DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 10-03999
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Caroline H. Jeffreys, Esquire, Department Counsel
For Applicant: Philip D. Cave, Esquire

April 13, 2011

Decision

HARVEY, Mark, Administrative Judge:

On May 27, 2009, Applicant violated information technology (IT) security protocols, when he went to a gaming-fan website using his Government-issued computer. His use of the gaming-fan website potentially exposed the Department of Defense (DoD) network to malware and viruses. He received additional training and expressed remorse. He learned from his mistake, and violations of IT security rules will not recur. Eligibility for access to classified information is granted.

Statement of the Case

On February 26, 2010, Applicant submitted an Electronic Questionnaires for Investigations Processing (e-QIP) version of a security clearance application (SF 86) (GE 1). On October 28, 2010, the Defense Office of Hearings and Appeals (DOHA) issued an SOR to Applicant, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended; and the adjudicative guidelines (AG) promulgated by the President on December 29, 2005.

The SOR alleged security concerns under Guidelines M (use of IT systems) and E (personal conduct). (Hearing Exhibit (HE) 2) The SOR detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant and recommended referral to an administrative judge to determine whether Applicant's clearance should be granted, continued, denied, or revoked. (HE 2)

On November 27, 2010, Applicant responded to the SOR. (HE 3) Applicant requested a hearing. (HE 3) On February 23, 2011, Department Counsel indicated she was ready to proceed on Applicant's case. On March 14, 2011, DOHA assigned Applicant's case to me. On March 14, 2011, DOHA issued a hearing notice. (HE 1) Applicant waived his right to 15 days notice of his hearing. (Tr. 10-11) On March 15, 2011, Applicant's hearing was held. At the hearing, Department Counsel offered nine exhibits (Tr. 14-15), and Applicant offered 18 exhibits (Tr. 16-24). (GE 1-9; AE A-R) There were no objections, and I admitted GE 1-9. (Tr. 15, 24-26) Additionally, I admitted the hearing notice, SOR, and Applicant's response to the SOR as hearing exhibits. (HE 1-3) On March 21, 2011, I received the transcript.

Findings of Fact[1]

In Applicant's response to the SOR, he admitted the three SOR allegations with explanations. (HE 3) His admissions are accepted as findings of fact.

Applicant is a 38-year-old employee of a defense contractor, who provides technical training for Air Force personnel.[2] (Tr. 33-35; GE 4) He joined the Navy in September 1996, and he served on active duty in the Navy until 2001. (Tr. 28-29) He continued his service in the Navy active reserve until 2003. (Tr. 29) He left the Navy inactive reserve in October 2008. (Tr. 50) His rating was electronic technician. (Tr. 28-29) He left active duty as an E-5. (Tr. 50) He has never married. In 2004, his son was born. In 2005, he received a bachelor's degree. (Tr. 32) He did not disclose any illegal drug use or alcohol-related offenses on his February 26, 2010 SF 86. He disclosed his conviction of disturbing the peace in 2007 and his violation of IT security rules, which resulted in his termination of employment. He held a top secret clearance from 1997 through most of his Navy service. (Tr. 31-32, 51)

[1]Some details have not been included in order to protect Applicant's right to privacy. Specific information is available in the cited exhibits.

[2]Unless stated otherwise, the source for the information in this paragraph is Applicant's February 26, 2010 SF 86. (GE 1)

Use of information technology (IT) systems and personal conduct[3]

In May 2009, Applicant received a gaming-website link from someone he met on the internet. He had not had an in-person meeting with the person who provided the gaming-website link, and could not describe a basis for believing the person was reliable and trustworthy. (Tr. 52) On May 27, 2009, he received a spam email at work that included the same gaming-website link.[4] (Tr. 36, 52-53) His home printer was broken, and he wanted to print some information from the gaming website at the office to improve his ability to play a computer game. (Tr. 36, 52; GE 9) During a break from his Government work and while in a Government building and using his Government-issued unclassified computer, Applicant clicked the link in the span email, which opened a link to the gaming website. (Tr. 54) At the gaming website, he opened a link to a window in a gaming-fan website. (Tr. 56; GE 9) He had no work-related reason to go to either website. He had some concern about what he was doing at the time he did it; however, his concern was insufficient to deter him from clicking the link to the gaming-fan website because he did not think harm or malware was present on the gaming-fan website and he did not believe his actions would damage the DoD network. (Tr. 56-57) Although he had never experienced a computer virus, he had no basis for believing the gaming-fan website should be trusted not to contain malware or a harmful virus. (Tr. 57)

