DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
REDACTED	)	ISCR Case No. 18-02006
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andre M. Gregorian, Esq., Department Counsel
For Applicant: *Pro se*

07/29/2019

_____

Decision

_____

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant caused the improper shipment of classified hardware to a foreign military in February 2013, in violation of security and export control requirements. In June 2014, he placed an order for classified parts from a foreign vendor without contract security classification specifications in existence to ensure that the classified hardware would be protected. Applicant and his employer have implemented procedures to preclude a recurrence. Clearance is granted.

Statement of the Case

On October 22, 2018, 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to*

Classified Information or Eligibility to Hold a Sensitive Position (AG) effective within the DOD on June 8, 2017.

On November 19, 2018, Applicant answered the SOR allegations and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On April 10, 2019, 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. On April 15, 2019, I scheduled a hearing for May 7, 2019.

I convened the hearing as scheduled. Three Government exhibits (GEs 1-3) were admitted in evidence, which included as GE 2 administrative inquiries detailing the security violations alleged in the SOR. A December 27, 2018 letter forwarding the proposed GEs to Applicant and a list of the GEs were marked as hearing exhibits (HEs I-II) for the record but not admitted in evidence. Four Applicant exhibits (AEs A-D) were admitted in evidence without any objections. Applicant testified, as reflected in a transcript (Tr.) received by DOHA on June 4, 2019.

Findings of Fact

The SOR alleges under Guideline K that, in about April 2016, Applicant was found culpable by his employer for the improper shipment/unauthorized export of classified hardware in 2013 from his employer to a foreign country (SOR ¶ 1.a) and that, in about May 2016, he was found culpable by his employer for placing a purchase order with a foreign supplier per the direction of the lead engineer without verifying that a contractual relationship outlining security procedures was in place (SOR ¶ 1.b). When he answered the SOR allegations, Applicant admitted his role in the violations. He provided a detailed response in which he attributed the violations to his failure to validate information provided by the program engineer manager, who had given him "incorrect or overly broad advice." Applicant detailed steps taken to address the systemic issues and knowledge gaps within his company that contributed to the violations. After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is a 53-year-old married father with two daughters, ages 21 and 20. He has a bachelor's degree awarded in June 1989. He has worked for his employer since college. He has held his current Secret clearance since June 2004. He received annual security trainings to as recently as January 2019. (GE 1; Tr. 40-43.)

A violation of the International Traffic in Arms Regulation (ITAR) prompted Applicant's employer to have an independent party review all shipments in the previous five years involving a technical program (program). The review discovered two security violations involving the program for which Applicant and an engineering manager in the program management office (engineer X) were deemed culpable. The details of those violations are as follows.

The first violation (SOR ¶ 1.a) involved the shipment of classified hardware as unclassified to a foreign military in 2013. In February 2011, a foreign military placed a "replenishment spares order" (RSO) for ten units of a part that was identified in the RSO as Confidential. A supply chain manager, Applicant processed the order for his employer. He identified an authorized supplier, who requested the classified drawing needed to build the part. In March 2011, the then lead engineer on the program notified Applicant and three export/import (EX/IM) managers that there was no license authorizing the export of the classified hardware to the foreign country, and that shipment of the parts was dependent on approval of a DSP-85 export license for classified material. The export license was approved in early June 2011. (GE 2; Tr. 45-46.)

In November 2012, the manufacturer sent ten units of the hardware to a company approved for off-site storage and shipping (shipping agent) of the program's repair and return hardware. After nine of the ten units failed an onsite inspection by Applicant's employer, the hardware was returned to the manufacturer for repair. The repaired parts were received by the shipping agent in early December 2012. In mid-January 2013, the shipping agent notified Applicant and a procurement specialist, who as a subordinate assisted Applicant in export control matters, that it would export the parts under the export license to the attention of the security officer. Two days later, on Applicant's order, Applicant's assistant notified the shipping agent that the hardware was not classified, so the shipment should be marked for the supply department. In mid-February 2013, the ten units were exported as unclassified hardware by the shipping agent to the foreign military, who received the parts, but did not alert Applicant's employer about the improper shipment. (GE 2; Tr. 46-48.)

