DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-02899
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Tovah Minster, Esq., Department Counsel
For Applicant: Mark S. Zaid, Esq.

12/19/2017

Decision

HARVEY, Mark, Administrative Judge:

Applicant's use of an information technology system from another government agency (AGA)-1 after she began her AGA-2 employment was authorized.[1] She used the AGA-1 information technology system to benefit AGA-1. Use of information technology, handling protected information, and personal conduct concerns are mitigated. Eligibility for access to classified information is granted.

Statement of the Case

On April 14, 2015, Applicant completed and signed a Questionnaire for National Security Positions (SF 86) or security clearance application (SCA). Government Exhibit (GE) 1. On November 21, 2016, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued a statement of reasons (SOR) to Applicant under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry*, February 20, 1960; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), January 2, 1992; and the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, effective on September 1, 2006 (Sept. 1, 2006 AGs).

[1] The identities of AGA-1, her employer from 2008-2010, and AGA-2, her employer in 2010 after she left employment with AGA-1, are in the record. Tr. 61-62; AE A at 3. Both employers are non-DOD federal entities with sophisticated security systems.

The SOR detailed reasons why the DOD CAF did not find under the Directive that it is clearly consistent with the interests of national security to grant or continue a security clearance for Applicant, and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. Specifically, the SOR set forth security concerns arising under Guidelines M (use of information technology), K (handling protected information), and E (personal conduct). Hearing Exhibit (HE) 2.

On December 15, 2016, Applicant provided a response to the SOR and requested a hearing. HE 3. On February 8, 2017, Department Counsel was ready to proceed. On August 15, 2017, the case was assigned to me. On September 21, 2017, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing, setting the hearing for October 25, 2017. HE 1. Applicant's hearing was held as scheduled.

During the hearing, Department Counsel offered three exhibits; Applicant offered seven exhibits; there were no objections to any exhibits, except to parts of GE 3;[2] and all proffered exhibits were admitted into evidence. Tr. 13-29; GE 1-3; AE A-G. On November 2, 2017, DOHA received a copy of the hearing transcript.

[2] In response to DOHA interrogatories, Applicant provided a heavily redacted summary of an adjudication record from AGA-1. GE 3 at 11-17. Applicant objected to admissibility as a due process violation because it was incomplete and unfair. Tr. 15-18; GE 3 at 11-17. AGA-1 generated the document in 2011, and Applicant contended that she is prejudiced because she may be unable to remember the information summarized in the AGA-1 document. Tr. 25. Department Counsel responded that the source for the documents was Applicant, and she cited ISCR Case No. 10-08390 (App. Bd. Mar. 30, 2012) and ISCR Case No. 11-07509 (App. Bd. June 25, 2013), which discuss admissibility of redacted information and correspondence from AGA-1. In ISCR Case No. 10-08390, the cover letter conveying the documentation from AGA to DOHA states that:

> (1) the document was redacted "to delete classified information, extraneous and administrative data and other information excludable pursuant to applicable law or regulation;" (2) the exhibit is a true copy of the original maintained during the regular course of AGA business; (3) it was the regular course of business for AGA personnel with knowledge of the matters at hand to record or transmit to be recorded information to be included in the record; and (4) the record was made at or near the time of the matters at hand. The letter goes on to say that AGA would permit the Judge to examine unredacted copies to allow admission into the record of the redacted ones.

Id. at 3. The Appeal Board found the cover letter to be decisive in establishing the admissibility of the documents AGA provided. In ISCR Case No. 11-07509 (App. Bd. June 25, 2013) the Appeal Board admitted evidence from AGA that explained AGA's revocation of access to classified information stating "[o]fficial records or evidence compiled in the regular course of business are routinely admitted in DOHA hearings. Directive ¶ E3.1.20. *See* ISCR Case No. 04-12678 at 3-4 (App. Bd. May 7, 2007). As with public records admitted under Federal Rule of Evidence 803(8), official records are presumed to be reliable by virtue of the agency's duty of accuracy and the high probability that it has satisfied that duty. *See, e.g.*, *United States v. Carter*, 591 F.3d 656, 659 (D.C. Cir. 2010)." *Id*. at 5 n. 3. I overruled Applicant's objection, and the redactions go to the weight of the evidence. Tr. 26.

Applicant made a policy objection to the admissibility of the Office of Personnel Management (OPM) summary of Applicant's interview. Tr. 26-27. In response to DOHA interrogatories, Applicant reviewed the OPM summary and made several corrections and clarifications. She otherwise admitted the accuracy of the OPM summary. I overruled Applicant's objection. Tr. 27.