Applicant was not specifically alerted that the gaming-fan website was a prohibited, blocked or particularly risky website to access. The DoD pop-up notice asking about whether a site is trusted did not appear. Applicant had no reason to believe the command-blocking software would be ineffective. He did not know clicking the link to the gaming-fan website would open a link to proxy server, and he did not intend to expose the DoD system to malware. (Tr. 55-56; GE 9 at 2) Applicant did not download any software or open any executable files from the gaming-fan website. (Tr. 38)

Because the gaming-fan website was an untrusted website, malware could have potentially entered Applicant's computer from the gaming-fan website link,[5] and then the malware could have entered the DoD network from Applicant's computer. As soon as the malware was detected, IT security blocked Applicant's computer access, and he contacted his supervisor and IT security. (Tr. 40) IT Security notified Applicant that

[3]The descriptions of Applicant's breach of information technology rules are consistent. (Tr. 36-58; GE 1 at 39, 41, 61, and 65-67; GE 2; GE 9; SOR response) The most thorough descriptions of this incident are Applicant's April 9, 2010 statement to an Office of Personnel Management (OPM) investigator and his hearing statement. (Tr. 36-58; GE 2)

[4]Later, Applicant learned the organization that sent the spam email is known for their creation of proxy servers. (Tr. 53) On May 27, 2009, Applicant did not know anything about the span organization, and he opened the email because the subject line was the gaming-website address. (Tr. 54)

[5]The incident report relating to Applicant's IT security breach indicates that after examination of the DoD network, "the good news is that the host computer (command) is not infected with any malware." (GE 3 at 4)

malware was traced to his computer. Security escorted Applicant out of the Government building. Applicant cooperated with the investigation of his breach of IT security.

Normally, command network security devices are effective in blocking untrusted websites. (GE 3 at 1) However, in this instance, when Applicant went to the gaming-fan website, he connected his Government computer to a "cutting-edge web anonymizer" or proxy server, which was designed to hide or "obfuscate" traffic from monitoring devices and avoid the blocking effects of DoD network security devices. (GE 3 at 1, 5) Applicant was not aware that that the gaming-fan website would cause a proxy server to avoid or evade the command's website's blocking software. (GE 9 at 1) Further investigation revealed that Applicant only went to one "fan site dedicated to a very old video game. Applicant printed some screen shots, and he did not download anything on to his Government computer." (GE 9 at 1) "The game is available for download at the site." (GE 3 at 5) The proxy is also a "malware delivery device" which caused the security software to detect the proxy. (GE 3 at 5)

On May 29, 2009, DoD added the gaming-fan website to the list of untrusted websites, which are blocked. (GE 3 at 1) DoD developed security measures to detect and block this type of proxy system. (Tr. 43) The proxy server "was used predominately to visit . . . a site dedicated to a decade old-video game. There appears to be nothing malicious about the website." (GE 3 at 2; GE 7 at 1) No malware actually received access to the DoD network. (Tr. 41-42) "The malware failed to execute against" the DoD network. (GE 3 at 5)

On June 20, 2008, Applicant digitally signed his organization's Computer User Agreement (CUA), which makes Applicant responsible for his use of his Government-issued computer and subjects him to administrative disciplinary action for failure to comply with his CUA. (GE 5; GE 6) His CUA authorizes him to use his Government-issued computer "for limited personal use" that conforms with DoD and local command policies. Such personal use must be of "reasonable duration and frequency, and whenever possible, is made during personal time (such as after-duty hours or lunch-time)." (GE 5 at 2 ¶ 9) His CUA does not restrict his access to any particular website.[6]