Applicant was interviewed on March 3, 2016, about the shipment during an administrative inquiry by his employer into the violation. Applicant explained that the program team was aware the parts were classified when the purchase order was placed. However, in late 2012, he had a discussion with engineer X, who was new to his position in the program management office and was the authorization official for the purchase order. Applicant indicated that engineer X told him that the part was not classified in a steady state, but that the frequency data inputted during testing was classified, so it then became a classified part. He and engineer X jointly decided that because the part would be shipped in a steady state without the frequency data, it was not classified. (GE 2; Tr. 34, 49-50.) Applicant relied on engineer X, who had been the quality inspection manager and had more expertise about the hardware. (Tr. 51-52.) Applicant acknowledged during his employer's administrative inquiry that he had told his assistant to notify the shipping agent to ship the order as unclassified. (GE 2; Tr. 52.) Applicant and the lead engineer were deemed culpable for causing a security violation in that the classified hardware was not shipped in accord with the marking and packaging requirements of the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M. They also committed an ITAR violation because the hardware was shipped under a DSP-5 export license for unclassified parts and not a DSP-85 export license for classified parts. (Tr. 52.) Applicant's employer concluded that because the classified parts were not properly marked or packaged, the parts were

vulnerable to unauthorized disclosure for the duration of the shipment, which was approximately 16 days, and that compromise was suspected. (GE 2; Tr. 53.) Applicant now understands that he should have sought additional guidance to verify the classification level for the parts. (Tr. 50-51.)

The second violation (SOR ¶ 1.b) involved the placement of an order for classified parts with a foreign supplier without the proper security agreements. In June 2014, engineer X sent an email to Applicant that a Technical Assist Agreement (TAA) with the foreign supplier allowed for the procurement of "pretty much anything classified or unclassified." (AEs A-B; Tr. 54.) The TAA itself provided that "[c]lassified information and material generated under this agreement must be assigned a security classification as specified by the separate contract(s) security classification specifications provided with the contract(s)." (GE 2.) Under the TAA, the foreign supplier was specifically authorized to produce unclassified electromechanical parts and assembly components for the system. (GE 2.) Acting on the advice of engineer X, who as "Authorization Owner" for program licenses served as liaison between the EX/IM staff and the program, Applicant placed a purchase order by email with the foreign supplier for ten units each of two parts that were classified as Confidential. (GE 2; AE B; Tr. 26, 56.) The purchase order contained a mix of classified and non-classified line items. Applicant identified those parts which were classified on the purchase order. (AE A.) The purchase order indicated in the header "Classified Items Exist: No." However, in the details about the order, Applicant noted "L/I 10 and 20 MUST BE MARKED AS CLASSIFIED." (AE B; Tr. 27.) Before placing the order, Applicant was responsible for ensuring that there was a current Contract Security Specification (a DD 254) or a Security Aspects Letter, which was utilized by the company for classified production with foreign vendors without a DD 254. Applicant did not review the TAA and did not verify that a contractual relationship outlining security procedures was in place. There was no DD 254 or Security Aspects Letter for the foreign supplier. (GEs 2-3; Tr. 26-27, 59.) Applicant understands that he should have sought clarification or validation about the scope of the procurement authorization. (Tr. 55.) He cites the low volume of classified purchase orders placed by him as a factor in his failure to ensure that there was a DD 254 for the vendor. (Tr. 58.)

The classified parts were to be imported for inspection by Applicant's employer before being exported. Four days after Applicant placed the purchase order, he received shipping instructions and an import control worksheet from his employer's EX/IM office. The import control worksheet did not include a space to identify the items as classified. Applicant was instructed that the material should be imported on an "ATF" exemption rather than on a DSP-85 license issued for classified material. (Tr. 28.) The import control worksheet listed the TAA as the document authorizing the import. The shipping instructions did not include any handling instructions for classified material. (AE B.)

At the request of the EX/IM official assigned the purchase order, on January 6, 2015, Applicant gave the EX/IM office a separate material classification worksheet for each classified part. Those worksheets were required to import the parts from the

foreign supplier. On each worksheet, the classified part was identified as "Classified" as to the security classification of the product. The following day, Engineer X advised Applicant that their export license compliance manager had said "it is OK to import the two classified and the other unclassified line items against [the TAA]." (AE B; Tr. 29.)

On January 26, 2015, the foreign supplier notified Applicant and one of Applicant's co-workers (a buyer) that "[a]ll 20 items are marked as classified on their individual boxes and are packed in a crate, which was shipped on Friday." (AE B.) On February 3, 2015, new inventory control worksheets were issued for EX/IM officials, which again listed the TAA as the import authorization. On February 11, 2015, the EX/IM official managing the purchase order advised engineer X and a procurement specialist in Applicant's office that if the items were to be imported only temporarily and then shipped right back out, they "should have come in on a DSP61." (AE B.)

