DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 14-05067
	)	
Applicant for Security Clearance	)	

Appearances

For Government: David F. Hayes, Esq., Department Counsel
For Applicant: Donna Price, Esq.

12/31/2015

_____

Decision

_____

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guideline K (Handling Protected Information). Eligibility for access to classified information is granted.

Statement of the Case

Applicant submitted a security clearance application (SCA) on June 24, 2013. On February 21, 2015, the Department of Defense (DOD) sent him a Statement of Reasons (SOR) alleging security concerns under Guideline K. The DOD acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) implemented by the DOD on September 1, 2006.

Applicant answered the SOR on April 1, 2015, and requested a hearing before an administrative judge. Department Counsel was ready to proceed on July 31, 2015, and the case was assigned an administrative judge on August 31, 2015. It was reassigned to me on September 2, 2015, due to workload. On October 7, 2015, the Defense Office of Hearings and Appeals (DOHA) notified Applicant that the hearing was

scheduled for October 28, 2015. I convened the hearing as scheduled. Government Exhibits (GX) 1 and 2 were admitted in evidence without objection. Applicant testified, presented the testimony of three witnesses, and submitted Applicant's Exhibits (AX) A through D, which were admitted without objection. DOHA received the transcript (Tr.) on November 5, 2015.

Correction of Transcript

On December 6, 2015, Applicant's counsel requested three corrections of the transcript. With the concurrence of Department Counsel, I made the requested corrections. (Order, December 10, 2015, attached to the record as Hearing Exhibit I.) The corrections are handwritten in red ink on pages 44, 126, and 152 of the transcript.

Administrative Notice

At Applicant's request, and without objection by Department Counsel, I took administrative notice of the system for identifying and protecting classified and sensitive material established by the North Atlantic Treaty Organization (NATO) Communications and Information Agency (NCIA).[1] The facts administratively noticed are set out below in my findings of fact.

Findings of Fact

In his answer to the SOR, Applicant admitted all the allegations. His admissions in his answer and at the hearing are incorporated in my findings of fact.

Applicant is a 51-year-old U.S. citizen employed by NATO as a principal scientist since June 2002.[2] He graduated from college in June 1986 with a bachelor's degree in aerospace engineering. (GX 1 at 11; Tr. 110.) He married in November 1986. He and his wife have no children. He received a DOD security clearance in 1986, while employed by a defense contractor, and his DOD clearance was revalidated in 2003 after he was employed by NATO in 2002.

NATO employees usually are hired for three years, and their contracts can be renewed in three-year increments. After nine years, a valuable employee may be offered an indefinite contract. Applicant has an indefinite contract. (Tr. 59-60.)

[1] The directives attached to the request to take administrative notice were published after the conduct alleged in the SOR, but the parties agreed that the documents, combined with the testimony of the security manager for the NCIA, accurately reflected the systems in effect at the time of the conduct alleged in the SOR.

[2] The Directive ¶ 3.1 specifically applies to "any U.S. citizen who is a direct-hire employee . . . [of] NATO and who holds or requires NATO certificates of security clearance or security assurances for access to U.S. or foreign classified information . . . ."

NATO has four levels of classified materials: COSMIC top secret (with two sub-categories), NATO secret, NATO confidential, and NATO restricted (NR). The first three classifications are the same as the U.S. classifications and are given equivalent protection. NATO NR material is equivalent to "for official use only" *See* ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). (FOUO). NATO material classified as NR is required to be protected in a manner that will prevent disclosure to non-government personnel. NR information may be stored in filing cabinets, desks, or other containers located in rooms where internal building security is provided during non-duty hours by government or government contractor personnel. Where such internal security is not available, locked buildings or rooms usually provide adequate after-hours protection. (AX D; Tr. 26, 43-44.)

Applicant's workplace uses the same computers for NATO unclassified and NATO NR materials. The computers have a toggle switch to select the unclassified or NR mode. If the user sends a NATO NR email to a civilian address or an unclassified computer, the firewall will block it from being sent and send a warning message to the sender. (Tr. 73.)

