DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 14-05396
	)	
Applicant for Security Clearance	)	

Appearances

For Government:
Jeff Nagel, Esquire, Department Counsel

For Applicant:
Arran Treadway, Esquire
Claery & Green LLP

August 31, 2016

DECISION

ROSS, Wilford H., Administrative Judge:

Applicant submitted his Electronic Questionnaire for Investigations Processing (e-QIP), on July 20, 2012. (Government Exhibit 1.) On November 6, 2015, the Department of Defense issued a Statement of Reasons (SOR) detailing the security concerns under Guidelines K (Handling Protected Information), M (Use of Information Technology Systems), and E (Personal Conduct) concerning Applicant. The action was taken under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the Department of Defense on September 1, 2006.

Applicant answered the SOR in writing on November 24, 2015 (Answer), and requested a hearing before an administrative judge. Department Counsel was prepared to proceed on March 9, 2016. This case was assigned to me on March 15, 2016. The

Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on March 18, 2016. I convened the hearing as scheduled on April 18, 2016. The Government offered Government Exhibits 1 through 9, which were admitted without objection. Applicant testified on his own behalf, and submitted Applicant Exhibits A through EE, which were also admitted without objection. Applicant asked that the record remain open for the receipt of additional documents. Applicant submitted Applicant Exhibit FF on April 29, 2016, and Applicant Exhibit GG on May 4, 2016. Both exhibits were admitted without objection. DOHA received the transcript of the hearing (Tr.) on April 27, 2016. The record closed on May 4, 2016. Based upon a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Findings of Fact

Applicant is 55 and married. He has a bachelor's degree in mechanical engineering, and a master's degree in procurement and acquisition management. He is employed by a defense contractor, and seeks to retain a security clearance in connection with his employment.

The Government alleges under Paragraph 1, Guideline K, Handling Protected Information, that Applicant engaged in a course of conduct between approximately August 2012 and April 2013 that showed a noncompliance with security regulations. The Government further alleges under Paragraph 2, Guideline M, Use of Information Technology Systems, that the same conduct showed a noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems. The Government finally alleges under Paragraph 3, Guideline E, Personal Conduct, that Applicant's conduct under Guidelines K and M also shows questionable judgment, or an unwillingness to comply with rules and regulations. He denied all three allegations in the SOR.

Beginning in 1993 Applicant worked for Company A. In approximately 2012 Company B acquired Company A. For many years Applicant was heavily involved in working on a piece of equipment that was covered under a specific Company A contract, Contract One. As part of his work on Contract One, Applicant created a great deal of classified material that had been designed and developed under Company A's program. This material was retained by Applicant in his classified safe. Contract One ended on January 31, 2011.

As part of Contract One's close-out procedure all the materials involving that contract were removed from the possession of all safe custodians, such as Applicant, and transferred to the local location's Facility Security Officer (FSO) safe. This occurred in May 2011. At that time, according to Company B's corporate FSO, "[Applicant] was informed that he could review the [Contract One] materials however they must be returned to the FSO by the end of the day to be kept in the FSO safe." (Government Exhibit 4 at 2.) Applicant did not agree with this decision. (Tr. 117-118.)

Under the National Industrial Security Program Operations Manual (NISPOM) (DoD 5220.22-M)[1] Chapter 5, "Safeguarding Classified Information," Section 7, "Disposition and Retention," Subsection 5-701, "Retention of Classified Material":

> Contractors are authorized to retain classified material received under a contract for a period of 2 years after the completion of the contract, provided the GCA [Government Contracting Activity] does not advise to the contrary. If retention is required beyond the 2-year period, the contractor must request and receive written retention authority from the GCA.

The two-year retention period for Contract One materials expired on January 31, 2013. "However, per [Applicant's] request, twenty three (23) classified materials consisting of CDs and hard copies were retained." According to Company B's corporate FSO a request had been made on October 15, 2012, to transfer these documents to a new contract, Contract Two, that Applicant was then supporting and involved the same piece of equipment. As of May 1, 2013, the request was still pending. (Government Exhibit 4 at 2, Government Exhibit 7 at 8.)