The crate containing both classified and unclassified hardware was sent by unsecured means from the foreign supplier to Applicant's employer. (GE 2; AEs A-B; Tr. 59.) Approximately one month later, Applicant had no information that the shipment had cleared U.S. customs, so he alerted the warehouse about the shipment. He indicated in his email that shipments would soon be in transit to the warehouse, including some classified items; that multiple shipments shipped from the foreign vendor were currently in U.S. customs; and that, for the items that are classified, "they will be identified with a label on individual boxes inside the crate." (AE B.) Applicant wanted to ensure that the warehouse was aware of the need to segregate and secure the classified hardware. On March 3, 2015, Applicant received a status report from the warehouse that did not list the classified shipment. (Tr. 31.) Concerned because the shipment should have been received by then, Applicant asked the warehouse for proof of the shipment's delivery. The freight forwarder showed that the shipment was received in the warehouse on February 16, 2015. After Applicant provided proof of delivery to the warehouse, the shipment was located and the classified material, which was marked as Confidential, was then properly segregated and secured. (GE 2; AEs A-B; Tr. 31-32, 60.)

When questioned in January 2016 about his role in the security violation, engineer X asserted that he was told by the export license compliance manager that he could order classified parts from the foreign supplier under the existing TAA. When the compliance manager was interviewed, she stated that she more likely told him that the agreement had a classified component or element, but that he should read the agreement and validate it himself, and contact the EX/IM official assigned the matter. Engineer X never contacted the EX/IM official on the TAA. As a result of his incorrect translation of the TAA and his directions to Applicant, the classified parts were not properly shipped. They were vulnerable to unauthorized disclosure for about four days while in transit and for approximately two weeks while unsecured in the warehouse. Applicant was deemed culpable by his employer for failing to ensure that there was a current contract security classification specification or Security Aspects Letter with the foreign vendor. The foreign vendor held a NATO Secret facility clearance, but the lack of proper security classification guidance raised questions about the methods used by

the foreign vendor for the protection of classified information within its control. Compromise was suspected because it could not be ruled out. (GE 2; AE A.)

Neither Applicant nor engineer X had any previous security infractions on their records. For his role in the security violations, Applicant received a two-week unpaid suspension from work, which was consistent with his employer's published disciplinary process. He was also ineligible for supplemental compensation (merit pay) from his employer in 2017. Applicant was reeducated on the importance of safeguarding classified information. (GEs 2-3; Tr. 44.) His security violations were reported to the DOD on June 3, 2016. (GE 3.)

Applicant immediately set out on March 3, 2016, to establish a procurement procedure to ensure that classified purchase orders would be properly marked. Among the procedures, he established that, on receipt of a classified customer requisition order, supply chain management would identify a supply source and then make a DD 254 determination. Requisitions from the program management office would include in the request the classification for the material. Purchase orders would be required to state "Yes" in the header for "Classified Items Exist," and the buyer would have to note in the header that a DD 254 is required, and to add in the text of the purchase order "The PN for this PO is CLASSIFIED. Department of Defense contract security classification specification, DD form 254 has been forwarded under separate cover." (AEs A, C.) His employer improved its processes to ensure that classified purchase orders and shipments are executed in compliance with regulations. License authorization authority moved from the program management office to an EX/IM role. All company technical information/services and material orders are now vetted to determine whether a U.S. export or import authorization or license is required from the U.S. State Department or U.S. Commerce Department. Checks were established to ensure that new orders are compliant with the authorization. To avoid any ambiguity, for the two systems in his supply chain accountability, Applicant had all the classified material listed in the security classification guidance (SCG) for the systems entered into a material-tracking database against which any new order is matched. If an item is flagged in the database, it is treated as classified. (AE A; Tr. 35-37.) His employer also instituted a transportation plan, and Applicant set up a process to track the transportation of any classified material. (Tr. 32-33, 39.)

Applicant completed more than 40 hours of security authorization and export/import training after the violations were discovered in 2016. (Tr. 44.) As of May 2019, he had issued two classified purchase orders and managed or participated in nine classified shipments since the violations. (AE A; Tr. 61.) There is no evidence that he failed to comply with his company's procedures or NISPOM requirements in those instances. (AE A; Tr. 40.) He sought guidance from his employer's security staff before initiating any purchase order or equipment. (Tr. 61.) In 2019, Applicant was recognized by his employer for his trustworthiness. He has a reputation for always doing the right thing for his company and for maintaining open and honest dialog with leadership and customers. (AE D.)