Applicant's workplace is protected by several layers of security. He works in a locked area in a building to which access is controlled. NATO NR material is locked in cabinets or desk drawers. Higher-level classified documents are secured in safes. His building is surrounded by a physical barrier under electronic and physical observation. Certain laboratory and working spaces in the building are protected by double-lock systems. (AX C.)

When NATO security teams discover a failure to properly protect classified materials, they leave a bright red card on the offender's desk or in a prominent location, informing the offender of the violation, and they seize the unsecured materials. The offender is instructed to report to the guard desk, explain the incident, and retrieve the materials that were seized. (Tr. 53.)

Each member of the NATO staff has a personal security file, in which all violations are recorded. The file is open for inspection by national investigators who are conducting renewals of security clearances. After three years, an incident is removed from the individual's personal security file and kept in the security office. Thus, a review of the personal security file of any individual will reflect only incidents occurring in the last three years. (Tr. 54-55.)

In October 2002, shortly after Applicant was hired by NATO, he left a NATO NR document unsecured on his desk. The security team left a red tag on his desk and seized the document. He was required to report to the security desk, explain the violation, and retrieve the seized document. He testified that he had "a conversation" with his immediate supervisor about the October 2002 incident. (Tr. 116-17.)

In November 2003, Applicant failed to properly secure a NATO laboratory containing secret material. The laboratory was protected by two locks, a numeric pad,

and a combination lock with a spin dial. A roster was maintained, assigning a member of the laboratory to ensure that the laboratory was secured. Applicant testified that he was scheduled to check the security of the laboratory and spin the dial, but he was not aware that he was scheduled for security duty because of a miscommunication. The NATO security team discovered that the combination lock dial had not been spun. Applicant took responsibility for the failure to check the security of the laboratory because he was the senior person on the team. The incident resulted in Applicant being formally interviewed by his supervisor, because it involved secret material. (Tr. 117-20.) According to the NATO security manager, a formal interview amounts to a "mild counseling session." (Tr. 66.)

Applicant did not disclose the October 2002 and November 2003 incidents in his June 2013 SCA, because they occurred more than seven years before he submitted the SCA. The incidents also were not reflected in his personal security file when he submitted his SCA, because they had occurred more than three years preceding it.[3]

When Applicant submitted his SCA in June 2013, he disclosed four warnings for security violations, which are alleged in SOR ¶¶ 1.b-1.e. The evidence concerning these incidents is summarized below.

In November 2006, Applicant left a NATO NR document in an unlocked drawer in his desk (SOR ¶ 1.e). He received a written notice of violation from NATO security agents who discovered the unlocked cabinet. (GX 2 at 12.) He testified that the office doors are locked during the workday, so that a NATO NR document can be left on the desk. However, after duty hours, the office doors are unlocked so that the security team can check the desk cabinets as well as the NATO secret safes. (Tr. 122.) He received a verbal warning from his supervisor. (GX 1 at 13.)

In March 2008, Applicant left a NATO classified safe open and unattended (SOR ¶ 1.d). The NATO security team discovered the unlocked safe and summoned Applicant to return to his office. A locking bar had been put in place, but the dial on the lock had not been spun. Applicant returned to the office and secured the safe. All classified documents were accounted for and there was no compromise of classified information. (Tr. 123-24.) The NCIA chief verbally reprimanded him. (GX 2 at 5, 11-12.) The security manager testified that the verbal reprimand was "a very formal sit-down." (Tr. 70.)

In April 2010, Applicant emailed what he thought was an unclassified document to his unclassified NATO laptop computer for future reference. An attachment to the

[3] Conduct not alleged in the SOR may not be used as an independent basis for revoking a security clearance, but it may be considered to assess an applicant's credibility; to decide whether a particular adjudicative guideline is applicable; to evaluate evidence of extenuation, mitigation, or changed circumstances; to consider whether an applicant has demonstrated successful rehabilitation; or as part of a whole-person analysis. ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006). I have considered the two unalleged security violations for these limited purposes.

email contained NATO NR information (SOR ¶ 1.c). Applicant received a verbal warning from his supervisor. (GX 1 at 13.)