Regarding information systems (IS) use before Company A was purchased by Company B, according to Applicant, "the classified computing systems and the documentation and the hard drives associated with them were all assigned to individual employees, so that individual employees had complete control over the data, the computing system." (Tr. 31.)

After the purchase of Company A by Company B, also according to Applicant, "they went through a transition, and the computers became networked, and they became group property, to the point where you cannot run a classified computing system without the ISSO [Information Systems Security Officer] also logged in physically into the system." (Tr. 32.)

On July 20, 2012, Applicant acknowledged receiving a briefing entitled, "Lab Procedures." Part of the written briefing states, "Classified information will be segregated into hard drives designated for each project. Hard drives are not interchangeable on any other information system." (Government Exhibit 9 at 2.)

The NISPOM in Chapter 8, "IS Security," states in Section 1, "Responsibilities and Duties," Subsection 8-103, "Contractor Responsibilities," at subparagraph c, "All IS users will: (1) Comply with the ISs security requirements as part of their responsibilities for the protection of ISs and classified information. (2) Be accountable for their actions on an IS."

In addition to the requirements of the NISPOM, Applicant's employer has its own Corporate Security Standard Practice and Procedures (SPP). Applicant's conduct, as

[1]Available at http://www.dtic.mil/whs/directives/corres/pdf/522022M.pdf.

described below, is alleged to have violated various SPPs. They will be set forth under the appropriate allegation. (Government Exhibit 5.)

The allegations in the SOR will now be discussed in chronological order:

1.c. It is alleged in this subparagraph that in August 2012 Applicant was involved in knowingly and improperly attempting to introduce four Contract One CDs into an IS system that was accredited only for Contract Two material.

As stated, Contract One had ended in January 2011. The classified information about that contract was located in the FSO safe after May 2011. Applicant acknowledged that he could only have daily access to it. On the date in question, Applicant acquired four CDs containing Contract One material and asked the duty ISSO to burn the material onto Applicant's assigned hard drive. The hard drive was accredited to Contract Two, an active contract, and was not to be used for Contract One data. (Government Exhibit 4 at 2-3, Government Exhibit 7 at 9, Government Exhibit 8; Tr. 97-98.)

Applicant disagreed with the above statement. He testified that he was not informed he could not look or store Contract One material on Contract Two's IS or hard drive until sometime after August 2012. It was his opinion that there were no contract limits on his ability to use the hard drive that was assigned to him. (Tr. 97-105.)

The local FSO became concerned about what Applicant had on his personally-assigned hard drive at that time. She stated:

> When [Applicant] was informed that myself and [the ISSO] would be checking his hard drive to ensure there was no [Contract One] data on the hard drive he became upset, expressing possessiveness with what he referred to as "his data". His behavior suspiciously became excited as though to conceal a hidden agenda. In his frustration he stated that removing the data would change the need of his requested CD's being burnt.
>
> . . . .
>
> After investigating [Applicant's] hard drive we found four complete CD's from [Contract One] consisting of over 3,000 files accounting for 98% of his hard drive data. (Government Exhibit 8 at 2-3.)

Applicant argued that he had permission from the local FSO and the ISSO to introduce the Contract One material into the Contract Two hard drive. (Tr. 30-31, 118-123.) However, Applicant also acknowledged that after January 2011 he was no longer supposed to be working with Contract One materials, since the contract had ended. (Tr. 74-75.)

Applicant's conduct is alleged to have violated SPP 3.5.1, "Loss, Compromise or Suspected Compromise - Processing classified information on a non-approved computer." (Government Exhibit 5 at 2.)

1.b. It is alleged in this paragraph that Applicant possessed Contract One materials without authorization in January 2013. Also, it was alleged that Applicant did not sign appropriate receipts for this material.

After the incident in August 2012, discussed above, Applicant's personally-assigned hard drive was taken from him and stored in the local FSO safe. He was given back the hard drive in early January 2013. This action appears to have been properly authorized. (Government Exhibit 7 at 8.)

On January 3, 2013, Applicant's director sent an email to the local FSO. The email stated, "[Applicant] needs to move his secret data from the FSO safe to the one in [the IS lab] so he can work on it." The director also stated in a later email dated April 23, 2013, "I was unaware that material had been removed from [Applicant's] safe previously for specific reasons and this might be the data he was trying to get back. He did not provide a specific reason he needed the classified data, and I'm not read into the program he is working on." (Government Exhibit 7 at 4, 5.) Applicant agreed with this statement concerning the director's knowledge. (Tr. 105-107.)