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.

Applicant violated the NISPOM in several aspects when he caused classified hardware to be shipped as unclassified in February 2013 (SOR ¶ 1.a). The evidence shows that, in February 2011, he processed a RSO for a foreign military customer for parts that were classified Confidential under the program's SCG. As a supply chain manager, Applicant lacked technical knowledge about the parts, so he consulted with engineer X in the program office, who told him that the parts were not classified unless matched to the frequency data. Together, Applicant and engineer X determined that the parts were not classified because they would be shipped in a steady state. NISPOM ¶ 4-103 indicates that classification guidance is the exclusive responsibility of the government contracting activity (GCA). Under NISPOM ¶ 4-104, issues about the classification level are to be discussed with the pertinent GCA. While engineer X may have had some expertise about the parts, Applicant violated his security responsibilities by failing to verify the classification level for the parts.

At Applicant's direction to handle the shipment as unclassified, the shipping agent sent the parts to the foreign military in February 2013 without the markings, packaging, and other security protections required of the NISPOM, and on an export license for unclassified material in violation of ITAR regulations. Under ¶ 4-200, classified material is to be physically marked at the appropriate level to warn and inform holders of the degree of protection required. NISPOM ¶ 5-400 requires that classified material be transmitted in a manner that prevents loss or unauthorized access. NISPOM ¶ 5-401 specifies that classified information be enclosed in opaque inner and outer covers with the inner cover to bear the appropriate classification markings. NISPOM ¶ 5-405 sets forth certain requirements for transmission of classified material to a location outside the United States. Applicant's actions led to hardware classified as Confidential in the SCG being vulnerable to unauthorized disclosure for the duration of the shipment. Compromise was suspected because it could not be ruled out.

Applicant also violated his security responsibilities in June 2014 when he placed an order for both classified and unclassified parts with a foreign vendor that lacked the proper security agreements for supplying the classified hardware. Applicant relied on the erroneous advice of engineer X, who told him that classified items could be purchased from the foreign supplier under the TAA. Applicant did not review the TAA,

which stated, in part: "Classified information and material generated under this agreement must be assigned a security classification as specified by the separate contract(s) security classification specifications provided with the contract(s)." The TAA specifically authorized the foreign supplier to produce unclassified electromechanical parts and assembly components. No DD 254 or Security Aspects Letter existed for the production of classified hardware by the foreign vendor. As set forth in ¶ 4-103 of the NISPOM, the contract security classification specification (DD 254) is a contractual specification necessary for performance on a classified contract. Applicant knew that some of the items in the order were classified. In early January 2015, before the parts were imported, Applicant gave the EX/IM office the material classification worksheets required for the import of the parts from the foreign supplier. The worksheets for each classified part indicated "Classified." While Applicant may have been misled by engineer X about the TAA, and he listed on the material classification worksheets that the parts were classified, neither circumstance relieved him of his security obligation to ensure that a security agreement and security classification guidance existed before he placed the order. His violation of this fundamental security requirement led to classified parts being manufactured by a foreign supplier without adequate security agreements and security measures in place; to the shipment of classified parts by unsecured means to Applicant's employer; and to the classified parts not being properly protected or secured in his employer's warehouse for some two weeks. Compromise was suspected because it could be ruled out.

Disqualifying conditions AG ¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information," and ¶ 34(h), "negligence or lax security practices that persist despite counseling by management," apply. Although compromise was suspected in both instances, it was not proven that protected information was accessed by anyone without the appropriate clearance level and need-to-know. AG ¶ 34(i), "failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent," is not established.

Applicant handled classified information without any problems before the incidents at issue. Nevertheless, he has a significant burden to mitigate the security concerns raised by his noncompliance with the rules and regulations for handling protected information. AG ¶ 35(a) has some applicability because the infractions were infrequent. 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.

Even so, the seriousness with which his employer considered the violations is evident in the discipline imposed. Applicant was suspended without pay for two weeks and ineligible for extra (merit) compensation in 2017.