While this case was pending a decision, the Director of National Intelligence (DNI) issued Security Executive Agent Directive 4, establishing in Appendix A the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), which he made applicable to all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. The new AGs supersede the Sept. 1, 2006 AGs and are effective "for all covered individuals" on or after June 8, 2017. Accordingly, I have evaluated Applicant's security clearance eligibility under the new AGs.[3]

Findings of Fact[4]

Applicant's SOR alleges in SOR ¶ 1.a, "You intentionally accessed a government Information Technology system and viewed protected information without authorization from approximately 2008 through 2010." SOR ¶¶ 2.a and 3.a cross-allege SOR ¶ 1.a. In Applicant's SOR response, she denied the allegations in the SOR. HE 3. Additional findings of fact follow.

Applicant is a 55-year-old systems manager with expertise in "technical leadership, project management, systems integration, business process analysis and re-engineering, and business development." Tr. 71, 91; AE A at 1. She has 32 years of experience, mostly as a U.S. Government contractor. GE 1; GE 3 at 11. In 1983, Applicant received a bachelor's degree in business administration. Tr. 71, 92. In 1987, Applicant married, and her daughter is 23. Tr. 91; GE 1. Her husband is retired from his employment from AGA-1. Tr. 91. Applicant's employment from 2008-2010 involved AGA-1 and AGA-2. She has not served in the military. Tr. 92. Applicant has held a security clearance since 1994. Tr. 72, 88.

Use of Information Technology, Handling Protected Information, and Personal Conduct

Applicant's AGA-1 adjudication states:

> In SEP 2010, subject reported she printed information [ ] that was not related to her assigned work. Subject accessed [ ] classified [ ] information she did not have a need to know on two five occasions. Subject checked [ ] for famous people because she was curious [ ]. Subject said she should not have returned to [AGA-1] space or accessed their system since [ ] not [AGA-1] work. Subject knew what she did was wrong but did it out of curiosity.[5]

[3] Application of the AGs that were in effect as of the issuance of the SOR would not change my decision in this case. The new AGs are available at http://ogc.osd.mil/doha/5220-6_R20170608.pdf.

[4] Some details were excluded to protect Applicant's right to privacy. Specific information is available in the cited exhibits.

[5] The quoted information is from an adjudication summary from AGA-1. GE 3 at 11-12. Applicant received the summary in response to her request for information from AGA-1. Tr. 96-97. The brackets are

On February 17, 2011, AGA-1 officials revoked Applicant's access to classified information based on Guidelines K and M. GE 3 at 15-16.

Applicant's May 14, 2015, OPM PSI indicates during an AGA-1 pre-polygraph interview, she disclosed that she looked up information on an AGA-1 database to prepare for briefings.[6] Her reviews of the AGA-1 database were part of her employment responsibilities. In 2010, she reviewed AGA-1 material while working on an AGA-2 contract. She believed AGA-1 interpreted her uses of AGA-1's database as being for "curiosity," and alleged her uses of AGA-1's database were not related to her AGA-1 duties. Based on Guidelines K and M, AGA-1 revoked her security clearance. She said AGA-1's allegations were "baseless."

Applicant denied that she intentionally violated AGA-1's database access rules. Tr. 75. AGA-1's polygrapher did not understand Applicant's job responsibilities. Tr. 76. She said she told the polygrapher she accessed information about people who are infamous for their terrorism activities. Tr. 76-77. She accessed the information on high-profile terrorists because it was her responsibility to do so. Tr. 77. She did not access information about movie stars or political people. Tr. 93.

When Applicant was working for AGA-2, AGA-1 had extended her AGA-1 badge and clearances until AGA-2 had clearance approval. Tr. 78. AGA-1 had a sensitive compartmented information facility (SCIF) in the same location as her AGA-2 office. Tr. 78. AGA-1 and AGA-2 knew Applicant was continuing to access AGA-1's database. Tr. 78. She received communications from AGA-1 and AGA-2 during the same day. Tr. 79. She planned to do AGA-1 work when she was using AGA-1 space and AGA-2 work when she was using AGA-2 space. Tr. 80. She was unsure whether she had ever accessed the database on behalf of AGA-1 from her AGA-2 workspace. Tr. 85.

AGA-1 and AGA-2 use the same database. Tr. 93. The only way to access the database is to utilize AGA-1 provided equipment, network connection, and SCIF. Tr. 93. Applicant insisted that she was allowed to access the database on behalf of AGA-1 while she was working in an AGA-2 workspace. Tr. 85. Her AGA-1 and AGA-2 supervisors had agreed that she could work on behalf of AGA-1 and AGA-2 at the same time. Tr. 86.

Applicant told the polygrapher that she printed some personal items such as Mapquest directions or a recipe using an unclassified government computer and printer. Tr. 81-85. She wanted to be thorough and completely candid with the polygrapher. Tr. 82.