Applicant went to the FSO who, based on the director's instructions, gave Applicant his hard drive. The FSO also gave Applicant additional classified material at Applicant's direction. According to the FSO, "He [Applicant] told me the items he wanted from what I remember that they were his; as directed . . . [by Applicant's director] I gave him [Applicant] the files, because I didn't know what he was working on." (Government Exhibit 7 at 3.)[2]

Applicant was given 13 Contract One materials, which he put into his safe. Applicant did not sign internal receipts for the material, and he kept the material in his safe for some period of time. Eventually all the classified material was removed and returned to the FSO safe. Once again, according to Company B, "[Applicant] is aware he cannot have the [Contract One] materials in his possession." (Government Exhibit 4 at 4.)

Applicant also disagreed with this description of the incident. According to him, the FSO and Applicant's director knew the exact nature of the documents he was obtaining from the FSO. (Tr. 39-43, 79-82.) He further stated that the documents were in the safe in his office for approximately a week. This was in violation of the rules. He knew that such material had to be returned to the FSO at the end of each work day. However, he further stated that different FSOs on several occasions gave him permission to have the material in his safe overnight. There were also several occasions, according to Applicant, where he remained at work late, the FSO had left for the day, and he had to store classified material, including Contract One material, in his

[2] *See* Applicant Exhibit GG.

safe. His explanation was to state simply, "Sometimes overnight happens." (Tr. 107-118.)

His conduct in requesting through his director to have classified material transferred to him was alleged to be in violation of SPP 14.5, "Transmission of Classified Material - All classified material being transmitted or dispatched from [Company A] must go through Security." His retention of Contract One materials was alleged to be in violation of SPP 14.11.1, "Completion of a Classified Contract - The materials are to be returned to the Security Office for accountability and proper retention and disposition."

1.a. It is alleged in this paragraph that in April 2013 Applicant put a Contract One CD into an unapproved classified IS and printed classified material, without authorization.

In April 2013 Applicant was still in possession of at least one Contract One CD containing classified information. He went to the ISSO and the ISSM (Information System Security Manager) with the disc and asked them to print a document for him. Proper security protocols were not followed, which required prior permission from Corporate Security to print the document and obtaining a control number for the print out. (Government Exhibit 6.)

After the fact, Corporate Security was contacted and it was discovered that the document was from a Contract One CD. At that time a complete classified inventory of Applicant's safe was conducted and all classified materials were removed and stored in the FSO safe. (Government Exhibit 4 at 4, 5, 7.)

Applicant testified that at the time he did not believe the disc was connected to Contract One. He also stated that it was the responsibility of the ISSO and ISSM to make sure that his printing of the document was authorized. (Tr. 50, 79, 107.)

This conduct was alleged to have violated SPP 14.7, "Reproduction of Classified Material - Approval to print and/or reproduce a classified document must first be obtained from the Security Office and appropriate control numbers shall be assigned."

As a result of the course of conduct described above, Applicant received a letter of reprimand from his management on May 6, 2013. The letter stated that Applicant's actions, as set forth above, "are a clear violation of the company's Corporate Security Standard Practice and Procedures." The letter included this statement of concern:

> The aggressive and persistent nature of your actions in your attempts to gain possession of classified materials in which you were told by corporate security that you could not possess on more than one occasion raises suspicions about your intent in regard to proper handling of classified materials.

The letter goes on to state that Applicant could be terminated for his conduct. He was offered the alternative of accepting one day of leave without pay, which he accepted. Applicant signed the letter, which merely acknowledged that he had received a copy of the letter and had an opportunity to discuss it. (Government Exhibit 5.)

Applicant vehemently disagreed with the decision to reprimand him. There was a great deal of discussion in the record as to the circumstances under which Applicant signed the letter, particularly whether there was coercion. There was also discussion as to whether Applicant could be subject to coercion in the future. As stated, Applicant accepted the letter, and his signature merely signified receipt of it, not that he agreed with the contents. (Applicant Exhibit FF; Tr. 50, 70-74, 85-88, 92-95.)