Applicant has a case for 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." Notwithstanding engineer X's technical expertise about the classified hardware sent to the foreign military, Applicant understands his error in not seeking additional guidance and verification before notifying the shipping agent to treat the parts as unclassified. He accepts responsibility for failing to verify whether the advice from engineer X was accurate about the TAA allowing the procurement and import of classified hardware from a foreign vendor. He also acknowledges that he failed to ensure that there was a current contract security classification specification with the foreign vendor before he placed the order for classified parts. He completed more than 40 hours of security and export/import control training after the violations were discovered. He immediately began taking remedial measures by creating a procurement procedure for classified material. Applicant's employer, with some assistance from Applicant, established and implemented processes to ensure that all technical information and material orders are vetted for the proper export/import license or authorization; that classified material is properly identified under the SCG and then handled appropriately (documented in compliance with EX/IM requirements, packaged, inspected, stored, and transported); that classified shipments are tracked; and that classified purchase orders are properly marked and identified. Applicant's unrebutted testimony is that he has issued two classified purchase orders and managed or participated in nine classified shipments since the violations with no problems.

AG ¶ 35(c), "the security violations were due to improper or inadequate training or unclear instructions," warrants some consideration. Engineer X was culpable in advising Applicant that the hardware to be exported to the foreign military became classified only when matched to the frequency data and that the TAA with the foreign vendor permitted the requisition of both classified and unclassified hardware. As a supply chain manager, Applicant would not have had the same level of technical understanding of the program hardware as engineer X, who had experience as a parts inspector and, as an "authorization owner," was the point person for ITAR requirements; initiated EX/IM licenses and TAA requests; and was liaison with EX/IM officials. EX/IM officials knew or should have known that the TAA was being relied on for the import of classified items from the foreign supplier because the TAA was listed as authorization for the import of the classified parts. Even so, Applicant can reasonably be faulted for not ensuring that a foreign supplier was authorized to manufacture or supply classified components for such a sensitive military system before he placed the order.

AG ¶ 35(d), "the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern," has some applicability. Applicant should have questioned engineer X's assessment that the hardware subject to the February 2011 RSO was not classified in a steady state. However, it was not shown that he deliberately chose to circumvent security requirements for shipping classified hardware. Applicant's behavior with regard to the June 2014 purchase order for classified and non-classified items from the foreign vendor shows that he attempted to ensure that security procedures were followed for handling and shipping classified

information. Available documentation shows that Applicant identified the classified parts in the text of the purchase order submitted to the foreign vendor. He identified the parts as classified on material classification worksheets. He alerted EX/IM officials about the classified nature of the hardware to be supplied by the foreign vendor. When the warehouse had no record of receiving the shipment containing the classified items, Applicant requested a proof of delivery from the freight provider, which showed that the items were in the warehouse. AG ¶ 35(d) does not fully apply, however. Applicant may not have fully understood at the time that the hardware sent to the foreign military in February 2013 was in fact classified, or that the TAA with the foreign supplier in June 2014 required a security agreement for classified parts. He knew in March 2015 that the crate containing both classified and unclassified items had been in his employer's warehouse for approximately two weeks without the classified items being properly segregated and secured. There is no evidence that he alerted his security office about the security violation. Instead, it was discovered approximately one year later, during a five-year review for ITAR violations by his employer. As a longtime employee with a security clearance, Applicant can be expected to have known to report security issues that came to his attention, even if his experience handling classified information was limited.

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 in AG ¶ 2(d):

> (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.

Some of the adjudicative process factors were addressed under Guideline K, but some warrant additional comment. Although it does not excuse Applicant's role in the two security violations, his culpability is minimized somewhat because he relied in good faith on the advice of a lead engineer, who had some technical knowledge of the program as program engineering manager and had authority for requesting TAAs and export/import licenses. Applicant was motivated to perform his duties as supply chain manager properly. He understands now that he should have taken a more active role in ensuring he was complying with security procedures.

The security clearance adjudication involves an evaluation of an applicant's judgment, reliability, and trustworthiness in light of the security guidelines in the

Directive. *See* ISCR Case No. 09-02160 (App. Bd. Jun. 21, 2010). It is not designed to punish applicants for past mistakes or shortcomings. He presented evidence of the procedures instituted by him and his employer to ensure a culture of security compliance at the company. His employer entrusted him with classified information since the violations, and there is no evidence that he failed to comply in any regard with security practices and procedures. While his role in the security violations is not condoned, after considering all the facts and circumstances, I conclude that it is clearly consistent with the national interest to continue Applicant's security clearance eligibility.

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:	FOR APPLICANT
Subparagraphs 1.a-1.b:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, 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.

_____
Elizabeth M. Matchinski
Administrative Judge