DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-06315
	)	
Applicant for Security Clearance	)	

Appearances

For Government: John B. Glendon, Esq., Deputy Department Counsel
For Applicant: Mark S. Zaid, Esq.

02/29/2016

Decision

MASON, Paul J., Administrative Judge:

On June 21, 2011, Applicant displayed a serious lapse in judgment when, without authority, she copied and sent classified proprietary budget information to three of her company supervisors. However, she has committed no other security violations or unethical behavior in her military and civilian career that spans almost 40 years. Having weighed and balanced all the circumstances, Applicant's laudable character evidence outweighs the seriousness of her misconduct. Eligibility for access to classified information is granted.

Statement of the Case

Applicant certified and signed her Electronic Questionnaire for Investigations Processing (e-QIP) on August 6, 2013. She was interviewed by an investigator from the Office of Personnel Management (OPM) on September 10, 2013. The interview summary was not entered into evidence. On January 6, 2014, DOHA issued a Statement of Reasons

(SOR) detailing security concerns under personal conduct (Guideline E), criminal conduct (Guideline J), and noncompliance with regulations pertaining to information technology systems (Guideline M). 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), implemented by DOD on September 1, 2006.

Applicant submitted her notarized answer to the SOR on January 28, 2015. DOHA issued a notice of hearing on August 6, 2015, for a hearing on September 16, 2015. The hearing was held as scheduled. At the hearing, the Government called one witness. Six exhibits (GE 1-6) were admitted in evidence to support the Government's case. Applicant and three witnesses testified. Nine exhibits (AE A, B, D-J) were admitted in her behalf without objection. Applicant's four post-hearing exhibits (AE K-N), were admitted in evidence without objection. DOHA received the transcript on September 24, 2015, and the record closed on October 1, 2015.

Rulings on Procedure and Evidence

I am taking administrative notice of 18 United States Code (U.S.C.) § 641 (HE 1). I will also take administrative notice of AE C (information about carbon monoxide poisoning and its effect on the body and mind), which has been remarked as HE 2.

Findings of Fact

The SOR alleges that on June 21, 2011, while working as a contractor employee for X company supporting a government agency, Applicant, without authorization, sent classified proprietary information to three of her X-company supervisors. Her conduct constitutes questionable judgment under both the personal conduct (SOR ¶ 1.a) and the criminal conduct guidelines (SOR ¶ 2.a). Her conduct also raises security concerns under the guideline for noncompliance with rules and regulations pertaining to information technology systems (SOR ¶ 3.a). In her answer to the SOR, Applicant qualified her admission to SOR ¶ 1.a by noting that she was unaware the information was classified. She denied SOR ¶¶ 2.a and 3.a.

Applicant is 60 years old. She has been married since March 1984. She received a bachelor's degree in political science in May 1977, and a master's degree in public administration in June 1994. She served in the United States Air Force (U.S.A.F.) from May 1977 until her honorable discharge as a colonel in June 2007. She is currently in the Air Force Reserve. Since February 2013, she has been employed as a senior analyst with a defense contractor (Z company). Before her current employment, she was a policy analyst promoted to a project manager for another contractor (X company) from June 2010 to

February 2013. Applicant has held a security clearance since she began her military career in May 1977. (GE 1 at 16; Tr. 156)

Identification of Hearing Witnesses

Government's witness

S/A - special agent from the inspector general's (IG) office of Y federal agency.

Applicant's Witnesses

Witness A - division chief of the science and technology office of Y agency in June 2011.

Witness B - former employee of Y agency who worked with Applicant from 2010 to January 2015; currently operates his own company.

Witness C - chief of staff of Y agency; currently chief operating officer (CEO) of Z company, Applicant's current employer.

X Company - Applicant's former employer when she copied and sent email in June 2011.

Z Company - Applicant's current employer since February 2013.