Mitigation

Applicant is highly respected in his field. A senior government employee, who has worked with Applicant for ten years, states that he has, "utmost confidence that he [Applicant] always handles classified information in accordance with all Department of Defense and Government regulations." (Applicant Exhibits A and B.) Ten other people with knowledge of Applicant's work experience also supplied letters on his behalf. (Applicant Exhibits C-K, P.) Many of them discussed his knowledge of security requirements, and his ability to follow security rules and regulations. He submitted several documents concerning his contributions to his employer. (Applicant Exhibits Q-U.)

Applicant served in the U.S. Air Force for many years as a reservist, retiring in the rank of major. His career was successful, as shown by the awards and commendations he received. (Applicant Exhibits L, V-AA, DD-EE.)

Policies

Security clearance decisions are not made in a vacuum. When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used as appropriate 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 AG ¶ 2 describing the adjudicative process. The administrative judge's over-arching 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. In addition, the administrative judge may also rely on

his or her own common sense, as well as knowledge of the law, human nature, and the ways of the world, in making a reasoned decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that, "Any 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

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 the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance 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. Security clearance decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to protect or 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.

Finally, as emphasized in Section 7 of Executive Order 10865, "Any determination under this order adverse to an applicant shall be a determination 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

Paragraph 1 (Guideline K - Handling Protected Information)

The security concern relating to Handling Protected Information 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 security concern.

I have considered the disqualifying conditions under AG ¶ 34 and especially considered the following:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information; and
>
> (h) negligence or lax security habits that persist despite counseling by management.

I have also considered the mitigating conditions under AG ¶ 35 and especially considered the following:

> (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.

Paragraph 2 (Guideline M - Use of Information Technology Systems)

The security concern relating to the guideline for Use of Information Technology Systems is set out in AG ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

I have examined the disqualifying conditions under AG ¶ 40 and especially considered the following:

> (d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

(e) unauthorized use of a government or other information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations; and

(g) negligence or lax security habits in handling information technology that persist despite counseling by management.

I have also considered the mitigating conditions under AG ¶ 41 and especially considered the following:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

Paragraph 3 (Guideline E - Personal Conduct)

The security concern relating to Personal Conduct is set out in AG ¶ 15:

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

I have examined the disqualifying conditions under AG ¶ 16 and especially considered the following:

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information; and

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the

person may not properly safeguard protected information. This includes but is not limited to consideration of:

(3) a pattern or dishonesty or rule violations.

I have also considered the mitigating conditions under AG ¶ 17 and especially considered the following:

(c) the offense is minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

The analysis begins with what is given. First, Applicant is an able, talented and competent engineer. His contributions to the defense industry, the Air Force, indeed the nation, have been substantial. Second, Applicant, by his own admission and as stated by others, is knowledgeable about security issues. He has held a security clearance for many years and obviously knows his responsibilities. Third, Applicant was intimately involved for many years in work under Contract One. He created literally thousands of pages of classified material while working on this contract.

It is Applicant's conduct with regard to Contract One after the contract ended that is at issue here. He obviously felt a sense of ownership and entitlement about the material he had created over the years concerning this contract. From the evidence, and indeed as stated by him, it is clear that Applicant had serious issues with the security requirements imposed on him after the contract ended. He felt that the requirements were onerous, unnecessary, and impacted his ability to do his job. What is also clear is that he knew, or should have known, what those security requirements were and that he had a responsibility, whether he liked it or not, to follow them.

Based on my analysis of all of the evidence, I find that Applicant did commit all the acts alleged in the SOR. I further find that the acts were intentional, and that he was responsible for all of them. By that I mean he committed them knowingly, and he did them in an attempt to work around the strictures on his access to Contract One material. Applicant attempted to say that the FSOs or the ISSOs had responsibility to make sure he was following the rules. There may indeed be instances of joint culpability here. However, at all times, as Applicant well knows, he is individually responsible for following security rules, no matter what other people may do.

