DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND
APPECOMPANY AS

In the matter of:)
)
) ISCR Case No. 09-07219
)
Applicant for Security Clearance)

Appearances

For Government: Alison O’Connell, Esq., Department Counsel
For Applicant: *Pro se*

06/27/2012

Decision

Rivera, Juan J., Administrative Judge:

Applicant knowingly accessed classified information without having the required documentation. He improperly used his personal computer to process controlled unclassified information. He improperly marked an unclassified proposal as Secret to improve the possibility that his employer would receive a government contract. He was honest with Defense Security Service (DSS) investigators and credible at this hearing. Personal conduct concerns are mitigated; however, handling protected information concerns are not mitigated. Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on December 21, 2008. On December 8, 2011, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) listing security concerns under Guidelines K (handling protected information) and E (personal conduct).[1] Applicant

[1] DOHA acted under Executive Order 10865, Safeguarding Classified Information Within Industry (February 20, 1960), as amended; Department of Defense (DOD) Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program (Directive) (January 2, 1992), as amended; and the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (AG), implemented by the DOD on September 1, 2006.

answered the SOR on January 5, 2012, and requested a hearing before an administrative judge.

On February 21, 2012, Applicant's case was assigned to another administrative judge. On March 8, 2012, DOHA transferred Applicant's case to me. On May 3, 2012, DOHA issued a hearing notice, setting the hearing for May 22, 2012. Applicant's hearing was held on May 22-23, 2012. At the hearing, the Government offered exhibits (GE) 1 through 18. Applicant testified and submitted exhibits, which are cited by Applicant's tabbing methodology. (Transcript (Tr.) 40-46; 84-87; GE 1-18) There were no objections, and I admitted GE 1-18 and Applicant's proffered exhibits. (Tr. 51-52, 87) GE 19 for identification is the list of Government exhibits. (Tr. 52) I received the hearing transcript on May 31, 2012.

Procedural Issues

Before the hearing, Department Counsel made a motion to permit a material, factual witness to testify using a speaker telephone. (Tr. 18-19) Applicant objected, and I sustained Applicant's objection. (Tr. 19; Appellate Exhibit 1) The witness testified in person. (Tr. 54-140)

At the hearing, Department Counsel moved to amend the SOR by adding ¶ 1.g to allege that in January 2009, Applicant violated security protocols when he used his personally-owned computer to process controlled unclassified information. (Tr. 373) Applicant did not object, and I granted Department Counsel's motion. (Tr. 373-374)

Findings of Fact

Applicant's SOR response admitted, with explanations, the allegation in SOR ¶ 1.a - that he accessed classified material in a request for proposals (RFP) without proper authorization. At the hearing, he admitted SOR ¶ 1.g - that he violated security protocols when he used his personally-owned computer to process controlled unclassified information. He denied the remaining SOR allegations with explanations. His admissions are incorporated as findings of fact. After a thorough review of all the evidence, and having observed Applicant's demeanor and considered his testimony, I make the following findings of fact.

Applicant is a 73-year-old consultant working for several defense contractors. (Tr. 7; GE 1) He served on active duty in the Army from 1958 to 1961. He earned a bachelor's degree in classical languages in 1974, and a master's degree in operations research and systems analysis in 1977. He has held a security clearance for over 35 years. He worked in the federal civil service from 1961 to 1999, and he retired as a Senior Executive Service (SES) 5. He was an SES from 1981 to 1999. After his retirement, he worked for various defense contractors until the present. (Tr. 10-12) He has many years of experience in material development, government contracting practices, and the security clearance processes. (Tr. 198) He has written proposals for government contracts, and he is thoroughly familiar with security and procurement rules and procedures. (Tr. 282) Aside from the SOR allegations, there has never been an allegation that Applicant violated security rules. (Tr. 13) He is currently a senior vice president at L, a company with government contracts. (Tr. 199)

Around 2008, a Department of Defense (DoD) entity was developing a military vehicle. The DoD entity sent out requests for proposals (AE RFP 10) that contained a classified annex. Company A hired Applicant to generate a proposals in response to the entity's RFP shortly before Company A's proposals was due.