In June 2011, Applicant, a contract employee (policy analyst) with X company, was working with about 15 other contract and government employees in an office of science and technology for Y federal agency. She was supervised by a senior government employee whose title was division chief (witness A). Due to witness A's heavy meeting schedule inside and outside the office within Y federal agency, he sent an email invitation to Applicant and other staff employees (he was unable to identify) indicating that they could add to his computer calendar application. The next day Applicant viewed witness A's calendar and saw a meeting invitation that he had accepted. The meeting notice invitation had an attachment containing classified proprietary budget information for an element of Y agency that had a potential impact on Applicant's company. Mistakenly believing she had authority to view the attachment, she opened it, copied the classified budget information, cut-and pasted it in an email, and sent it to three X company supervisors, thereby potentially giving X company an unfair competitive advantage over other bidders on task orders (TO) of a contract that Y agency had. The entire process took about 15 seconds. An investigation by a S/A of the IG of Y agency followed and determined that Applicant committed a theft of information in violation of 18 U.S.C. §641. (Tr. 126-131)

In support of its *prima facie* case, the Government called the S/A of the IG of Y federal agency to testify about his investigation of Applicant. He explained that the investigation was focused on a theft of government information (18 U.S.C. § 641) and whether X company gained and unfair competitive advantage on a contract or contracts. He began his portion of the investigation in May 2012, by reviewing the case file, then reviewing the computer calendar of the witness A of the office of science and technology of Y agency. The calendar contained an attachment with estimated classified proprietary budget information to a meeting appointment invitation that witness A accepted. (Tr. 16-19, 37)

On June 20, 2011, the S/A learned that witness A sent invitation requests for Applicant and certain other contract and government employees to have access to his computer calendar. The computer calendar allowed persons to schedule meetings, accept meetings, and attach documents that pertained to meetings scheduled. The purpose was to allow the employees to add information to witness A's calendar so he could keep track of progress made on their activities. According to the S/A, the invitation did not allow them to remove information or search his calendar. (GE 6 at 16; Tr. 20-22)

The S/A discovered that on June 21, 2011, Applicant opened and extracted the budget information attachment to an appointment invitation on witness A's calendar. She cut and pasted the information to an email. He indicated that she indicated in about two sentences in the email that the budget information related to upcoming TOs that X company was negotiating on a contract that Y agency had. When asked how much time elapsed in the copying, pasting, marking, and sending of the classified email, the S/A indicated about 15 seconds though he really did not know. According to the S/A's interview with witness A, Applicant did not have a need to access the budget calendar because her job responsibilities did not involve budget and financial activities. The S/A noted in his May 2013 report that he was unable to prove that X company management used the classified budget information to gain an unfair advantage on the pertinent contracts, or that the information left the classified system. (GE 5 at 2, ¶ 7.c; GE 5 at 3, ¶ 8.d; GE 6 at 11-13; Tr. 23-25, 39-41, 47-48, 65)

Applicant was interviewed by an S/A of Y agency on October 4, 2012, about 16 months after she sent the email. Though she signed a statement prepared by the S/A initially denying that she sent the June 21, 2011 email, and admitting that she sent the email after the S/A showed it her, the S/A acknowledged at the hearing that when he initially asked her whether she had originally sent the email, she responded that she was not sure or did not recall. According to the statement, when presented with the email, she admitted sending it, but denied stealing the budget information. Under the circumstances of his criminal investigation to determine whether Applicant stole government budgetary information and emailed it to her X company supervisors, the S/A did not agree that her failure to recall was synonymous with denying she sent the email. Further, he did not believe that her later admission to sending the email was the same as recalling she sent the email to the three X company supervisors. The S/A was directed to the third paragraph of Applicant's October 2012 statement indicating that

she knew it was wrong to provide the information to her three X company supervisors and that she sent the information thinking it would benefit X company management. The S/A testified that when he asked Applicant why she sent the information, she initially responded that she was really not sure. She agreed with the S/A's suggestion that wanting to please X company while receiving personal benefit made sense as motives. If, however, Applicant did not believe that she had committed a crime in copying and sending the email, the S/A acknowledged that she may not have had the requisite state of mind to commit a crime. (GE 4 at 1, ¶ 4; GE 6 at 11-13; Tr. 48-50, 61-65)

