DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-01077
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Carroll J. Connelley, Esquire, Department Counsel
For Applicant: Alan V. Edmunds, Esquire
Ryan C. Nerney, Esquire

01/17/2018

Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant failed to comply with security requirements involving submitting visitor requests, contact reports, and, in a separate instance, using a personal cell phone in a closed area in November 2014. In May 2015, he violated security regulations relating to foreign travel by not obtaining proper approval for his trip and by not ensuring he was in compliance with information technology and export regulations. He also emailed company-sensitive information without obtaining proper approval. Clearance is denied.

Statement of the Case

On March 27, 2017, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, handling protected information, and explaining why it was unable to find it clearly consistent with the national interest to grant or continue his access to classified information. The DOD CAF took the action under Executive Order (EO) 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 for Determining Eligibility for Access to Classified Information* (AG) effective within the DOD on September 1, 2006.

On April 17, 2017, Applicant answered the SOR allegations and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On June 1, 2017, the case was assigned to me to conduct a hearing to determine whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Counsel for Applicant entered an appearance on June 16, 2017. On June 28, 2017, I scheduled a hearing for August 1, 2017.

While this case was pending a hearing, Security Executive Agent Directive 4 was issued establishing National Security Adjudicative Guidelines (AG) applicable to all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. The AG supersede the adjudicative guidelines implemented in September 2006 and are effective for any adjudication made on or after June 8, 2017.[1] Applicant was informed with the Notice of Hearing that the new AG would be considered in his case.

I convened the hearing as scheduled. Four Government exhibits (GEs 1-4) and ten Applicant exhibits (AEs A-J) were admitted into evidence without objection. Testimony was taken via speakerphone from a Government witness without any objection from Applicant. Applicant and one of his former co-workers testified in person, as reflected in a transcript (Tr.) received on August 8, 2017.

Summary of SOR Allegations

The SOR alleges under Guideline K that Applicant violated his then employer's security requirements under its Special Security Agreement (SSA) in November 2014 by not submitting a timely visit request that included all of the affiliates visiting various company facilities or a timely contact report after the visit (SOR ¶ 1.a). Additionally, Applicant is alleged to have been found culpable by the employer in June 2015 of deliberately disregarding security requirements and demonstrating a pattern of carelessness in approximately May 2015 by: (1) emailing an affiliate detailed information about various company locations without obtaining required approval; and (2) failing to complete security requirements for foreign travel in that he did not complete a visit request; obtain approval for his travel abroad; notify the required official before his trip; contact information technology to ensure that his electronic equipment was updated and protected; or comply with reporting requirements regarding overseas travel (SOR ¶ 1.b). Moreover, Applicant is alleged to have committed a security violation in mid-November 2015 by taking his cell phone into a secured area, using the phone in the secured area against the direction of the facility security officer (FSO), and attempting to re-enter the secured area with his cell phone (SOR ¶ 1.c).

[1] Application of the AGs that were in effect as of the issuance of the SOR would not change my decision in this case.

In a detailed, *pro se* response, Applicant denied the allegation in SOR ¶ 1.a and explained that he was unable to verify his whereabouts or activities of November 2014. Applicant admitted the conduct in SOR ¶ 1.b but denied that it was deliberate. He explained that he had been selected to attend a chief executive officer (CEO) conference at corporate headquarters and had planned a family trip with that business travel. When the conference was cancelled, he obtained approval from his supervisor to continue with his business travel to broaden his knowledge of the company. While abroad, he participated in a weekly financial meeting via conference call and emailed the information discussed to an affiliate so that could print the report. He indicated that he "completely absentmindedly forgot to take the proper steps in compliance with [his then employer's] SSA." He denied any other infraction in over 33 years of holding a security clearance. Applicant denied the incident alleged in SOR ¶ 1.c, which he claimed he was unable to verify because he has left that employment.