Applicant's consultant agreement with Company L was issued in January 2009. (Tr. 156, 158) At the time, L had a facility site clearance,[2] but it did not have an information assurance program. Applicant erroneously believed that Company L also had safeguarding authority (authority to store classified information). (Tr. 182, 311, 317) In June 2008, Company L lost its authority to store classified information, and it was not reinstated by January 2009. (Tr. 142-145, 147) Applicant arrived at Company A's place of business on January 2, 2009. (Tr. 208-209) He knew that Company A had applied for a facility clearance; however, it would not be approved before the proposal was due. (Tr. 209)

In compliance with the DoD 5220.22-M, National Industrial Security Program Manual (NISPOM), February 28, 2006, the RFP entity refused to permit contractors or companies to access the classified annex of the RFP without a DD Form 254 (DoD Contract Security Classification Specification). The security manager for the entity issuing the RFP with a classified annex generated DD Form 254s for classified contracts. (Tr. 55-56, 61)

A company interested in making an offer on the contract could request the classified RFP annex. The security manager reviewed their request for a DD Form 254 to ensure the company had a facility security clearance, classified storage capability in their facility (if they were going to have classified information in their facility), and if an individual working for the company had a clearance. (Tr. 56-57, 59-60, 101) Without a DD Form 254, a company or individuals working for the company were not authorized to review a particular contract file, including any classified annex of the contract, information for bids (IFB), and RFPs. (Tr. 58, 60-61, 126) Applicant knew that a DD Form 254 was required for him to work on a classified contract. (Tr. 282) Applicant, Company L, and Company A did not have a DD Form 254 to respond to the entity's RFP. (Tr. 62, 88-90, 96-100, 162, 184)

On January 5, 2009, Applicant went to Company FP, which had the classified annex to review it. (Tr. 214) He specifically asked FP's facility security officer to verify his security clearance (Tr. 288-289), and to observe him while he took some notes, containing the paragraph numbers and paragraph headings of the classified annex. (Tr.

[2] The DSS report states that Company L lost their facility storage clearance in 2008, because they lacked the need for it. L could have had their clearance to store Secret documents restored by establishing a need to safeguard or store classified information. (Tr. 184-186; GE 15) The DSS report notes that L had Top Secret facility authorization. (GE 15 at 2)

214, 371) Applicant denied that he copied any classified information. (Tr. 371) He provided a copy of his notes as an exhibit. (Tr. 215; AE 1.a.2-4, 1.b.3) He wanted Company A's proposal to have the same organization or format as the classified annex because he believed the proposal would be summarily rejected if it lacked the sequencing of the classified annex. (Tr. 298-299)

Applicant admitted that he took a shortcut and reviewed the classified annex at Company FP, in violation of the rule that he needed a DD Form 254 to document his authority for access. (Tr. 218) He said that he was not thinking about circumventing or "disregard[ing] a basic rule" when he accessed classified information at FP without first obtaining a DD Form 254. (Tr. 283, 301) He promised that he would never violate such a rule again. (Tr. 302)

Applicant denied the allegation that he took classified documentation from FP's facility. (Tr. 217, 223-224; SOR ¶ 1.b; GE 15) He inserted in the proposal certain unclassified test procedures and results, but no classified information.[3] In the executive summary of his proposal, he indicated the test results in the proposal would probably need to be updated. (Tr. 215, 219-220, 306) He emphasized that the only information from the classified annex included in the proposal were the paragraph headings, which were not classified. (Tr. 217, 227)

Initially, Applicant planned to submit an unclassified proposal. (Tr. 311, 317-318; GE 4 at 4) Later, Applicant determined that the proposal needed to go through classified channels because the RFP required this processing. (Tr. 311-314) The RFP indicated, "Offers must have a copy of the classified annex in order to meaningfully respond to the solicitation." (Tr. 207; AE RFP 10 at 10, ¶ L.1.4.1)

Applicant told the security manager that he double wrapped and marked the proposal as Secret; however, he told her that the material was not actually classified. (Tr. 114; AE 2.c.8) Incorrectly marking documents as classified violates classification rules. (Tr. 114) The SOR did not allege that Applicant improperly marked his proposals as Secret. Applicant insisted that he did not mark the internal pages with a classification. (Tr. 249) He said he did not think the document was actually classified unless each page is marked individually, and it reaches a classification authority. (Tr. 248-249, 365-366) He said that one could infer that a package with a classified cover sheet contained classified information. (Tr. 365-366) As the person who generated the document, he had derivative classification authority, and his marking of the document Secret renders it presumptively Secret.[4] (Tr. 249) He said that he marked some of the individual pages as unclassified. (Tr. 250)