The S/A testified that after Applicant sent the email in June 2011, she did participate in one of the task orders related to an upcoming contract with Y agency, but did not use any of the budgetary information contained in the email. (GE 6 at 13; Tr. 53-54)

On May 24, 2013, the S/A presented his findings to the inspector general (IG) of Y agency who concluded that the theft of information (18 U.S.C. 641) allegation was substantiated. On December 12, 2012, the Assistant United States Attorney (AUSA) determined that there was credible evidence supporting a charge of theft of information by Applicant. The AUSA declined to prosecute the theft offense because damage to the Government could not be determined and the offense "did not warrant prosecution." (GE 5 at 7, ¶ 12; GE 5 at 7, ¶ 13)

Applicant called three witnesses to testify. The testimony of witness A will be addressed first because in June 2011, he was the division chief of the science and technology office when Applicant sent the email.[1] He was the senior government employee who had daily contact and oversight of Applicant and about 15 other contract and government employees. (GE 5 at 3, ¶ 8.d; GE 6 at 2-3; Tr. 126-132)

Witness A gave calendar access to Applicant and probably a couple of other contract employees to help him manage and prepare his meeting schedule. He identified a June 20, 2011 email sent out to Applicant and other employees as a typical calendar invitation to give his employees access to his day-to-day activities "so that they would understand what [witness A] needed support with." Though he is currently aware that access to his personal calendar includes access to any attachments posted to that calendar, he was not aware in June 2011 that by accepting a calendar invitation with an attachment, the attachment would be posted to

[1] Currently, witness A is the senior operating officer for an office within the larger office of science and technology. (Tr. 124)

the calendar and visible to others with access to his personal calendar.[2] He did not recall any written or verbal restrictions or warnings on the contract employees who had access to his calendar. (GE 5 at 3, ¶ 8.d; GE 6 at 2-3; Tr. 126-132)

Witness A could not recall whether the budget information had markings indicating that it was restricted to government employees. In his view, marking the information as government proprietary was a good practice in order to keep it out of the possession of contract employees. Witness A conceded that he may not have properly marked the budget information. With the help of the IG of Y agency in March 2012, witness A instituted a restriction on the computer calendar meeting invitations to government employees with a need to know in order to prevent a future recurrence of the June 2011 incident. (GE 5 at 4, ¶ 8.h; Tr. 132-140)

The first time witness A learned that Applicant sent classified budget information to her three X company supervisors was in September 2012, when he was contacted by S/A of Y agency. On receiving this information, he was stunned because her conduct was inconsistent with her flawless security record and her expertise as an intelligence officer and strategic thinker. He was aware that in June 2011, Applicant had a personal or family issue and he later found out her mother passed away. In sum, witness A believed that Applicant's transmission of the email was a misuse of information that was not supposed to be furnished to her, and was probably due to a mistake by a government employee or witness A in failing to mark the information properly. (GE 5 at 4, ¶ 8.h; Tr. 132-148)

Applicant explained that witness A endorsed the idea of giving more access to his computer calendar so he could coordinate his meetings and outside activities because he expected the staff employees to operate the office when he was out of the office. When Applicant accepted access to witness A's calendar, she believed she would:

> be able to add meetings to his calendar with his coordination and that if there was something within the calendar that [Applicant] needed to be aware of because it was part of the invitation that [Applicant] should and would be obligated to review that as part of [her] review of his daily calendar. (Tr. 157)

Applicant indicated there were no written or verbal limitations on her when she accessed anything in the calendar. There were no limitations within the computer calendar program that limited access to the calendar. She believed that she had complete access to the calendar and its contents. She believed that all contract and government employees of witness A's work

