DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-10457
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esquire, Department Counsel
For Applicant: William F. Savarino, Esquire

January 25, 2012

Decision

METZ, John Grattan, Jr., Administrative Judge:

Based on the record in this case,[1] Applicant's clearance is granted.

On 16 June 2011, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline E, Personal Conduct.[2] Applicant timely answered the SOR, requesting a hearing. DOHA assigned the case to me 9 September 2011, and I convened a hearing 29 September 2011. DOHA received the transcript (Tr.) 9 October 2011.

[1]Consisting of the transcript (Tr.), Government exhibits (GE) 1-2, and Applicant exhibits (AE) A-B.

[2]DOHA acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the DoD on 1 September 2006.

Findings of Fact

Applicant admitted the SOR allegations, except for SOR 1.a. He is a 51-year-old senior systems engineer employed by a Government contractor since November 2002. He seeks reinstatement of the security clearance he has held largely without incident since 1986, except for a time from October 1999 to November 2002 when he was employed with a company that did not require him to hold a clearance (GE 1).

Applicant has been the subject of favorable background investigations in December 1985, April 1991, December 1998, and January 2003. Consequently, he has had both clearance and access as necessary until his clearances were suspended in January 2007 and ultimately revoked in February 2008. As that clearance involved special access, Applicant contested this action at a personal appearance in March 2009. The agency upheld its initial decision in August 2009 and Applicant did not appeal that action to the final decision authority.

In 2006, Applicant was employed as a contractor onsite at another Government agency (AGA). Applicant was a program manager for his company supervising a team of company employees working on a Government contract supporting AGA. There was another program manager for another company supervising a team of that company's employees working on another Government contract supporting AGA. Applicant and his fellow program manager reported to an AGA program manager.

In late 2006, AGA program manager announced at a program meeting that he was giving access to his Lotus Notes calendar to his secretary, Applicant, and his fellow program manager to better coordinate their efforts on AGA programs. Lotus Notes is a proprietary product of IBM Corporation. IBM heavily markets Lotus Notes for its "Calendar Delegation" feature—among other features.

The calendar delegation feature (AE B) allowed AGA program manager to delegate responsibility for his calendar and email to other groups or individuals. Only the account holder can change the settings necessary to delegate the calendar. There are a number of setting choices the account holder must make to enable the feature.[3] The record contains no information about what options AGA program manager intended to enable for his secretary, Applicant, and his fellow program manager. However, he enabled "All Mail . . ." to Applicant and at least gave access to "Read any document."

Applicant discovered this fact in about October 2006, when he noticed he could access AGA program manager's email. Initially, he was disconcerted by this discovery,

[3]The account holder must first decide how much mail to delegate. The options are "All Mail, Calendar, and To Do" or "Only Calendar and To Do." Once the account holder makes that choice, the account holder must decide how much access to give. There are different access options depending on the level of delegation chosen. "Only Calendar and To Do" has only two access options: read only or read, create, edit and delete. The "All Mail . . . " option has five access options, ranging from read only to variations of read, edit, create, delete documents or send email on behalf of the account holder.

but when he checked the access permissions and saw that both the secretary and his fellow program manager had the same access permissions, he figured that AGA program manager had intended him to have that access.

During the next few weeks, he read AGA program manager's emails to adjust his team's work priorities to match the concerns reflected in the email traffic. He saw nothing untoward in the access he had been given and did not discuss his access with AGA program manager, his subordinates, or his fellow program manager. His fellow program manager never mentioned to him that she had access to AGA program manager's emails.

Applicant used his access to AGA program manager's emails only for purposes of managing his program with AGA with two exceptions: He once looked at an "eyes only" email thinking that it might have something to do with his program. It did not, and he never opened another "eyes only" email. Once, his curiousness got the better of him and he looked at AGA program manager's leave and earnings statement (LES) to see how much he made.