[3] In general, if the contractor develops the test procedures and results, and there is no end application specified on the vehicle, then the data would not be classified. (Tr. 308) The contract security classification guide "is the bible" under these circumstances for determining when or if a document is classified. (Tr. 309)

[4] NISPOM, paragraph 4-102(b) Derivative Classification Responsibilities states:

Applicant copied his proposal on several CDs. He placed a CD marked Secret into the computer system at Company L. (Tr. 342) He used the printers at L to make two copies of the proposal for the RFP entity, and left one copy of the proposal at Company L. (Tr. 343) The copy of the proposal left at Company L was marked Secret. (Tr. 344-346) Applicant insisted that nothing in the proposal was actually Secret. (Tr. 344) The documents were marked Secret to meet the expectations of the RFP entity, to comply with the RFP instructions, and because Applicant believed an unclassified proposal submission would not be processed to the evaluation committee.[5] (Tr. 228, 346) Applicant kept another copy of the proposal on a mass storage device or flash drive. (Tr. 346-347)

Applicant prepared the proposal on his personal computer, and it contained controlled unclassified information (CUI). (Tr. 326-332, 341-342) He acknowledged that he violated a security rule when he used his personal computer to prepare the proposal. (Tr. 333, 350, 392) He said he used a flash drive and not the computer hard drive to store the information. (Tr. 374)

> b. Employees who copy or extract classified information from another document, or who reproduce or translate an entire document, shall be responsible:
>
> (1) For marking the new document or copy with the same classification markings as applied to the information or document from which the new document or copy was prepared and (2) For challenging the classification if there is reason to believe the information is classified unnecessarily or improperly.
>
> NISPOM, paragraph 4-104. Challenges to Classification, provides:
>
> Should a contractor believe (a) that information is classified improperly or unnecessarily; or (b) that current security considerations justify downgrading to a lower classification or upgrading to a higher classification; or (c) that the security classification guidance is improper or inadequate, the contractor shall discuss such issues with the pertinent GCA for remedy. If a solution is not forthcoming, and the contractor believes that corrective action is still required, a formal written challenge shall be made to the GCA. Such challenges shall include a description sufficient to identify the issue, the reasons why the contractor believes that corrective action is required, and any recommendations for appropriate corrective action. In any case, the information in question shall be safeguarded as required by this Manual for its assigned or proposed level of classification, whichever is higher, until action is completed.

[5] The SOR did not allege that Applicant intentionally marked documents Secret that he knew were unclassified. In ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006) the Appeal Board listed five circumstances in which conduct not alleged in an SOR may be considered stating:

> (a) to assess an applicant's credibility; (b) to evaluate an applicant's evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether an applicant has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for whole person analysis under Directive Section 6.3.

(citing ISCR Case No. 02-07218 at 3 (App. Bd. Mar. 15, 2004); ISCR Case No. 00-0633 at 3 (App. Bd. Oct. 24, 2003)). I have considered the non-SOR misconduct about improperly marking documents as Secret for the five above purposes, and not for any other purpose.

The security manager believes that in early January 2009, she received two proposals classified at the Secret level prepared by Applicant on behalf of Companies A and L in response to the RFP. (Tr. 64-68, 105-110, 120, 123; AE 1.d.5) Actually, Applicant submitted two proposals on behalf of Company A. (Tr. 258) The second proposal was submitted because Company A wanted to amend the executive summary of their first proposal. (Tr. 258) The first one was mailed, and Applicant hand delivered the second one. (Tr. 258-259, 337-339, 355) Applicant double wrapped the packages, and on the inside it was marked Secret. (Tr. 318, 355) Applicant testified the contents were not actually classified and the markings were form over substance in order for the proposal to receive a more positive consideration from the source selection group. (Tr. 318) Applicant insisted that none of the internal paragraphs or pages were marked as classified. (Tr. 339)