[2] The division chief was not aware of the visibility of the posted attachments because his first use of the computer calendar application was in 2010, when he began employment at the science and technology office at Y agency. (Tr. 124, 143)

group had access to his calendar. She held that belief in November 14, 2014, when she provided answers to the government's interrogatories. (GE 2 at 3; Tr. 157-160, 182-183, 190)

On June 21, 2011, witness A was not present in the office when Applicant pulled up the calendar to help prepare witness A for meetings. She saw this meeting invitation with an unusual icon embedded in the message. Because she wanted to determine whether there was something about the meeting she should know, she clicked on the icon and saw that it contained a table with fiscal year (FY) budget information for 2012. She copied the budget information, cut and pasted it in an email and sent it to three supervisors in X company. Not knowing why she copied and sent the email was probably due to the minuscule amount of time (about 15 seconds) to prepare and send the email. Thinking the budget information would benefit her team, she sent the email containing the budget information without fully comprehending the ramifications of her transmission. (Tr. 157-160, 182-183, 191, 198-199)

In the June 2011 time frame, Applicant recalled having difficulty maintaining attention at work because of her mother's medical condition. On June 21, 2011, she received a call (about the same time that she sent the email) that her mother had only 48 hours to live. While Applicant was upset over her mother's illness and imminent death, it is no excuse for sending the email to her supervisors. (Tr. 160-163)

Applicant was notified of the IG investigation in October 2012. Between June 2011 and October 2012, she had no further contact with the budget information. In January 2012, Applicant and her husband experienced carbon monoxide poisoning because of a faulty home furnace. She indicated that she was hospitalized for three days and sustained various mental and physical problems which, according to the medical records, improved substantially in the year. She has some lingering memory issues. (HE 2; AE J; Tr. 166-172)

Concerning Applicant's interview with the S/A in October 2012, she did not recall the June 21, 2011 email until he showed her the email. After she stated that she was not sure why she sent the email, she informed the S/A that his suggested motives of wanting to please X company while gaining personal benefit sounded reasonable. Even though she did not agree with the S/A's suggestions for her conduct, she did not want to give the impression that she was withholding information or being dishonest in her responses during the interview with the S/A. (Tr. 173-180)

Applicant indicated her conduct in the June 21, 2011 incident was a regrettable but isolated incident in almost 40 years of having security clearance access. She does not believe she will make this mistake again. Should she confront a similar situation in the future, she will seek advice in determining whether she has authorized access, including a need to know. In October and November 2012, she completed two courses on remedial ethics training.

Applicant enjoys her work. She is an elder and a school teacher in her church. She enjoys reading. (AE A, B; Tr. 181, 184-188)

Character Evidence

Witness B, a retired U.S.A.F. colonel, who owns his own company, testified that he met Applicant in 2010, when she was working for X company and he was working for another contractor. He hired her into a policy position to assist him in preparing projects on a daily basis. In 2012, they went to different job locations, but continued to work on the same project and communicated with each other about once a month. Witness B was not aware of the June 2011 email incident, but did know that Applicant's mother was seriously ill during the month, and her mother's condition appeared to have an impact on Applicant's attention at work. After Applicant told him about her mother's condition, he provided her more time to submit support data for his projects. In the time witness B worked with Applicant, she has always followed security rules and regulations. Witness B would recommend Applicant for a position of trust because he believes her conduct was a mistake and unintentional. (AE H; Tr. 78-89)

Witness C was employed by Y agency for 20 years. When he left the agency in 2004, he was the agency's deputy director for administration and chief of staff. After working for another federal agency for about a year, he was hired by Applicant's current employer (Z company) in 2006, and is presently the chief executive officer (CEO). Witness C held several security clearances while he was employed by two federal agencies, and those clearances are still active. In early 2013, Z company was looking for a candidate with a policy and intelligence background. During her employment interview, Applicant told witness C about the IG investigation. Though Applicant was hired, witness C could not keep her because the open IG investigation prevented her from working on any Y agency contracts. Z company is still sponsoring Applicant. (Tr. 94-101, 108-110)