Findings of Fact

After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is 57 years old. He and his spouse married in October 1988. They have one daughter, who graduated from college in 2017. Applicant was awarded a bachelor's degree in industrial engineering in May 1982. He has worked in the U.S. defense industry since April 1983, although he has been with his current employer since only February 2017. He works as a senior program manager on a program requiring access to controlled unclassified information and classified information. (GE 1; AEs B-C; Tr. 71-72.) Applicant was first granted a DOD secret clearance in approximately February 1987. His security clearance was upgraded to top secret in October 2005 (GE 1), although he held a secret clearance when the conduct in the SOR occurred. (GE 3.)

Applicant had a successful career with his first defense-contractor employer (company X). Over his 30 years with the company, he held positions of increasing responsibility in manufacturing engineering management, quality management, and product-line program management. He worked in operations from 2002 to 2008. As an operations director, he held a top secret clearance and sensitive compartmented information (SCI) access eligibility. During his last six years at the company, he worked as a program manager on two significant DOD programs. (AE A; Tr. 84.) In September 2013, he left the company during a reduction in force. (GE 1.)

After approximately six months of unemployment, Applicant began working in March 2014 for a U.S.-based unit of a foreign company involved in U.S. defense work. A foreign-owned company with its corporate headquarters in Europe, the company was organized in four sectors, only one sector (sector Y) being authorized to perform classified work for the DOD. Sector Y was authorized to bid for, and allow its employees to work on contracts involving U.S. classified information only in accord with the SSA approved by the DOD in June 2011. Under Sector Y, there were two business units covered by the SSA. Applicant was vice president of one of the business units, which

had five separate sites located in five states over which he had cognizant responsibility. His work required extensive travel. (AE A; Tr. 56-57, 79.)

The SSA set forth specific security procedures for the company in addition to the security requirements specified in the National Industrial Security Program Operating Manual (NISPOM) required of all DOD contractors to maintain a facility clearance and bid for U.S. classified information. The SSA included procedures regarding telecommunications; procedures for visits and contacts between a sector Y facility or employee located within the SSA ("non-affiliate") and a sector Y facility or employee not within the SSA ("affiliate"); and procedures for the transfer to foreign persons of controlled unclassified information and commodities, technical data, or services subject to International Traffic-in-Arms Regulations (ITAR) and Export Administration Regulations (EAR). In September 2013, Applicant's employer completed a technology control plan (TCP) as an addendum to the SSA, which provided guidance to all personnel regarding the export of technical data and commodities under the EAR and ITAR. (GE 4.)

Applicant held a DOD secret security clearance, and he received security refresher training in May 2014 and SSA/TCP training in July 2014 (GE 3; Tr. 20-21), informing him in part that all communications between employees and affiliate employees were required to be documented, whether they be visits (face-to-face, video teleconference, streaming video), phone conversations, teleconferences, emails, faxes, or voicemails. He also learned that the SSA required submission of a visit request form to the facility security officer tasked with overseeing compliance of the SSA at least three working days before a routine visit and at least seven working days before all other ("non-routine") visits. Any meeting that included access to classified material or an affiliate officer (defined for visit requests as the parent company's CEO and or direct reports) was considered to be a non-routine visit. If a visit request included non-affiliate employees from multiple sites, the employee submitting the visit request was required to submit a contact report within seven days of the visit. (GE 4.)