When Applicant submitted an appeal to the AGA-1's decision to revoke her security clearance, she did not seek advice from counsel or submit any supporting statements. Tr. 82. Her appeal consisted of an interview by an AGA-1 adjudicator. Tr. 88-89. She did not file a written appeal or make a written statement for her appeal. Tr. 94. Applicant promised to comply with all security regulations and requirements. Tr. 83.

---

in the original. There are no quotation marks indicating verbatim collection of Applicant's words in the summary.

[6] The information in this paragraph is from Applicant's May 14, 2015 Office of Personnel Management personal subject interview. GE 3 at 20.

Applicant's Supervisor on the AGA-1 Contract

Applicant's supervisor from 2007-2010 said Applicant was responsible for collecting information about non-United States residents for counter-terrorism purposes. Tr. 48-52. As part of her duties, Applicant had access to AGA-1's database. Tr. 53. Applicant was authorized to review any information in the database. Tr. 56. When a high-profile case implicating counter-terrorism would surface in the media, Applicant was supposed to check AGA-1's database for information on the case. Tr. 57. Applicant was responsible for assembling the information she collected and sending it to senior U.S. officials and other agencies. Tr. 57. Applicant was supposed to show initiative and be proactive about searching for and gathering information to address current issues, and officials in AGA-1's security may not have understood the scope of her responsibilities. Tr. 68. Applicant never accessed information when she did not have authorization or a need to know based on her duties and responsibilities. Tr. 58. AGA-1 security officials never consulted with Applicant's supervisor about the scope of Applicant's duties or otherwise. Tr. 69.

In 2010, Applicant's support responsibilities moved away from AGA-1 to AGA-2. Tr. 60. AGA-1 and AGA-2 shared the same database. Tr. 60-61. AGA-1 "wanted to continue to leverage her expertise on an ad hoc basis, until [the contractor] found the right replacement for her within that position because it was a pretty key position." Tr. 61. Applicant was supporting two different customers, AGA-1 and AGA-2. Tr. 61-62. AGA-1 authorized her continued access to the AGA-1 database; otherwise her access would have been removed. Tr. 62, 110. AGA-1 limited access to areas in which users had a need to know for their professional duties. Tr. 66-67. AGA-1 continued to hold Applicant's clearance. Tr. 111. Applicant was authorized to perform work for AGA-1 while using AGA-2 workspace. Tr. 109. For example, if Applicant received an email from AGA-1 while she was working in an AGA-2 workspace, she could reply to the email using AGA-2 workspace and computer systems because such collaboration is authorized. Tr. 109. Applicant worked on the same program for both AGA-1 and AGA-2. Tr. 109. The only time Applicant ever violated a security rule was on one occasion she self-reported herself for bringing her cell phone into a restricted area. Tr. 62, 87.

Applicant had limited access to unclassified computers in her work environment. Tr. 59-60. Employees were authorized to send and receive personal emails with attachments, subject to limitations relating to excessive use of paper or employee time. Tr. 59-60. Access to content such as pornography was prohibited. Tr. 59.

Character Evidence

Applicant has never received any disciplinary actions from her employer. Tr. 83-84. She has continued to receive security training to the present. Tr. 90. A coworker who has worked with Applicant since 2008 described her as careful about safeguarding classified information, diligent, professional, responsible, trustworthy, reliable, and honest. Tr. 32-45. Applicant's former supervisor described her as exceptionally careful about compliance with security rules. Tr. 63-64. She received excellent performance appraisals. Tr. 64. She is a valuable asset to national security. Tr. 70. She is trustworthy, honest, responsible, and reliable. Tr. 65, 69-70. Two former supervisors cited Applicant's

trustworthiness, integrity, and protection of classified information. AE F; AE G. Their statements support reinstatement of her security clearance. Tr. 32-66; AE F; AE G.

In 2004, an important government official wrote two letters lauding Applicant's skill, professionalism, leadership, competence, and "herculean effort requiring tremendous attention to detail" for her work on the terrorism database. AE E; AE F. Her "tremendous work ethnic, technical skill set, common sense, and excellent communications skills" made "a difference in the war on terrorism." AE E. In 2005, Applicant received a citation from her director. AE B. In 2010 and 2011, she received citations from AGA-1. AE C; AE D.

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

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

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. Thus, nothing in this decision should be construed to suggest that it is based, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. It is merely an indication the applicant has not met the strict guidelines the President, Secretary of Defense, and DNI have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of

establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Use of Information Technology

AG ¶ 39 articulates the security concern for use of information technology:

> Failure to comply 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 includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying including:

> (a) unauthorized entry into any information technology system;
>
> (b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;
>
> (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, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
>
> (e) unauthorized use of any information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized;

(g) negligence or lax security practices in handling information technology that persists despite counseling by management; and

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

SOR ¶ 1.a alleges, "You intentionally accessed a government Information Technology system and viewed protected information without authorization from approximately 2008 through 2010." I find the statements of Applicant and her supervisor to be credible. Applicant's access to the AGA-1 database and specific files within that database from 2008 through 2010, concerning high-profile foreign terrorists was authorized. The information she accessed was pursuant to her duties and not based on personal curiosity. She needed to know the information she obtained from AGA-1's database to respond to AGA-1's requests. She has met her burden, and she has refuted the allegation in SOR ¶ 1.a. The allegation made under the use of information technology guideline is not substantiated.