Witness C reviewed Applicant's interrogatory answers dated November 14, 2014, and recalled having discussions with her about the content of her answers in the exhibit. In June 2011, she was a senior staff person who was allowed access to information, including information in the computer calendar, to improve her performance on behalf of her supervisor. Based on witness C's discussions with Applicant, there was some question in June 2011 whether the classified information (that Applicant copied and sent in an email) was unauthorized. It was not until later that it was determined during the investigation that the information should not have been "shared." Though witness C believes Applicant should not have copied and sent the email to her company, he believes witness A was in error by having the attachment available on his calendar. Applicant's access and transmission of the attachment in June 2011 was a mistake in an otherwise outstanding career showing no security incidents. Witness C still recommends Applicant for a position of trust. (GE 2 at 3-4; AE I; Tr. 102-106, 108-111, 117-120)

Applicant provided her *vitae* and her record of awards and medals received while on active duty and in the Reserve. (AE A, B)

Applicant also furnished eight character statements. Reference D has known Applicant since she began her employment with Z company in February 2013. Reference D believes Applicant's SOR action is an aberration to her historical compliance with security procedures. The reference recommends Applicant for a security clearance. (AE D)

Reference E, a consultant, has known Applicant since 2005 when Applicant was in the military and reference E worked for Y agency. Because he believes that Applicant made a mistake that she will not repeat, reference E recommends Applicant for a position of trust. (AE E)

Reference F, who met Applicant in 2003, under similar circumstances as Reference E, does not have first-hand knowledge of the circumstances of the SOR, but believes her mother's serious illness had a negative impact on Applicant's otherwise "normal attention to duty." Reference F recommends Applicant for a security clearance. (AE F)

Reference G is a program manager for Z company. Based on his recommendation, Z company hired Applicant in February 2013, and they occupied the same work location for about a year in Z company. In Reference G's opinion, Applicant deserves security clearance access because her poor judgment in the email incident will not be repeated. (AE G)

Reference K, a retired military officer and intelligence officer for Y agency since 2002, has known Applicant since 2010, when she worked for X company. In his professional association with Applicant, she has always complied with security rules and procedures. Her June 2011 email incident was a mistake in judgment and does not preclude Reference K from recommending her for a position of trust. (AE K)

Reference L, a vice president of a consulting company, has known Applicant since 2007. Applicant has always followed security rules and procedures. Reference L, who was one of the supervisors who received the June 2011 email containing the classified proprietary information, believes Applicant made a mistake in sending the email, rather than sending it for personal gain. She recommends that Applicant be granted a security clearance. (AE L)

Reference M is a business manager for a consultant company. He has known Applicant since 2010, when they worked together at a Y agency location. Though he has no first-hand knowledge, he believes the SOR incident was a mistake in judgment in a career where she has always complied with security rules. He recommends her for a security clearance. (AE M)

Reference N, a defense expert in intelligence for Y agency since 2009, has known Applicant since 2011. She became his trusted advisor. Reference N has no knowledge of

Applicant's conduct in the SOR, but has never observed that conduct in the time he worked with her. He recommends her for position of trust with the Government. (AE N)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the AG. Each guideline lists potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an applicant's eligibility for access to classified information.

The administrative judge's ultimate goal is to reach a fair and impartial decision that is based on commonsense. The decision should also include a careful, thorough evaluation of a number of variables known as the "whole-person concept" that brings together all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision. Likewise, I have avoided drawing inferences grounded on speculation or conjecture. Decisions include, by necessity, consideration of the possible risk 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 the potential, rather than actual, risk of compromise of classified information.

Under Directive ¶ E3.1.14., the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.l5., 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 as to obtaining a favorable security decision.