The RFP entity reviewed Applicant's proposal, and sent numerous items for discussion (IFD), using email, discussing his proposal. (Tr. 352-353) The RFP entity did not express any concern about his failure to indicate any part of the proposal was classified. (Tr. 261-266; GE 11 at 32)

The security manager knew that she had not issued a DD Form 254 to Companies A and L, and Applicant. (Tr. 64-68) She wondered whether they had facility security clearances. (Tr. 124) She asked Applicant for the DD Form 254s from Companies A and L because she did not have one on file to document the release of the classified annex. (Tr. 65) Companies A and L did not have DD Form 254s. (Tr. 371) According to the security manager, the submitters are responsible for classifying their submissions. (Tr. 65) She recalled that some paragraphs of their submissions were marked Secret. (Tr. 66, 103-104) However, she was unable to opine whether or not the proposals received from Companies A and L were actually classified. (Tr. 68) The base document that her company sent out seeking RFPs was unclassified. (Tr. 66)

Upon receipt of the proposals from Company A, the security manager contacted Applicant and asked him where he prepared the documents and his authority for preparing them. (Tr. 70) He responded that he had a letter from Company A authorizing him to prepare the proposals. (Tr. 71-72) The security manager knew that Applicant was a consultant for both Companies L and A, and that he prepared both proposals. (Tr. 76) Applicant told the security manager that he took classified information out of L's facility on a CD, in a notebook, and in a laptop computer. (Tr. 73, 134) He prepared the proposal in a closed area in Company L. (Tr. 74) He did not advise her that the packages did not contain classified information. (Tr. 125)

Company L did not have an accredited information system (AIS) approval to process classified information. (Tr. 74, 144-145) It would be a security violation to open a classified CD or download a classified document onto Company L's server or onto one of Company L's computer hard drives. (Tr. 146) The security manager knew that Company L had a facility clearance, but no authorized storage for classified documents. (Tr. 71) Company A did not have a facility clearance. (Tr. 71) She asked Applicant whether he viewed the classified annex to the contract, and he said that he received the information from another individual, who viewed the annex and provided the information to Applicant. (Tr. 75, 110-111, 134-135; AE 2.c.8) She contacted military intelligence and DSS about her concerns. (Tr. 72-73)

A DSS investigator (M) went to Company L to find out about a possible "spill" of classified information. (Tr. 151-152) The investigator removed two binders, two CDs, and a laptop from Company L's safe. A Company L employee told the investigator that Applicant had provided these materials. (Tr. 153, 184) One CD was marked Secret, and the other CD had the classification crossed out. (Tr. 153, 155) The investigator did not review the contents of the CDs. (Tr. 173) The top and bottom of the cover sheet on each binder were marked Secret. (Tr. 155, 175, 180) M did not see paragraph markings of classification. (Tr. 175) Inside the binders, M recalled that a small portion of the pages were marked Secret. (Tr. 155, 173) A Company L employee said that he was told the documents were not classified, and M asked the Company L employee why they were marked Secret. The Company L's employee noted that "the threat information had to be married up in there." (Tr. 187, 193-194) The documents marked Secret are presumed to be Secret, and there was no classification review to determine whether they were properly classified. (Tr. 174, 188-190) M did not compare the documents from Company L's safe with the RFP's classified annex or compare it to the RFP entity's classification guide. (Tr. 191) M removed the two binders and the CDs from Company L's facility, and she retained the binders and CDs in her office until they were destroyed. (Tr. 154, 163)

Applicant said he marked one CD as Secret because he wanted it to conform to the requirements of the RFP. (Tr. 341) He denied that any of the information on the CDs, laptop computer, or in the notebook was classified. (Tr. 246-247)

Another DSS investigator (S) stated that Applicant told him he had a DD Form 254 authorizing him access to the RFP entity's classified annex. S knew that Applicant did not have a DD Form 254. (Tr. 234-236; GE 15 at 3; SOR ¶ 2.a) Applicant credibly testified that he never told S that he had a DD Form 254. (Tr. 267)

Applicant told S that he accessed the RFP's classified annex at Company FP, and he copied some information from it; however, Applicant denied that he removed classified information from FP. (GE 15 at 3) SOR ¶ 2.b alleges that Applicant lied to a DSS investigator by stating he had not removed classified material from the RFP's classified annex located in FP's facility. (GE 15 at 3) Applicant described S's claims as "patently absurd." (Tr. 234-245, 268-269) Considering the evidence as a whole I find that Applicant did not remove classified material from FP. Therefore, he did not make false statements to S.