During the second week of November 2014, Applicant was scheduled to host affiliates at three sites. Three days before the scheduled visits, the sites had not completed a visit request, prompting the facility security officer at Applicant's home site (hereafter FSO) to remind Applicant to submit a visit request for approval and to turn in the monthly logs of phone conversations he had with affiliates. A last minute visit request was submitted on Applicant's behalf by the FSO at Applicant's home site, and the visit request was approved by the chairman of the government security committee (GSC) overseeing the SSA. However, the list did not include the attendees from each site. Applicant was advised to add the missing names to the contact report that was required to be submitted within seven days after the meeting. In early January 2015, the FSO advised Applicant in an email that he was putting both the FSO and the company in a difficult situation by not completing the contact report or monthly telephone logs of his correspondence with affiliates for the past three months. Applicant was asked to submit the paperwork within five days so that the FSO did not have to report the violations. On January 2, 2015, Applicant submitted contact logs for October through

December 2014, and indicated that he would complete the rest of the task over the weekend. Ten days after the FSO's request, Applicant submitted the contact report with the names of employees of non-affiliates at his location, but it included no names of employees from other sites involved in the November 2014 visit. (GE 3.) The FSO testified that when contacted about the logs, Applicant was apologetic, but they had trouble getting Applicant to do the logs. The FSO believes that Applicant was just overwhelmed or negligent and did not deliberately disregard the requirement. (Tr. 22-24.) Applicant denies any recollection of the failure to submit timely visit requests or contact reports or logs. (Tr. 93.)

In mid-November 2014, Applicant was visiting a company site when he asked the facility security officer at the facility to escort him to a closed area to meet with technicians. Applicant had a cell phone in hand. When reminded by the security officer that he could not have his phone in the closed area, Applicant indicated that he understood. However, when in the closed area, Applicant removed his cell phone from his pocket and made a phone call.[2] He left the closed area at the direction of the security officer, but approximately five minutes later, he sought to enter the closed area with his cell phone still in hand. At the request of the security officer, he left the phone outside the room, explaining that he thought he just could not be on the phone in the closed area. (GE 3.) Applicant did not file any report of his visit with his FSO. (Tr. 26.) Applicant was not disciplined for the incident at the time (Tr. 76), but the FSO did not learn of the incident before May 2015. (Tr. 26.) Applicant denies any recollection of the incident involving his cell phone. (Tr. 93-94.) He has no record of his reported visit. (Tr. 98.)

Selected to attend a CEO conference scheduled for May 2015 at his employer's headquarters in Europe, Applicant planned a family vacation in conjunction with that business trip. After the conference was cancelled in April 2015, Applicant went ahead with his trip. Applicant indicates that he had the approval of his supervisor to travel to visit other company sites to broaden his knowledge of the company, and while there, to participate in a weekly financial meeting held with the company's chairman/CEO. Before his trip, Applicant did not complete a SSA visit request or receive required approval from the GSC for his travel to the affiliate location. He did not contact the appropriate "Empowering Official" to confirm that his laptop and phone did not have any Export/ITAR information. Nor did Applicant contact IT personnel to ensure that his electronic equipment was properly updated and protected. While overseas at a company Y affiliate location, Applicant attended the weekly meeting conducted by teleconference between his U.S. supervisor and their foreign chairman/CEO. Applicant emailed a Power Point slide and five Excel spreadsheets that contained detailed

[2] The FSO testified discrepantly from his written report. He testified that Applicant brought his cell phone into a closed area after being advised by the site FSO that he could not have his phone; that the phone rang and he answered it in the closed area. (Tr. 26.) In his written report to his vice president of security, he indicated that while in the closed area, Applicant "reached into his pocket, and pulled out his cell phone and made a phone call." (GE 3.) Whether or not Applicant initiated a call, he had his cell phone in the closed area after he acknowledged he knew he could not have his cell phone in the closed area.

information about his home office's work to an affiliate foreign-national employee in the chairman/CEO's office and asked her to print the attachments. (GE 3.)