Analysis

Personal Conduct

The security concern for personal conduct is set forth in AG ¶ 15:

> AG ¶ 15. Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following potentially disqualifying conditions under AG ¶ 16 are:

AG ¶ 16(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 the person may not properly safeguard protected information. This includes but is not limited to consideration of: (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information; (2) disruptive, violent, or other behavior in the workplace; (3) a pattern of dishonesty or rule violations; and (4) evidence of significant misuse of Government or other employer's time or resources; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign country or intelligence service or other group.

On June 20, 2011, Applicant received an email from witness A informing her that she and a few other contract and government employees on his staff could add to his computer calendar. The purpose of the email was to let the staff know where he was and what events he needed support with. On June 21, 2011, Applicant abused her authority when she copied the contents of the classified proprietary meeting invitation attachment to witness A's meeting invitation. She compounded her misconduct by copying and pasting the information, then sending the contents to three supervisors at X company, her employer. Her conduct, though brief, falls within the ambit of AG ¶ 16(d)(4). However, AG ¶ 16(d) applies to conduct "not explicitly covered under any other guideline." Since Applicant's alleged criminal conduct is specifically covered under Guideline J (AG ¶¶ 30-32), and her unauthorized preparation and transmission of the classified proprietary information is specifically addressed under Guideline M (Use of Information Technology Systems, AG ¶¶ 39-41), the security implications of her conduct will be discussed under those guidelines. I do not believe AG ¶ 16(e)(1) applies because Applicant has been cooperative throughout the course of the security investigation. Her inability in October 2012 (S/A interview) to immediately recall an email that she generated 16 months earlier in June 2011, does not create a vulnerability to coercion under circumstances of this case. I conclude her responses to the government's interrogatories in November 2014 were based on the erroneous belief about the scope of her authority, and do not create a vulnerability to coercion and duress.

The mitigating conditions under AG ¶ 17 that are potentially pertinent are:

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

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate stressors, circumstances, or factors that caused untrustworthy, unreliable or other inappropriate behavior, and such behavior is unlikely to recur; and

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

Though not minor, Applicant's mishandling of classified proprietary information was an isolated incident that was brief in duration, and occurred more than four years ago. There is sufficient evidence from Applicant and witnesses B and C that shows her mother's serious illness clouded her judgment in June 2011. There is evidence showing that witness A may not have placed the proper classified markings on the budget information attachment and was not aware that attachments on the computer calendar were visible to staff employees. The remedial action taken in March 2012 by the IG and witness A to prevent the June 2011 incident from recurring, cannot be overlooked. I conclude that the incident was an exception in an impressive military and civilian record. Though it has taken some time for Applicant to fully comprehend that her June 2011 conduct was inappropriate and unauthorized, she laments the poor judgment she exercised in June 2011. I am confident she understands that she will not repeat similar behavior in the future. Assuming that Applicant's personal conduct is found to create vulnerability to coercion, the circumstances have changed. She never tried to conceal her mishandling of the classified proprietary information. Once she saw the email in October 2012, she remembered generating it. She fully realizes her poor judgment and has credibly explained the measures that she will institute to ensure she receives the necessary access under a need to know. AG ¶¶ 17(c), 17(d), and 17(e) apply.

Criminal Conduct

The security concern for criminal conduct is set forth in AG ¶ 30:

Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

AG ¶ 31 of the criminal conduct guideline lists two disqualifying conditions that may be applicable to this case:

(a) a single serious crime or multiple lesser offenses; and

(c) allegation or admission of criminal conduct, regardless of whether the person was formally prosecuted or convicted.