One day in December 2006, Applicant noticed that AGA program manager's email account was generating a "read receipt" for those messages that Applicant had read—something that the program had not done before. That made Applicant think, for the first time, that maybe AGA program manager had not meant to give Applicant access to the emails. When he could not delete the "read receipts," probably because AGA program manager had only granted "read only" access, he went to AGA program manager and reported that he had been given access to AGA program manager's email. AGA program manager gave him a noncommital response.

The next day, Applicant was removed from his program manager position, and his clearances and access were suspended. He was polygraphed twice in June and July 2007 and his clearances and access were revoked by AGA in February 2008 because of the email incident as well as two other incidents characterized as security violations alleged in SOR 1.a and 1.b. Both those incidents had previously been addressed in earlier background investigations and polygraphs and found to have no security significance.

In July 1997 (SOR 1.a), Applicant was working at a different AGA. Part of his job was taking classified AGA documents and portion marking them, i.e. marking each paragraph of the document with its proper classification in accordance with recently-implemented classification rules. The documents had originally been classified under older rules which classified the entire document at the highest level of any one paragraph without portion marking. Applicant had never worked on this kind of project before and it was the first time he had ever worked in a Government facility as a contractor. He got his instructions from AGA program manager and did his best to apply those instructions as he declassified/reclassified the documents. The program security office eventually double-checked his work (Tr. 46). Nevertheless, he later had personal qualms about whether he had performed the work properly, which apparently surfaced

or resurfaced during the 2007 polygraphs. However, his Government supervisor at AGA at the time had no such reservations. He recalled "[Applicant's] fastidiousness in document handling and our intense effort in generating project classification guidelines." (GE 2) He reiterated the quality of Applicant's performance during that project (Tr. 25) as well as two other occasions when he and Applicant worked together on projects in 2003 and 2005.

In 2003-2004, Applicant was the Information Systems Security Officer (ISSO) for a program office at yet a third AGA. A routine part of his job was to travel off-site to perform system audits of the information systems at other Government contractors performing contract work for AGA, to ensure the systems were properly configured. The audits were performed using unclassified standards published by the Defense Information Security Agency (DISA) on the agency website.

Applicant worked in a special compartmented information facility (SCIF) at AGA. The SCIF contained an unclassified computer which was not connected to the classified computers in the SCIF. Applicant used the unclassified computer to download the unclassified DISA specifications onto unclassified discs that Applicant then took with him to the site audits. AGA security officer provided the discs Applicant used for the audits.

The security requirements for transporting the discs varied with the audit destination. If Applicant was taking the disc from his SCIF to another SCIF, he need only comply with the normal courier rules for transporting classified material. However, if he was taking the disc to a facility without a SCIF, he needed a specific authorization signed by AGA security officer to remove the disc from the SCIF. If the audit revealed that the facility had many issues to address to bring its information systems into compliance, Applicant would sometimes leave the disc at the facility.

Applicant believes that he followed the rules for getting the discs cleared for removal from the SCIF. He never had an issue with it at the job site. However, in later polygraphs, he could not always recall whether he always obtained the necessary authorization.

Applicant's many work and character references consider him honest and trustworthy (GE 2). Most appear to be aware of the email incident that was the immediate precipitant of Applicant losing his clearances and access. Applicant has apparently handled classified information without incident, except for a minor security violation in 1999, for which he received a reprimand in March 2004 during a review of his security file.

Policies

The adjudicative guidelines (AG) list factors for evaluating a person's suitability for access to classified information. Administrative judges must assess disqualifying and mitigating conditions under each issue fairly raised by the facts and situation presented.

Each decision must also reflect a fair, impartial, and commonsense consideration of the factors listed in AG ¶ 2(a). Any one disqualifying or mitigating condition is not, by itself, conclusive. However, specific adjudicative guidelines should be followed where a case can be measured against them, as they represent policy guidance governing access to classified information. Considering the SOR allegations and the evidence as a whole, the relevant adjudicative guideline is Guideline E (Personal Conduct).

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an applicant's security clearance. The Government must prove, by substantial evidence, controverted facts alleged in the SOR. If it does, the burden shifts to applicant to refute, extenuate, or mitigate the Government's case. Because no one has a right to a security clearance, the applicant bears a heavy burden of persuasion.