In September 2011, Applicant left a NATO NR document in an unlocked drawer in his desk (SOR ¶ 1.b). The security team left him a written violation notice, and he received a verbal warning from his supervisor. (GX 1 at 13-14.)

In November 2013, after Applicant submitted his SCA, he received a verbal reprimand for sending NATO NR material to his NATO unclassified laptop computer (SOR ¶ 1.a). This incident occurred when Applicant received a meeting invitation from a NATO colleague that was marked "unclassified." Applicant wanted to refer to this document for a meeting later that day, and he tried to forward the email to his NATO unclassified laptop. He received a message that the NATO firewall had blocked the email because it detected NATO NR material. He looked at the email invitation and realized that there was an unmarked attachment to the email that contained NATO NR material. He reported the incident to the NATO security office. The security procedures were changed after this incident, and they now require employees who wish to forward an attachment to an email that they have not compiled to open the email and check it for classified or restricted information. (Tr. 49.)

Applicant's security manager testified that one of the "big failures" of their computer system is that they do not have a technical tool to allow users to check email attachments with confidence, particularly when large or complex attachments are involved and have not been checked due to time pressures. (Tr. 79.)

Applicant testified that, at the time of the incidents involving classified attachments to unclassified messages, NATO had stopped providing unclassified email accounts, which is why he sent NATO documents to his personal email account. In 2014, NATO began providing NATO NR laptops so that it is no longer necessary to use personal email accounts when working away from the office. (Tr. 126.)

The security manager for Applicant's agency is a retired Royal Air Force police officer who served for more than 34 years in the British Air Force. He has been employed by NATO as a security manager for 22 years. Based on Applicant's security record, his security manager would regard him as a high-qualified employee and not a security risk. (Tr. 59.) The security manager testified that his record of three violations in four years was not a concern, because two incidents involved only NR materials and only one involved secret materials. (Tr. 69.)

At the hearing, Applicant attributed his multiple security lapses to being rushed, "trying to do things too fast, prepare for a trip, [and] prepare at the end of the day to get everything sorted out." (Tr. 135.) He testified that none of his security violations resulted in written reprimands or extra training. (Tr. 143-50.)

In an effort to avoid further security lapses, Applicant has started sorting his work differently, making sure that files on his desk are limited to those he needs for the next

day's work. He has drastically reduced the reproduction of NATO-NR material. When he makes copies of NR material, he uses a yellow highlighter to clearly mark it, and at the end of the work day he examines everything on his desk to make sure that NR material is secured. Finally, he "triple-checks" the office to make sure the NR cabinets are locked and the dial on the classified safe has been spun. When he travels, he no longer carries NR materials, because he can now retrieve them online on his NATO-issued laptop. He testified that he is embarrassed and ashamed about his record of security violations. (Tr. 136-38, 156.)

Applicant's performance appraisals as a NATO employee have consistently rated him as meeting or exceeding performance expectations. He is highly respected as a subject-matter expert who willingly shares his expertise and is not interested in self-promotion. (AX A.)

Applicant and his wife are active in their church. He served as chair of the elder board, the governing body for the church. Applicant's former pastor for four years, who stayed with Applicant and his wife for six weeks while seeking housing in 2005, considers him a "very fine individual," whom he would trust with sensitive information. (Tr. 87-94.)

Applicant and his wife dated in high school, broke up, and resumed their relationship in college. They married shortly after graduating from college and have been married for 29 years. Applicant's wife held a security clearance when she was employed by a defense contractor. She testified that Applicant is extremely honest. He will readily admit a mistake and take responsibility for his actions. Before they were married, he told his now wife that he had fathered a child with another college girlfriend. She testified that he told her about his security violations and that he had been reprimanded for them. (Tr. 96-105.)

Applicant submitted 20 letters attesting to his good character. A few are from friends and family, and several are from NATO employees and former employees from other NATO countries. All are from supporters who have known Applicant and worked with him for many years. The letters all portray him as a talented and dedicated scientist, with a reputation for high integrity, honesty, reliability, and hard work. On a personal level, he is universally regarded as kind, friendly, amiable, compassionate, conscientious, and humble. He is deeply religious, morally responsible, and passionately devoted to his family. (AX B-1 through B-20.)