Though the IG of Y agency and the AUSA determined that a theft of information occurred, I disagree that the elements of 18 U.S.C. § 641 have been met. Theft is the taking of a person's property with the intent to permanently deprive the owner of that property. After weighing and balancing the October 2012 statement and the testimony of the S/A and Applicant, I conclude that Applicant did not have the requisite intent to steal the classified information when she copied and sent it to her three supervisors. There is no direct or circumstantial evidence that she permanently deprived the Government of the proprietary classified information. After her viewing of the information, cutting and pasting it in an email, then sending the information in a time period of about 15 seconds in June 2011, Applicant never saw the information again until October 2012, when she was interviewed by the S/A. In sum, Applicant's motive for sending the classified email was driven by her misunderstanding of the scope of her authority over the contents of witness A's computer calendar system, rather than an intent to steal the information. On the other hand, 18 U.S.C. § 641 includes the language "or knowingly converts to his use or use of another." Even though the element of knowledge is missing from the offense, Applicant's exercise of control over classified proprietary information without authorization is sufficient for come within the reach of AG ¶ 31(c).

AG ¶ 32 lists two pertinent mitigating conditions that may be applicable in this case.

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

(d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community development.

Assuming that Applicant's June 2011 actions in preparing and sending the classified information constitutes criminal conduct, AG ¶¶ 32(a) and 32(d) apply to mitigate those actions for the same reasons discussed under AG ¶¶ 17(c) and 17(d). Additionally, Applicant is active in her church as an elder and teacher.

Use of Information Technology Systems

The security concern for AG ¶ 39 is:

> 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 computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The potentially applicable disqualifying conditions under AG ¶ 40 are:

> (a) illegal or unauthorized entry into any technology system or component thereof;
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;
>
> (d) downloading, storing, or transmitting classified information on to or to any unauthorized software, hardware, or information technology system; and
>
> (e) unauthorized use of a government or other information technology system.

The June 20, 2011 email provided Applicant the ability to add information to witness A's calendar. Applicant abused her authority by copying and sending the email to her three company supervisors. AG ¶¶ 40(a), 40(c), 40(d), and 40(e) apply.[3]

The potentially mitigating condition under AG ¶ 41 is:

> (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.

As discussed under AG ¶¶ 17(c) and 17(d), Applicant's June 2011 conduct is mitigated by the passage of time coupled with the unusual circumstances of her mother's serious illness. The probability that the classified attachment was not properly marked (by a government

[3] While the S/A testified that Applicant placed classified markings on the email, I am unable to determine why he would not corroborate that assertion in Applicant's October 2012 statement to him. (Tr. 23)

employee or witness A) and witness A's lack of understanding about the visibility of attachments in his computer calendar to staff employees, must be considered. The fact that a new policy was implemented in March 2012, restricting computer access to only government employees, must also be weighed. Applicant presented credible testimony and documentation demonstrating that her unauthorized use of technology systems is unlikely to recur. AG ¶ 41(a) applies.

Whole-Person Concept

I have examined the evidence under the disqualifying and mitigating conditions in my ultimate finding for Applicant under the guidelines for personal conduct, criminal conduct, and technology systems. I have also weighed the circumstances within the context of nine variables known as the whole-person concept. In evaluating the relevance of an individual's conduct, the administrative judge should consider the following factors:

> 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 the participation was 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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be a commonsense judgment based on careful consideration of the guidelines and the whole-person concept.

Applicant is 60 years old and has been married for 31 years. She has held a security clearance since 1977. She was honorably discharged in 2007 from the U.S.A.F. following 30 years of distinguished service. Her job performance as a contract employee has been good since her military discharge. She has earned a reputation for trustworthiness and good judgment by current and former contractor and government coworkers. Though it has taken some time for her to fully accept her misconduct, she realizes she did not have authority to do what she did because she did not have a need to know. I am confident Applicant will not abuse her authority in the future and will seek timely and sufficient authorization and advice before she acts. Having carefully evaluated the disqualifying evidence with the mitigating evidence in the context of the whole-person concept, Applicant has successfully mitigated the security concerns arising from the guidelines for personal conduct, criminal conduct, and use of information technology systems.

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 E):	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2 (Guideline J):	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3 (Information Technology Systems):	FOR APPLICANT
Paragraph 3.a:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

Paul J. Mason
Administrative Judge