Applicant submitted in evidence only one Excel spreadsheet (AE I) and testified that he sent only one email with the financial tracker attached. He also sent a Power Point summary to the affiliate employee, but he does not have it. (Tr. 73-74.) The FSO testified to the Excel spreadsheet containing employee names, customer names, and part numbers. (Tr. 32-33.) Applicant takes issue with sending information containing employee names and part numbers. As for customer names, he testified that "they're all abbreviations, you know, for some of the customer names." (Tr. 74.) Applicant later clarified that AE I consisted of only one page of the Excel file that he sent by email. The Excel spreadsheet had five separate tabs of which AE I is one. (Tr. 88-89.) While he admitted that he no longer had access to the information apart from the single spreadsheet (AE I), he considered it "highly unlikely" that the Excel file contained any employee names or part numbers. (Tr. 89.) On reviewing the spreadsheet in evidence, Applicant acknowledged that it contains abbreviations of programs and some customer and product names, but he indicated that the information was entered by a financial controller. (Tr. 95-97.) Applicant does not consider his conduct to have been a flagrant security violation. (Tr. 75.)

Later that day, the FSO reviewed Applicant's email through the SSA email system. The SSA required security officers to review at least 10% of emails between personnel covered by the SSA and people outside the SSA (affiliates). Noting that there was information in Applicant's emailed attachments that needed prior approval from the GSC for dissemination to affiliates (Tr. 22), the FSO contacted Applicant for his release authority. Applicant indicated that his corporate location overseas did not have networked printers; that the information was on files discussed in a weekly call with his supervisor and the chairman; but also that the files did have program names "which was [his] error for printing with that information." Applicant related that he was "pretty sure" that he had a visit request for his business trip overseas. He expressed his understanding that information being sent to an affiliate needed prior approval. Applicant denied that any of the information was classified, and he expressed confidence that the program and customer information was not associated with any classified programs. The FSO conducted an internal investigation and determined that there has been a visit request approved for the CEO conference, but that the request had been cancelled in April 2015. No security personnel had been notified of any travel for Applicant. The FSO confirmed that the information Applicant had sent via email to the affiliate was not classified, but was associated with classified contracts, and Applicant had not contacted neither the "Empowering Official" for export support nor IT before his trip. Applicant admitted to the FSO that he did not have a visit request approval and did not seek export support. Fortuitously for Applicant and his employer, he had a "clean" loaner laptop that he had received from IT three or four days before his trip. The FSO concluded that Applicant was responsible for an SSA violation in not reporting his foreign travel to an affiliate location[3] and in not requesting approval for

[3] The FSO testified that employees were required to report all foreign travel because of the export and security risk. (Tr. 42.)

release of the information, which contained company-proprietary part names, customer names, program names, and employee names. (GE 3.)

In June 2015, Applicant was given security training by his FSO on DOD security requirements and the SSA requirements. (GE 2.) A week later, he was issued a letter of warning by his supervisor for deliberate disregard of security requirements. He was advised that his security breaches involving his trip in May 2015 were collectively considered a major violation requiring an adverse information report to the U.S. government and that his classified access was suspended pending a decision from the U.S. government about reinstatement. He was advised that any failure to practice diligence in his security-related responsibilities going forward, such as excusing himself from classified discussions, would result in further action up to and including employment termination. (GE 2; AE J.)

The FSO generated a culpability report under ¶ 1-304 of the NISPOM against Applicant "for showing a deliberate disregard of security requirements and a pattern of carelessness" in that he did not complete a SSA visit request, did not receive GSC approval for his travel in early May 2015, did not contact the official regarding export controls before his trip, and did not contact IT to ensure his electronic equipment was properly updated and protected before his trip. Additionally, Applicant did not fulfill his reporting requirements regarding overseas travel, and he sent an email with attachments associated with classified programs to an affiliate without appropriate approval. The FSO also cited Applicant for previous violations involving failure to submit a SSA visit request within the seven days required in November 2014, his failure to turn in a timely contact report after the visit, and his violation involving his cell phone.[4] The FSO advised the government that Applicant had failed to submit SSA visit requests on time and that personnel had arrived at facilities, or Applicant had visited affiliates, without the appropriate visit request. (GE 3.) While Applicant acknowledges that he violated security requirements in May 2015, he submits that he "absentmindedly" did not process a visit request. He attributes his failure to do so to his excitement at going to meet the company's CEO. (Tr. 77.) He admits that he "absentmindedly" did not think to have a check of the loaner laptop completed before his trip. (Tr. 85.) He knew he was required to have the laptop screened. (Tr. 99.)