SOR ¶ 2.c alleges that Applicant lied to S by stating that he prepared the proposal in a sensitive compartmented information facility (SCIF) on an accredited information system (AIS) at Company L. Applicant said that he prepared the proposal at Company L (Tr. 154), and he denied that he told S that he prepared the proposal in a SCIF on an AIS. Applicant knew that S could easily determine whether Company L had a SCIF and an AIS. There is no reason that Applicant would lie about these issues as he maintained he had not brought classified information or prepared a classified proposal at Company L.

SOR ¶ 2.e notes the applicability of FAR Clause - 52.204-2, also known as the security requirements clause. This FAR clause reinforces the NISPOM by incorporating those requirements into government contracts. SOR ¶ 2.e indicates that Applicant's conduct as alleged in SOR ¶¶ 1.a through 1.f also violates Federal Acquisition Regulation (FAR) clause 52.204-2.[6]

The security manager believed that Applicant told her that he prepared Company L's proposal in a SCIF, and that Company L had an accredited AIS. (Tr. 269-270; SOR ¶ 2.c) Applicant testified he would never use language about an "accredited AIS," and he denied that he made these statements to her. (Tr. 269, 273) He may have agreed with R that Company L or Company A had a cage code. (Tr. 270-271) A cage code is used to identify a company's security information. (Tr. 363) He told the security manager that Company L had a Top Secret clearance, and he mistakenly told the

[6] FAR Clause 52.204-2 provides:

> FAR CLAUSE - 52.204-2 Security Requirements "CLAUSE"
>
> The Industrial Security Program prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of information released by the US Government Executive Branch Departments and Agencies to their contractors. The proscribed Federal guidance is the National Industrial Security Program Manual (NISPOM).
>
> The Federal Acquisition Regulation (FAR) defines a "Classified Contract" as "Any contract that requires, or will require, access to classified information (Confidential, Secret, or Top Secret) by the contractor or its employees in the performance of the contract. A contract may be a classified contract even though the contract document itself is not classified."
>
> Company Al "Classified Contracts" must have, at a minimum, the Clause 52.204-2, Security Requirements, incorporated into the contract. This clause binds the contractor to meet the security requirements identified in the [NISPOM].
>
> The FAR states we "shall" use a DD Form 254 (Contract Security Classification Specifications) for classified contracts. This form must be part of the contract package and is used to identify other security requirements that HQDA would impose on a contractor. The DD Form 254 informs the contractor of the level of information they will be required to access, the level of security clearance the contractors will need, and how they will process, store, transmit, and destroy the classified information when the contract is complete.
>
> If the contractor then subcontracts the work, they are obligated, under the [NISPOM], to pass those requirements on to the subcontract.
>
> Contracts requiring work that is unclassified but sensitive should also be evaluated to ensure that contractors have undergone an appropriate level of background investigation to perform the required duties, and contractors must be made aware of any procedures or requirements regarding proper protection of unclassified but sensitive information.

security manager that Company L had the capability of safeguarding classified information. (Tr. 271, 363-364) A SCIF was not a material requirement for the solicitation. (Tr. 273)

Policies

Eligibility for access to classified information may be granted "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. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." Department of the Navy v. Egan, 484 U.S. 518, 528 (1988).

The AG list disqualifying and mitigating conditions for evaluating a person's suitability for access to classified information. Any one disqualifying or mitigating condition is not, by itself, conclusive. However, the AG should be followed where a case can be measured against them, as they represent policy guidance governing access to classified information. Each decision must reflect a fair, impartial, and commonsense consideration of the whole person and the factors listed in AG ¶ 2(a). All available, reliable information about the person, past and present, favorable and unfavorable must be considered.

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an applicant's security clearance. The Government must prove, by substantial evidence, controverted facts alleged in the SOR. If it does, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. The applicant bears the heavy burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance.