On July 29, 2009, Applicant's Senior Contracts Director, on behalf of his employer, wrote that Applicant has been "an exceptional employee" since April 2008 and concluded he did not have a malicious intent when he went to an untrusted website. (GE 4) Applicant received counseling on appropriate use of Government computers, and received ethics training. On December 14, 2009, he completed security education and refresher training, including IT security training. (Tr. 44, 48; GE 4; GE 7 at 2; AE R; SOR response) Initially, his employer placed him on probation for 180 days. (GE 4; GE 7 at 2; SOR response) Applicant "understands he made a huge mistake and is extremely upset with himself for his poor judgment." (Tr. 49-50; GE 4) He has educated himself about proxy servers and malware, and he promised his decision to access an

[6]After the hearing, I requested input from the parties concerning the federal Government's efforts to generate a list of trusted websites. Department Counsel objected to consideration of this information, and I sustained that objection. The pertinent emails and attachments are attached to the record. (HE 4)

untrusted website will never occur again. (GE 4; GE 9 at 2; SOR response) He would be reluctant to access websites unless he was absolutely sure they would be safe. (Tr. 58-59)

On August 10, 2009, the command's chief of staff and on August 17, 2009, the command's contracting officer permanently revoked Applicant's access to all command facilities.[7] (GE 6) On August 18, 2009, Applicant's employer terminated him from his employment because of his "improper use of government equipment" following the command's permanent termination of his access to Government facilities and network access. (GE 8; SOR ¶ 2.b)

Character evidence

Applicant submitted 17 character references, which supported reinstatement of his access to classified information. (AE A-Q) Some of his character references have known him for as long as 17 years. Others have more limited knowledge about his work performance and have known him for about 18 months. Several commissioned officers, contractor employees, systems engineers, a certified public account, and former Navy enlisted persons lauded his contributions to the Navy and his employer.

Applicant's character witnesses describe him as honest, hardworking, dependable, responsible, conscientious about compliance with rules, and dedicated to mission accomplishment. Several letters are particularly noteworthy. For example, a rear admiral, who commanded a submarine and served with Applicant on that submarine from July 1998 to March 2001, described his conduct as "always top notch," and Applicant never caused any doubt about his trustworthiness, reliability, or continued access to highly classified information. (AE B) A Navy commander, who served with Applicant aboard a submarine from July 1999 to August 2002, lauded Applicant's effectiveness, honesty, engaging personality, competence, value to mission accomplishment, and trustworthiness. (AE C) His character witnesses repeatedly emphasized their willingness to serve with Applicant in the future under dangerous and demanding circumstances because of his integrity and professionalism. (AE A-Q)

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

[7]The letters revoking access indicate Applicant signed an April 17, 2008 CUA. (GE 6) The CUA in the record was a form generated on June 19, 2008, which was digitally signed on June 20, 2008. (GE 5)

clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

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 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. 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. *See also* Executive Order 12968 (Aug. 2, 1995), § 3.1. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to applicant's allegiance, loyalty, or patriotism. It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense 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. 08-06605 at 3 (App. Bd. Feb. 4, 2010); ISCR Case No. 08-07290 at 2 (App. Bd. Nov. 17, 2009).

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). The DOHA Appeal Board may reverse the administrative judge's "decision to grant, deny, or revoke a security clearance if it is arbitrary, capricious, or contrary to law." ISCR Case No. 07-

16511 at 3 (App. Bd. Dec. 4, 2009) (citing Directive ¶¶ E3.1.32.3 and E3.1.33.3.).[8] The federal courts generally limit appeals to whether or not the agency complied with its own regulations.

Analysis

Upon consideration of all the facts in evidence, and after application of all appropriate legal precepts, factors, and conditions, I conclude the relevant security concerns are under Guidelines M (use of IT systems) and E (personal conduct).

Use of information technology (IT) systems

AG ¶ 39 articulates the security concern relating to use of IT systems problems:

> 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.