These security violations were not reflected in Applicant's annual performance evaluations for 2014 or 2015. Applicant was given a rating of exceptional performer for 2014. At his annual rating in February 2016 for 2015, Applicant's manager indicated that Applicant was "instrumental" in leading operations in support of the business through a very challenging year. Applicant "did an outstanding job in filling key leadership roles" at three company facilities, and he was acknowledged for his passion about his work and

[4] The FSO indicated in a memo to the director of security that the cell phone incident happened in November 2014. In the adverse information report, he mistakenly gave a date of November 2015 for the cell phone violation. The SOR alleges a date of November 2015, presumably because of the adverse information report. The incident involving Applicant's use of a cell phone in a closed area is likely to have occurred in November 2014, given it was related in the context of discussing events previous to the May 2015 NISPOM and SSA violations.

the success of the business. He was rated as a strong performer in 2015, and given a 3.00% raise in his base salary. (AEs D-F.) Applicant left the employ of the company in October 2016. (Tr. 87.)

Several co-workers of Applicant's from that employment attest to the high regard in which they held Applicant. As a supervisor, Applicant was respectful of others, cognitive of the importance of his position and their work, and "impressive for controlling what information he divulged." A manufacturing engineering manager who worked for Applicant describes him as "a very passionate and driven employee with a tremendous work ethic." He found Applicant to be honest and trustworthy. Applicant had a "noteworthy achievement" in seeing to the transition of work involving the manufacture of a high precision component from a sister facility to their own. An operations manager indicates that Applicant quickly gained credibility from management staff because of his drive and tireless work ethic. In his experience, Applicant was always respectful of rules, procedures, and restrictions. Regarding a sister company's sub-standard performance and the need for confidentiality, Applicant gave him no reason to doubt or question his integrity. (AE B.)

Another co-worker of Applicant's between 2014 and 2016 first became acquainted with Applicant in August 1982. They previously worked together for some 20 years at company X. Currently a director of quality at the company, he attested to the positive impact that Applicant had on his professional career and the career of others. He would trust Applicant with his children and grandchildren. (AE B; Tr. 60-61.) He testified in person about learning of visit request violations committed by other employees at their unit because these violations were highlighted during mandatory security training. (Tr. 59-60.) In his opinion, the FSO is an "excellent employee [who] does really well with our security at the facility." (Tr. 64.)

The Defense Security Service (DSS) placed sector Y on probation for six months for serious security shortcomings.[5] A new vice president of security was hired, and security training across all sites was more readily enforced. Applicant's home unit was not placed on probation. It received a "major point hit" by DSS during a government inspection in part because of the May 2015 infractions involving Applicant, but also because the DSS felt that the facility did not adequately inform the local DSS representatives about the incidents. (Tr. 36-38, 47-49, 61-62, 64.)

In February 2017, Applicant began working for his present employer, another foreign-owned company with a special security agreement. (AEs A-B; Tr. 103.) He took the position, which pays him a lower salary than his previous employment (AE F; Tr. 72), because it requires only limited travel. (AE A.) Applicant's current manager provided a positive account of Applicant's contributions. His performance has been excellent, and he has fulfilled his responsibilities and duties. The president of the company confirmed that Applicant requires access to both classified and controlled

[5] Applicant denies, and there is no evidence showing that his violations were a factor in sector Y's probation. Applicant admits that his "transgression on [his] trip" was cited against his home site in a separate DSS inspection. (Tr. 79.)