Persons with access to classified information enter into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability, and trustworthiness of those who must protect national interest as their own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government. "[S]ecurity clearance determinations should err, if they must, on the side of denials." Egan, 484 U.S. at 531; AG ¶ 2(b). Clearance decisions are not a determination of the loyalty of the applicant concerned. They are merely an indication that the applicant has or has not met the strict guidelines the Government has established for issuing a clearance.

Analysis

Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information:

> 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 ¶ 34 describes nine conditions that could raise a security concern and may be disqualifying in this case:

> (a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;
>
> (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;
>
> (d) inappropriate efforts to obtain or view classified or other protected information outside one’s need to know;
>
> (e) copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings;
>
> (f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information;
>
> (h) negligence or lax security habits that persist despite counseling by management; and
>
> (i) failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

AG ¶¶ 34(b), (c), (d), (f), and (g) apply. Applicant and Companies A and L lacked the required DD Form 254, and therefore he and both Companies were not permitted access to the classified annex to the entity's RFP. Applicant went to Company FP and accessed their copy of the classified annex of the RFP in violation of the NISPOM. He also used his personally owned computer to process CUI to generate Company A's proposal, which violated security rules.

AG ¶¶ 34(a), (e), 34(h) and, 34(i) do not apply. Applicant did not copy or disclose any classified information, there is no evidence that he received counseling about security rules prior to his security violations, and national security was not damaged.

AG ¶ 35 provides three conditions that could mitigate security concerns in this case:

> (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.

None of the mitigating conditions fully apply. Applicant is very knowledgeable about security rules, and remedial training is unnecessary. He knew what he did violated security rules and procedures, and he did it anyway. The Appeal Board has explained why security violations are difficult to mitigate:

> Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. Once it is established that Applicant has committed a security violation, he has "a very heavy burden of demonstrating that [he] should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an Administrative Judge must give any claims of reform and rehabilitation strict scrutiny." In many security clearance cases, applicants are denied a clearance for having an indicator of a risk that they might commit a security violation (e.g., alcohol abuse, delinquent debts or drug use). Here the issue is not merely an indicator, rather the Judge found Applicant disregarded in-place security procedures in violation of the NISPOM.

(Citations omitted). ISCR Case No. 04-04264 at 3-4 (App. Bd. Sep. 8, 2006). Applicant's security violations occurred in January 2009. He assures that he will strictly comply with security rules in the future. His assurances are sincere. Nevertheless, more time must elapse to eliminate doubt concerning his current reliability, trustworthiness, or good judgment.

Personal Conduct

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

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

Three personal conduct disqualifying conditions under AG ¶ 16 are potentially applicable:

> (b) deliberately providing false or misleading information concerning relevant facts to an . . . investigator . . . ;[7]
>
> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information; and
>
> (e) personal conduct, or concealment of information about one’s conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing. . . .

[7] The Appeal Board has cogently explained the process for analyzing falsification cases, stating:

> (a) when a falsification allegation is controverted, Department Counsel has the burden of proving falsification; (b) proof of an omission, standing alone, does not establish or prove an applicant’s intent or state of mind when the omission occurred; and (c) a Judge must consider the record evidence as a whole to determine whether there is direct or circumstantial evidence concerning the applicant’s intent or state of mind at the time the omission occurred. [Moreover], it was legally permissible for the Judge to conclude Department Counsel had established a prima facie case under Guideline E and the burden of persuasion had shifted to the applicant to present evidence to explain the omission.

ISCR Case No. 03-10380 at 5 (App. Bd. Jan. 6, 2006) (citing ISCR Case No. 02-23133 (App. Bd. June 9, 2004)).

AG ¶ 16(b) does not apply. Applicant credibly refuted the DSS investigator's statement indicating that Applicant told him he had a DD Form 254 (SOR ¶ 2.a), and that he prepared Company A's proposal in a SCIF on an accredited system at Company L (SOR ¶ 2.c). Applicant had previously talked to the security manager about these same issues, and Applicant was well aware that the Government knew he did not have a DD Form 254, and that Company L did not have a SCIF. This information was readily available to DSS. Applicant is too intelligent and detail oriented to make such statements to the DSS investigator. Applicant was honestly mistaken when he said that Company L continued to have classified safeguarding authority. The allegation that Applicant removed classified material from the RFP's classified annex located in Company FP's facility is not supported by substantial evidence. (SOR ¶ 2.b)

AG ¶ 16(c) does not apply because there is sufficient credible adverse information under the handling protected information guideline for an adverse determination.