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

> (a) illegal or unauthorized entry into any information technology system or component thereof;
>
> (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology 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 information on or to any unauthorized software, hardware, or information technology system;
>
> (e) unauthorized use of a government or other information technology system;

[8]See ISCR Case No. 09-03773 at 7 n. 4-6 (A.J. Jan. 29, 2010)(discussing appellate standards of review).

(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;

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

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

AG ¶¶ 40(a) and 40(b) do not apply because Applicant did not engage in any "illegal or unauthorized entry into any information technology system or component thereof," or any "illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system." AG ¶¶ 40(c) and 40(d) do not apply because he did not use "any information technology system to gain unauthorized access to another system or to a compartmented area within the same system," and he did not download, store, or transmit any "classified information on or to any unauthorized software, hardware, or information technology system." AG ¶ 40(h) does not apply because there is no evidence of any "damage to the national security."

AG ¶¶ 40(e), 40(f), and 40(g) apply because IT security personnel did not authorize Applicant's access to the gaming-fan website using his Government-issued computer while connected to a DoD network. He did not have a basis for trusting the safety of the gaming-fan website, and thus, his use of gaming-fan website is prohibited by "rules, procedures, guidelines or regulations." (SOR ¶ 1.a) When he went to the gaming-fan website, malware and viruses had the opportunity to be either duplicated or to obtain entry to the DoD network. Applicant had previously received counseling about proper IT procedures and security. Nevertheless, he went to the gaming-fan website, which was a breach of security protocols. Further inquiry about potential applicability of mitigating conditions is required.

Three conditions under AG ¶ 41 are potentially applicable:

(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;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Applicant's conduct warrants full application of AG ¶ 41(a). The first phrase, "so much time has elapsed since the behavior happened," has limited application because his misuse of the Government IT system occurred on May 27, 2009, which is relatively recent. Applicant's access to the gaming-fan website "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." DoD employees will not access the gaming-fan website because DoD has blocked access using DoD networks. Applicant received a significant penalty for his poor decision, and he is an intelligent person who has learned from this mistake. He will be very careful in the future about accessing websites using his Government computer. He expressed sincere remorse. He has received additional training and has a much better understanding of the risks of viruses and malware. Applicant's conduct did not cause any damage to national security or the DoD network. I am convinced that Applicant is fully committed to complying with security requirements. His presentation of mitigation evidence fully mitigates use of IT systems security concerns under Guideline M. However, assuming Guideline M mitigating conditions are insufficient to fully mitigate Guideline M security concerns, security concerns are separately mitigated under the whole-person concept, *infra*.

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 information."

Four personal conduct disqualifying conditions under AG ¶ 16 are potentially applicable. Those four disqualifying conditions provide:

> (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;
>
> (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: . . . (2) disruptive, violent, or other inappropriate behavior in the workplace; and (3) a pattern of dishonesty or rule violations.

(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. . . ; and

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

On May 27, 2009, Applicant's accessed a gaming-fan website using his Government-issued computer, while connected to a DoD network and violated a rule. He also violated his CUA, which required him to comply with command policies. This rule violation shows "questionable judgment, untrustworthiness and unreliability" and demonstrates that Applicant on that occasion did "not properly safeguard protected information." Violation of command IT security policies adversely affected Applicant's personal, professional, and community standing. AG ¶¶ 16(c), 16(d), 16(e)(1), and 16(f) apply and further analysis concerning applicability of mitigating conditions is required.

Three mitigating conditions under AG ¶ 17 are potentially applicable:

(c) the offense is 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;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the 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.