unclassified information as program manager of one of their four business enterprises. Applicant had security training in May 2017, and the president was unaware of internal or external adverse reports having been received by him or the company's FSO. (AE B.) In April 2017, Applicant sought some advice from the FSO at his previous employment about handling controlled unclassified information. (AE H.) On June 23, 2017, Applicant executed a statement of intention not to violate any security requirements with automatic revocation of his security clearance eligibility for any violation. (AE G.) He considers holding a security clearance to be a privilege. (Tr. 102.)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has 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). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered 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 overall 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. 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 ultimate burden of persuasion to obtain 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 that the applicant may deliberately or inadvertently fail to 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. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K, Handling Protected Information

The security concern for handling protected information is articulated in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information—which includes classified and other sensitive government information, and proprietary information—raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The evidence establishes that Applicant violated his then employer's SSA in several aspects. During the second week of November 2014, Applicant was scheduled to host affiliates at three of the facilities within his cognizant responsibilities. Applicant was required under the SSA to submit a visit request form to the FSO at least seven days before such a non-routine visit. He submitted a late request through his FSO, which, while approved by the GSC, was incomplete in that it did not contain the names of all the attendees. The SSA required submission of a contact report by the employee requesting the meeting within seven days following the visit. Despite being reminded to submit that contact report and to account for the non-affiliate attendees on the contact report, Applicant did not submit a contact report until January 2015.

I have no reason to doubt the FSO's report that, in mid-November 2014, Applicant violated security requirements by entering a closed area with his personal cell phone. When reminded by the security officer on site that he could not have his phone in the closed area, Applicant indicated that he understood. However, when in the closed area, Applicant removed his cell phone from his pocket and made a phone call. He left the closed area at the direction of the security officer, but approximately five minutes later, he sought to enter the closed area with his cell phone still in hand. Applicant's lack of present recollection of the security incidents in November 2014 does not mean that they did not occur.

The evidence does not substantiate the date alleged in SOR ¶ 1.c of November 2015 for the cell phone incident, and the Government did not seek to amend the SOR, despite its evidence that the FSO learned about the incident in May 2015, when he contacted security officials at the facility to determine whether Applicant had obtained the required approvals through them for his overseas visit to affiliate locations. The Appeal Board has held that administrative pleadings are not judged by the strict

standards of a criminal indictment and that they should be liberally construed. In ISCR 12-11375, decided on June 17, 2016, citing ISCR Case No. 99-0554 at 4 (July 24, 2000)(citations omitted), the Appeal Board stated in part:

> The purpose of an SOR is to give an applicant advance notice of the allegations against him or her so that the applicant has a reasonable opportunity to respond to them. . . . In assessing the sufficiency of an SOR, it is necessary to balance the need for fair notice to an applicant against the need to avoid transforming the SOR pleading into a game of wits in which a minor or technical misstep is decisive. . . . As long as there is fair notice to the affected party and the affected party has a reasonable opportunity to respond a case should be adjudicated on the merits of relevant issues and not concerned with pleading niceties.

Well-established Appeal Board precedent precludes the administrative judge from denying or revoking an applicant's security clearance eligibility on the basis of conduct not alleged in the SOR. Applicant was placed on notice of security concerns regarding his improper use of a cell phone. Concerning whether the erroneous date defeats adequate notice, Applicant denies any notice of the issue before he received the SOR. He was provided discovery of GE 3, which included the FSO's report of the incident to his director of security in which the FSO identified the incident as occurring on November 18, 2014. Applicant testified about the November 2015 date that the FSO told him that he thought the date was wrong and that it was November 2014. Applicant knew before his hearing that the date in the SOR was likely erroneous. Applicant did not object to lack of notice, and he did not seek a follow-up hearing due to lack of notice. Any objection to lack of notice was waived.