AG ¶ 16(e) applies. Applicant violated security rules when he accessed the classified annex to the entity's RFP at Company FP without a DD Form 254, and when he used his personally owned computer to process CUI to generate Company A's proposal. Violation of security policies and rules adversely affected Applicant's personal, professional, and community standing. Because the Government established disqualifying conditions, further analysis concerning the possible applicability of mitigating conditions is required.

Four mitigating conditions under AG ¶ 17 are potentially applicable:

> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (f) the information was unsubstantiated or from a source of questionable reliability.

AG ¶ 17(f) applies. The allegations that Applicant lied to DSS investigators are unsubstantiated. (SOR ¶¶ 2.a to 2.c) As previously stated, Applicant credibly refuted the investigator's statement. Because of his conversations with the security manager, Applicant was well aware that the Government knew he did not have a DD Form 254, and Company L did not have a SCIF. Applicant is too intelligent and detail oriented to make such statements to the DSS investigator. Applicant was honestly mistaken when he said that Company L continued to have classified safeguarding authority.

AG ¶ 17(e) applies to AG ¶ 16(e). Even though his violation of security policies adversely affected his personal, professional, and community standing, his disclosure eliminated any vulnerability to exploitation, manipulation, or duress. Applicant is fully committed to complying with security requirements. He could not be coerced into compromising national security by threats to disclose his security violations.

Any remaining personal conduct concerns under Guideline E are mitigated because the security violations are duplicated under both Guidelines E and K. The scope of his security-related conduct is thoroughly addressed under Guideline K and the Whole-Person Concept.

Whole-Person Concept

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case and under the whole-person concept. (AG ¶ 2(c)) I have incorporated my comments under Guidelines K and E in my whole-person analysis. Some of the factors in AG ¶ 2(a) warrant additional comment.

There are some facts supporting mitigation of security concerns under the whole-person concept; however, they are insufficient to fully mitigate the security concerns. Applicant is a 73-year-old consultant working with defense contractors. He served four years on active duty in the Army. He earned a master's degree in operations research and systems analysis. He worked in the federal civil service from 1961 to 1999. He was an SES from 1981 to 1999, and he subsequently worked for various defense contractors for several years. He has held a security clearance for over 35 years.

Applicant has many years of experience in material development. He is thoroughly familiar with security and procurement rules and procedures. Aside from the SOR allegations, there is no evidence to show that he has violated security rules and procedures. During his 35 years of government service, he was entrusted with important responsibilities and he made major contributions to national security. I am confident that he has the ability and maturity to comply with security requirements. He is an intelligent person, who understands the importance of compliance with security rules. There is no evidence of disloyalty. His admission that he intentionally violated security rules is an important step towards rehabilitation and mitigation of security concerns.

The evidence against approval of Applicant's clearance is more substantial at this time. Applicant knowingly violated three security rules: (1) He knew that the RFP entity refused to permit contractors or companies to access the classified annex of the RFP without a DD Form 254. He and his employer lacked the required DD Form 254. He went to Company FP to circumvent this security requirement, and he accessed FP's copy of the classified annex of the RFP; (2) He used his personally owned computer to process CUI to generate Company A's proposal; and (3) He marked Company A's proposal as Secret even though the contents were not classified in order to increase the probability that Company A's proposal would receive serious examination by the RFP entity. His security violations show lack of judgment and raise unresolved questions about Applicant's reliability, trustworthiness and ability to protect classified information.

Applicant's personal conduct security concerns are mitigated; however, he failed to mitigate handling protected information security concerns. For the reasons stated, I conclude he is not eligible for access to classified information.

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
Subparagraph 1.a:	Against Applicant
Subparagraphs 1.b to 1.f:	For Applicant
Subparagraph 1.g:	Against Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a to 2.e:	For Applicant

Conclusion

In light of Company Al of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant eligibility for a security clearance to Applicant. Clearance is denied.

JUAN J. RIVERA
Administrative Judge