Persons with access to classified information enter into a fiduciary relationship with the Government based on trust and confidence. Therefore, the Government has a compelling interest in ensuring each applicant possesses the requisite judgement, reliability, and trustworthiness of those who must protect national interests as their own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the government.[4]

Analysis

The Government established a case for disqualification under Guideline E. The Government's characterizations in SOR 1.b, 1.c, and 1.d that Applicant admits are enough to raise security concerns.[5] However, I am not bound by those characterizations in making a decision, and I conclude that those characterizations are not reasonable based on a reading of the entire record.

The facts alleged in SOR 1.a and 1.b arguably constitute security violations, yet this case was not alleged as a security violation case under Guideline K. A reasonable reading of the facts surrounding both allegations reveals that Applicant did the job he was tasked by his AGA to do, did it with direct instructions of, and oversight by, the Government, and did it to the best of his ability. The Government found no real-time fault with his handling of protected information, and his handling of protected information passed evaluation in earlier polygraphs. Security rules do not require perfection in handling protected information, and the fact that Applicant later questioned himself about his handling of protected information, notwithstanding the fact that he was acting under Government direction, bespeaks at least as great, if not greater, commitment to

[4] *See*, *Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[5] ¶ 16.(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;

protecting classified information than an Applicant who blithely assumes that his conduct is unimpeachable simply because he was following the Government's instructions, or thought he was.

Regarding the allegations in SOR 1.c, I specifically give little weight to the facts or characterizations of AGA in revoking Applicant's clearances and access. While AGA is free to make its own conclusions, the fact remains that the agency decisional document is an advocacy document based, not on any irrefutable recording of Applicant's statements (i.e. sworn statement) but on a polygrapher's (if not others) distillation of what Applicant said, colored by his perception of what the polygraph charts meant. Put another way, not every twitch under a polygrapher's gaze reveals nefarious intent. But a polygrapher has no incentive to conclude benign intent, and a decisional document concluding nefarious intent requires no marshaling of facts consistent with benign intent.

We will never know what AGA program manager intended to enable when he told the staff meeting that he was giving access to his calendar to his secretary, Applicant, and Applicant's fellow program manager, because his statements do not appear in the record. We do not know why he did not act on Applicant's behalf over what was, at worst, his careless mistake in granting email access.[6] Similarly, we do not know what the fellow program manager knew about her access to AGA program manager's emails or what actions she took if/when she discovered that access. We do not know what action, if any, AGA took against the other program manager. We do know that only AGA program manager could authorize access, and given the steps necessary to grant access, whatever he intended, his granting email access to Applicant and his fellow program manager could not have been inadvertent. Based on the group that had been given access, Applicant was perfectly reasonable in assuming that he had been given access deliberately and he largely used that access consistent with the presumed intent for giving such access: to facilitate program management responsibilities for AGA program manager and his two subordinate program managers—the very functions touted by IBM for its Lotus Notes. The fact that Applicant tried to delete the "read receipts" when he suddenly realized that his access must have been a mistake, does little to change this analysis. It is all too easy to sharp-shoot Applicant's actions with 20-20 hindsight, and I will not do so here.

Finally, none of Applicant's conduct occurred more recently than five years ago. Aside from his concededly poor judgment in reading the "eyes only" email and looking at AGA program manager's LES, and his one security violation in 1999, Applicant has a decades-long track record of properly handling protected information. The allegations in SOR 1.a and 1.b ultimately raise no security concerns, and whatever security concerns are raised by the allegations in SOR 1.c are mitigated by the passage of time and Applicant's overall record of properly handling protected information. The allegations of SOR 1.d raise no independent security concerns for me to resolve. I resolve Guideline E for Applicant.

[6]Similarly, we do not know if that mistake was AGA program manager's own violation of agency security rules.

Formal Findings

Paragraph 1. Guideline E: FOR APPLICANT

Subparagraph a-d: For Applicant

Conclusion

Under the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance granted.

JOHN GRATTAN METZ, JR
Administrative Judge