Any security concerns raised are mitigated under AG ¶¶ 17(c), 17(d), and 17(e). Applicant's May 27, 2009, accessing of a gaming-fan website using his Government-issued computer, while connected to a DoD network, was a serious rule and CUA violation. On that single occasion, he showed "questionable judgment, untrustworthiness and unreliability." His behavior (accessing an untrusted website) was infrequent, and it happened under unique circumstances. I am confident from Applicant's sincere statement of remorse, his remedial training, and the negative consequences he suffered ensure that he will not make the same or similar mistake. He fully cooperated with the IT security investigation from the beginning and fully acknowledged his improper behavior. Even though violation of command IT security policies adversely affected his personal, professional, and community standing, his disclosure eliminated any vulnerability to exploitation, manipulation, or duress. I am convinced that Applicant is fully committed to complying with security requirements. Personal conduct concerns under Guideline E are fully mitigated. However, assuming Guideline E mitigating conditions are insufficient to fully mitigate Guideline E security

concerns, security concerns are separately mitigated under the whole-person concept, *infra*.

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(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.

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. AG ¶ 2(c). I have incorporated my comments under Guidelines M and E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

The whole-person factors against reinstatement of Applicant's clearance are significant; however, they do not warrant revocation of his security clearance. Applicant's May 27, 2009, accessing of a gaming-fan website using his Government-issued computer, while connected to a DoD network, was a serious rule and CUA violation. He knew that accessing a gaming-fan website was risky behavior because such a website was untrusted. Accessing this gaming-fan website likely had a greater risk of accessing viruses and malware than going to well-known newspaper, corporate, legal, technical, and other non-Government sites, which are generally known to be trustworthy. His misuse of his Government-issued computer was imprudent, irresponsible, and improper. On that single occasion, he showed questionable judgment, untrustworthiness and unreliability.

The rationale for reinstating Applicant's clearance is more substantial. He was forthright and candid in his IT security interview, his OPM interview, his SOR response, and at his hearing about his accessing the gaming-fan website.[9] Applicant is a 38-year-old technical trainer, who provides services to the Air Force. He has achieved some important educational and employment goals, demonstrating his self-discipline, responsibility and dedication. He earned a bachelor's degree in 2005. He served successfully on active duty in the Navy, rising to the grade of E-5. He served in the

[9]ISCR Case No. 05-03554 at 4-6 (App. Bd. Aug. 23, 2007) (discussing factors an administrative judge should consider when making credibility determinations including consistency of statements).

Navy from September 1996 until 2003 on active duty or in the active reserves. His rate was electronic technician.

Applicant is an intelligent person, and he understands that his accessing the gaming-fan website was improper. He does not have a sophisticated knowledge of computers and was not fully aware of the risks to DoD networks from using Government computers to access untrusted websites. His intent when he accessed the gaming-fan website was not to damage the DoD network or to use a proxy server to avoid IT security detection. His intent was to access information about a 10-year-old computer game, and to print screen shots to assist his game-playing techniques. His actions did not cause malware or a virus to damage the DoD network. He received remedial IT security training, and he has educated himself about the perils of going to untrusted websites. He understands the security and network problems resulting from proxy servers, viruses, and malware. He acknowledges that he showed poor judgment, and he deeply regrets his bad decision. He is sincerely remorseful, and promise such poor judgment will not recur. He has held a top secret security clearance from 1997 through most of his Navy service without any other non-SOR security-related allegations of misconduct. Applicant's 17-character references emphasize his integrity, honesty, trustworthiness, and reliability. His character references included an active duty Navy rear admiral and Navy commander as well as several professional engineers, who served in close proximity to him. They have personal knowledge and the judgment necessary to accurately assess Applicant's character, integrity, trustworthiness, and reliability. He has demonstrated his loyalty, patriotism, and trustworthiness through his service to the Navy and to the DoD as a contractor. He is an asset to his employer. His security clearance application does not list any reportable incidents involving illegal drugs or alcohol. There is no non-SOR derogatory information about his financial history or abuse of IT systems.

I have carefully applied the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), Exec. Or. 10865, the Directive, and the AGs, to the facts and circumstances in the context of the whole person. I conclude use of information technology systems and personal conduct security concerns are fully mitigated, and he is eligible for access to classified information.

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 E:	FOR APPLICANT
Subparagraphs 2.a and 2.b:	For Applicant

Conclusion

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

_____

MARK HARVEY
Administrative Judge