable to Applicant's situation as well.

While much of Applicant's conduct is covered by Guideline M and can be resolved under that Guideline, there are allegations under each guideline that are not incorporated in the other. For example, subparagraph 2.b addresses Applicant's deliberate denial of falsifying his non-destructive record results when initially questioned by his employers's investigator. Applicant's involuntary separation from his previous employer following his admitted falsifications are incorporated in the Guideline E allegations; although, the reasons for his separation are integrally related to his falsifying his employer's non-destructive test record results. So, too, his reluctance to inform his employer's security staff of his falsifying test record results until subsequently confronted is not literally covered by Guideline M; even though, his delayed acknowledgments of falsifying the test results are integrally related to his falsifying of the test results.

Judgment concerns are tied to Applicant's falsifying non-destructive test record results on his employer's computer files repeatedly during a January 2009 period, his ensuing initial falsification denials over job concerns, and his employment termination following his acknowledged falsifications to his former employer. Applicant's actions are expressly covered by Guideline E, and are entitled to independent cognizance under this Guideline according to DOHA's Appeal Board. *See* ISCR Case No. 06-20964, at 6 (April 10, 2008).

Where there is additional probative adverse information covered by Guideline E that is not covered by Guideline M, and which reflects a recurring pattern of questionable judgment or irresponsibility, independent grounds do exist for considering questionable judgment and trustworthiness and exploitation and coercion risk allegations under Guideline M and Guideline E, respectively. In this case, the facts support the application of both Guideline M and Guideline E.

Authority for considering overlapping conduct under both guidelines is contained in the guidance provided in Enclosure 2, ¶ 2(d) of the Directive's August 2006 amendments. By virtue of D.C. ¶ 16(d) of Guideline E, "credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information," is fully applicable to Applicant's situation.

Judgment lapses and failure to adhere to established rules and policies governing the use of employer-serviced information technology systems are core concerns in Guideline M and E cases. DOHA's Appeal Board has consistently affirmed decisions denying clearance eligibility based on probative showings of unauthorized and non-compliant use of information technology systems. *See* ISCR Case No. 07-04193 (App. Bd. July 3, 2008); ISCR Case No. 05-13515 (App. Bd. July 19, 2007). DOHA's jurisprudence supports the employment of both Guideline M and Guideline E to the facts of Applicant's situation.

For sure, Applicant has demonstrated considerable remorse for his actions and has impressed his new employer with his honesty and performance as an engine mechanic responsible for documenting analysis of oil samples. By his statements and actions with his new employer, Applicant exhibits genuine understanding of his mistaken use of judgment at critical junctures in his testing of classified parts. For his efforts, he make take some advantage of MC ¶ 41(e), "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress," of the personal conduct guideline.

Still, less than two years have elapsed since Applicant ceased falsifying test record results with his previous employer, and his actions, as such, can not be characterized as aged and aberrant. Nor can his falsification of test records and ensuing

initial denials to company security personnel be considered minor or inadvertent. The proofs include detailed employer findings and documented Applicant admissions. While Applicant's subsequent admissions and expressions of remorse are commendable, they are not enough to mitigate security concerns. Due to the seriousness of his transgressions, more time is needed before safe predictions about Applicant's judgment, reliability, and trustworthiness can be made.

From a whole person perspective, Applicant has established a good relationship of trust with his current employer. He has been credited by his supervisor, coworkers, and former USAF NCOs with his honesty and reliability. These are qualities that serve him well in fulfilling his fiducial responsibilities in protecting accessed classified information. It is still too soon, however, to credit Applicant with mitigation of the Government's security concerns associated with his falsifying of computer files relating to non-destructive test record results, and his initial denials of his falsifications when confronted by company security personnel.

Taking into account all of the circumstances surrounding Applicant's recurrent falsifying of non-destructive test record results and initial denials when confronted, Applicant does not mitigate the Government's security concerns. Unfavorable conclusions warrant with respect to the underlying conduct covered by subparagraph 1.a of Guideline M and subparagraphs 2.a and 2.b of Guideline E.

Formal Findings

In reviewing the allegations of the SOR and ensuing conclusions reached in the context of the findings of fact, conclusions, conditions, and the factors listed above, I make the following formal findings:

GUIDELINE M: (INFORMATION SYSTEMS):	AGAINST APPLICANT
Subparagraph. 1.a:	Against Applicant
GUIDELINE E: (PERSONAL CONDUCT):	AGAINST APPLICANT
Subparagraph. 2.a:	Against Applicant
Subparagraph. 2.b:	Against Applicant

Conclusions

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue Applicant's security clearance. Clearance is denied.

Roger C. Wesley
Administrative Judge