Handling Protected Information

AG ¶ 33 describes the security concern for handling protected information:

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.

AG ¶ 34 lists conditions that could raise a security concern and may be disqualifying including:

(a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;

(b) collecting or storing protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;

(d) inappropriate efforts to obtain or view protected information outside one's need to know;

(e) copying or modifying protected information in an unauthorized manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

(g) any failure to comply with rules for the protection of classified or sensitive information;

(h) negligence or lax security practices that persist despite counseling by management; and

(i) failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

SOR ¶ 2.a cross-alleges under the handling protected information guideline the same conduct alleged under the use of information technology guideline. As indicated in the previous section, Applicant's conduct with AGA-1's database was authorized. She needed to know about high-profile terrorists as part of her duties. She has refuted the disqualifying conditions in AG ¶ 34. Handling protected information security concerns are unsubstantiated.

Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern stating:

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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

AG ¶ 16 describes three conditions that could raise a security concern and may be disqualifying in this case:

(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 individual may not properly safeguard classified or sensitive information;

(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 individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of: (1) untrustworthy or unreliable behavior . . . ; (3) a pattern of . . . rule violations; and
>
> (e) personal conduct . . . that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes: (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

SOR ¶ 3.a cross-alleges under the personal conduct guideline the same conduct alleged under the use of information technology guideline. As indicated in the use of information technology section, Applicant's conduct with AGA-1's database was authorized. She needed to know about high-profile terrorists as part of her duties. She has refuted the disqualifying conditions in AG ¶ 16. Personal conduct security concerns are unsubstantiated.

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 circumstances. The administrative judge should consider the nine adjudicative process factors listed at 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.

Under AG ¶ 2(c), "[t]he ultimate determination" of whether to grant a security clearance "must be an overall commonsense judgment based upon careful consideration of the guidelines" and the whole-person concept. My comments under Guidelines M (use of information technology), K (handling protected information), and E (personal conduct) are incorporated in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines but some warrant additional comment.

Applicant is a 55-year-old systems manager with expertise in "technical leadership, project management, systems integration, business process analysis and re-engineering, and business development." GE 3 at 1. She has 32 years of experience, mostly as a U.S. Government contractor. In 1983, Applicant received a bachelor's degree in business administration.

The general sense of the statements of a coworker and three former supervisors is that Applicant is careful about safeguarding classified information, diligent, professional, responsible, trustworthy, reliable, and honest. Their statements support reinstatement of her security clearance. In 2004, an important government official wrote two letters lauding Applicant's skill, professionalism, leadership, competence, and "herculean effort requiring tremendous attention to detail" for her work on the terrorism database. AE E; AE F. Her "tremendous work ethnic, technical skill set, common sense, and excellent communications skills" made "a difference in the war on terrorism." AE E. In 2005, Applicant received a citation from her director. In 2010 and 2011, she received citations from AGA-1.

Applicant and her supervisor's statements about Applicant's authorization for continued access to the AGA-1 database and specific files within that database concerning high-profile foreign terrorists were credible. The information she accessed was pursuant to her duties and not based on personal curiosity. She needed to know the information she obtained from AGA-1's database to respond to AGA-1's requests. When AGA-1 revoked Applicant's security clearance in 2011, it was based on incomplete or incorrect information. The AGA-1 adjudicator did not understand Applicant's dual roles with AGA-1 and AGA-2. There is no evidence that AGA-1 checked with Applicant's supervisor or AGA-1's information technology or security officer about whether she was authorized continued access to AGA-1's database after becoming employed in support of AGA-2. AGA-1 has the reputation of being punctilious about access to their computers, databases, systems, and records. AGA-1 authorized Applicant's access to those entities and did not revoke them even though AGA-1 was aware she had moved to her employment in support of AGA-2. Applicant did not act inappropriately, and the allegations in SOR ¶¶ 1.a, 2.a, and 3.a are unsubstantiated.

I have carefully applied the law, as set forth in *Egan,* Exec. Or. 10865, and the AGs, to the facts and circumstances in the context of the whole person. Use of information technology, handling protected information, and personal conduct security concerns are refuted or unsubstantiated.

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 M:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline K:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraph 3.a:	For Applicant

Conclusion

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

_____
Mark Harvey
Administrative Judge