The essential basis of this case is that, from August 2012 through April 2013, Applicant consistently acted in such a way as to keep working on and with documents that were connected to Contract One. That contract had ended. His employer had responsibilities under the NISPOM to control the classified material related to that contract, and in accordance with that responsibility they had moved the material to the local FSO safe. Applicant was told repeatedly that he could only have daily access to the material. He understood that stricture, even though he adamantly disagreed with it. However, he repeatedly acted in such a way as to circumvent the requirement.

The August 2012 incident is undoubtedly Applicant's responsibility. As of July 20, 2012, he knew that his hard drive was designated for a specific project, Contract Two. In fact, there is written confirmation of that fact. Instead of using it for that project, 98% of the hard drive had files connected to Contract One. This was entirely inappropriate and he knew it at the time. As a result of his conduct, his hard drive was taken out of his control and stored in the FSO safe.

In January 2013 Applicant attempted to work around the strictures on his access to Contract One material by using his director, who was not read into his program, as a go-between. There is no denying that Applicant took material connected to Contract One, as well as other classified material, and put it into his safe without authorization. Once again, and it cannot be emphasized enough, Applicant had been repeatedly told, and understood, that he had to return such material to the FSO at the end of each work day. He did not. Instead he retained the material for some unknown period of time. He says it was about a week, but since the FSO did not know that Applicant had the material, there is no way to say for sure. In addition, as Applicant admits, he continued to have at least one Contract One CD into April 2013. Once again, Applicant attempts to deflect blame onto the FSO, by saying he had permission to retain the material in his safe. However, the FSO has stated that he had no knowledge of what Applicant was working on. Therefore, the FSO could not have knowingly given Applicant permission to retain the material, which Applicant knew he could not retain overnight.

In April 2013 Applicant had the FSO and ISSO print a document from a Contract One CD. He states he did not realize it was a Contract One CD, but I frankly find that statement difficult to believe. He obviously knew the material. In addition, if he had gotten the FSO and ISSO to follow procedure and obtain permission and a control number before printing, as they should have done, it would have been discovered that the document was from Contract One.[3]

By this time Applicant's management had enough. The letter of reprimand Applicant received shows the seriousness with which his management took his repeated attempts to work with material on a contract that had ended more than two years earlier.

Applicant continues to this day to deny he did anything wrong concerning his attempts to store and use Contract One material without permission. He states repeatedly that the documentation was essential for him to do his job and support the mission. The fact is there is virtually no support for that statement. But even if true, that is not relevant to the discussion. It is obvious that Applicant believes that his requirements to supersede security rules. Security rules can be, and often are, onerous. What they are not, under any circumstances, is voluntary. Applicant treated them as such, and continues to argue that his interpretation is correct. It is not. All of the

[3]I agree that both the FSO and ISSO may have some culpability here. They also knew the rules and should have followed them in order to get prior permission, and receive a control number, before the subject document was printed. However, as previously stated, Applicant also had a personal responsibility to make sure that all security rules were followed.

disqualifying conditions described above, under all three guidelines, support security concerns based on this evidence. None of the mitigating conditions were established and mitigate his conduct, particularly given that he refuses to acknowledge he has done anything wrong. I find against the Applicant under Guidelines K, M, and E.

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 the applicant's conduct and all the relevant circumstances. 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. The administrative judge must 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 considered the potentially disqualifying and mitigating conditions in light of all the relevant facts and circumstances surrounding this case. The discussion under Guidelines K, M, and E, above, applies here as well. Applicant did not provide sufficient evidence to mitigate his conduct under any of the guidelines. His conduct was serious, and he knew what he is doing. I do not find that there is sufficient evidence of rehabilitation or other permanent behavioral changes. In particular, based on my analysis of the evidence, I cannot find that Applicant would be likely to properly obey security rules and regulations in the future if faced with the same or similar circumstances. Under AG ¶ 2(a)(2), I have considered the facts of Applicant's conduct, including his repeated attempts to circumvent security requirements with which he disagreed, and find that there is the potential for pressure, coercion, exploitation, or duress (AG ¶ 2(a)(8)).

Overall, the record evidence leaves me with continuing questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from his noncompliance with security regulations, misuse of information technology systems, and personal conduct. Accordingly, the evidence supports denying his request for a security clearance.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by ¶ E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

WILFORD H. ROSS
Administrative Judge