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly

consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Guideline K, Handling Protected Information

The security concern under this guideline is set out in AG ¶ 33: "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 concern."

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 an applicant has committed a security violation, he or she has a very heavy burden of demonstrating that he or she should be entrusted with classified information. Because security violations strike at the heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny. *See* ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006).The frequency and duration of the security violations are aggravating factors. ISCR Case No. 97-0435 at 5 (App. Bd. July 14, 1998).

Several of Applicant's violations involved NATO NR material, which would not be "classified" under U.S. security rules. Nevertheless, Guideline K extends beyond classified information and includes other sensitive information, such as FOUO, the U.S. equivalent of NATO NR.

The evidence establishes the following disqualifying conditions under this guideline:

> AG ¶ 34(g): any failure to comply with rules for the protection of classified or other sensitive information; and
>
> AG ¶ 34(h): negligence or lax security habits that persist despite counseling by management.

AG ¶ 34(c) ("loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment . . . .") is not established. Applicant's attempts to send NATO NR material to his personal computer were thwarted by the network firewall.

The following mitigating conditions are potentially relevant:

> AG ¶ 35(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; and

> AG ¶ 35(b): the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

AG ¶ 35(a) is established. Applicant's security violations were numerous and did not happen under unusual circumstances. However, his most recent security violation was about two years ago. The issue whether "so much time has elapsed" focuses on whether the conduct was recent. There are no "bright line" rules for determining when conduct is "recent." The determination must be based on a careful evaluation of the totality of the evidence. If the evidence shows "a significant period of time has passed," then an administrative judge must determine whether that period of time is sufficient "to warrant a finding of reform or rehabilitation." *See* ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). Applicant took his most recent violation seriously. He has demonstrated remorse and is determined to prevent recurrence. He has continued to work in a classified environment, but has significantly changed his work habits to prevent further violations. I am satisfied that his attitude and conduct during the past two years warrants a finding that he is rehabilitated.

AG ¶ 35(b) is established. Applicant has not received remedial training. His counseling for the first six violations did not prevent his November 2013 violation. Because his earlier violations were treated informally and somewhat casually, his most recent violation was the first to put him in fear of losing his clearance and his job. His performance during the past due years has demonstrated the "positive attitude" toward security matters required by this mitigating condition.

Applicant's record of security violations appears to have happened in an environment where they were not considered major events. However, security violations are not made less serious by the fact that others in the same office handle classified material in a casual manner. ISCR Case No. 01-24358 (App. Bd. Apr. 13, 2004). Furthermore, the fact that none of Applicant's violations resulted in a compromise of classified material does not render them less serious. ISCR Case No. 97-0435 (App. Bd. Jul. 14, 1998.) Nevertheless, Applicant has taken his violations seriously and taken significant steps to prevent recurrence.

Whole-Person Concept

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. In applying the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. An 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.

I have incorporated my comments under Guideline K in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under that guideline, but some warrant additional comment.

Applicant enjoys an outstanding reputation for integrity and technical skill. He was candid, sincere, and remorseful at the hearing, and he demonstrated the humility and moral courage observed by his colleagues, friends, and family members who presented evidence on his behalf. Before working for NATO, he worked for defense contractors and held a security clearance for 16 years, and he was one of the select few NATO employees who are offered permanent positions after multiple three-year contracts. On the other hand, he has a record of seven security violations, often repeating the same type of violation after previous counseling. However, the most recent violation and the specter of losing his job have gained his attention. Recent improvements in the NATO information technology structure should reduce the likelihood of the problems with email attachments and unclassified computers. His changed work habits have significantly reduced the likelihood of recurrence. I am satisfied that he has carried the very heavy burden of persuasion imposed on Applicants with multiple security violations.

After weighing the disqualifying and mitigating conditions under Guideline K, and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns raised by his multiple security violations. Accordingly, I conclude he has carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a-1.e:	For Applicant

Conclusion

I conclude that it is clearly consistent with the national interest to continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is granted.

LeRoy F. Foreman
Administrative Judge