Even if the cell phone violation could properly be considered only for limited purposes such as assessing Applicant's credibility, evaluating his evidence of extenuation, mitigation, changed circumstances, or rehabilitation, or as evidence for the whole-person analysis, ample security concerns arise because of his noncompliance with security requirements in May 2015. He failed to comply with reporting requirements regarding foreign travel. After a CEO conference at his company's overseas headquarters was cancelled, Applicant elected to proceed with the trip. He indicates that he had the approval of his supervisor. However, the evidence establishes that he did not report his travel plans, failed to obtain the required approvals for his visits to affiliate locations, and did not contact either the export control official or information technology personnel before his travel. While at an affiliate location overseas, he emailed information related to classified programs to an affiliate employee without obtaining the proper approval. The FSO subsequently determined that the information was not classified and that no export or ITAR violations occurred, but Applicant did not follow his company's security regulations regarding obtaining approval for sending the company-proprietary information.

Disqualifying condition AG ¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information," is established because of his failures to

submit timely visit requests and contact reports in November 2014; his violation of security procedures regarding use of a personal cell phone in a closed area in November 2014; and, in May 2015, his failure to notify the cognizant security and export control organizations about his foreign travel plans; his failure to contact technology and export control personnel to obtain required authorization to share company-sensitive information while on foreign travel; his lack of contact with IT to have his computer prepared for foreign travel; his failure to submit a visit request for authorization for his teleconference attended by foreign persons and affiliate officers; and his emailing of company-proprietary information in violation of the SSA to a foreign affiliate employee. He did not obtain prior approval for the dissemination, so AG ¶ 34(a) and AG ¶ 34(c) also have some applicability. Those disqualifying conditions provide:

> (a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences; and
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium.

Applicant has the burden of mitigating the security concerns raised by his repeated noncompliance with the rules and regulations for handling protected information. Applicant's failure to comply with the SSA in several different aspects between November 2014 and May 2015 is difficult to fully mitigate under AG ¶ 35(a), even if it may reasonably be considered infrequent in light of his many years of holding a DOD clearance without any security violations or infractions. AG ¶ 35(a) provides:

> (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.

Applicant showed some mitigation under 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," by contacting the FSO, including in March 2017, for guidance regarding handling controlled unclassified information at his present employment. Applicant's current manager and the company's president both corroborate Applicant's compliance with rules and regulations since he began working for their company in February 2017. However, Applicant displayed at his August 2017 hearing an unacceptable lack of accountability for his noncompliance with security requirements in his previous job. Although he testified that he "blew it" when he failed to submit a visit request for his trip to company affiliate locations overseas and failed to have his laptop checked by IT, he attributes these security failures to being absentminded and excited at the prospect of meeting the CEO. It is also difficult to believe that Applicant would have no recall of not submitting the timely visit request,

contact report, and monthly contact logs in 2014, given the FSO and other security personnel had to remind him of his obligations. Regarding the emailed spreadsheets, he testified that he considered it "highly unlikely" that the Excel file contained any employee names or part numbers. Yet, when I asked him to review the spreadsheet in evidence, Applicant acknowledged that it contains abbreviations of programs and some customer and product names. The handling protected information security concerns are not adequately mitigated.

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 his conduct and all relevant circumstances in light of the nine adjudicative process factors listed at AG ¶ 2(d).[6]

Applicant had oversight over five units in five different states. His extensive travel to fulfill his duties for his employer from March 2014 to October 2016 does not excuse his failure to comply in several aspects with the company's SSA. Although there were some security issues at the sector level that led the company to hire a new vice president for security, Applicant had held a security clearance many years, so he is reasonably expected to have known of the importance of complying with security requirements. The high regard in which Applicant continues to be held by his former co-workers weighs in his favor. However, it is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or renewal of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990). Based on the facts and circumstances before me, for the reasons noted above, I do not find it clearly consistent with the national interest to continue Applicant's security clearance eligibility at this time.

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.c:	Against Applicant

[6] The factors under AG ¶ 2(d) are as follows:

> (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.

Conclusion

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

_____
Elizabeth M. Matchinski
Administrative Judge