DATE: November 28, 2007

In re:	)	
	)	
----------	)	ISCR Case No. 07-01509
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

DECISION OF ADMINISTRATIVE JUDGE
ROGER C. WESLEY

APPEARANCES

FOR GOVERNMENT
Julie R. Edmunds, Department Counsel

FOR APPLICANT
Chester (Skip) Morgan, II, Esq.

SYNOPSIS

Applicant has a history of demonstrated judgment lapses associated with his use of classified computer systems and related software in his work and in his use of accessing adult pornographic materials and engaging in sex-related conduct in public areas. Applicant's collective actions resulted in the denial of his requested access to sensitive comparted information (SCI). Similar conclusions are warranted here under the personal conduct guideline based on Applicant's demonstrated pattern of poor judgment in a number of areas and circumstances. Applicant's collective actions represent overall poor judgment that is for the most part still too recent to mitigate. Only Applicant's past access of adult pornographic material on his office computer and his related engaging in sexual misconduct is sufficiently isolated and dated to be successfully mitigated. Clearance is denied.

STATEMENT OF THE CASE

On June 7, 2007, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to Applicant, which 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 clearance should be granted, continued, denied or revoked.

Applicant responded to the SOR on June 29, 2007, and requested a hearing. The case was assigned to me on August 3, 2007, and was scheduled for hearing on September 11, 2007. A hearing was held on September 11, 2007, for the purpose of considering whether it would be clearly consistent with the national interest to grant, continue, deny, or revoke Applicant's security clearance. At hearing, the Government's case consisted of seven exhibits; Applicant relied on two witnesses (including himself) and three exhibits. The transcript (R.T.) was received on September 19, 2007.

PROCEDURAL ISSUES

Before the close of the hearing, Applicant requested the record by kept open to afford him the opportunity to supplement the record with documented proof of the curriculum materials he was provided at a parenting course he attended 2004 following his NSA interviews. There being no objection from the Government, and good cause being demonstrated, Applicant was granted seven days to supplement the record. The Government was afforded three days to respond. Within the time permitted, Applicant provided documentation of the curriculum materials provided him in his parenting course. The submission was admitted as exhibit D.

SUMMARY OF PLEADINGS

Under Guideline E, Applicant is alleged to have been denied eligibility to access secret compartmented information (SC) by another government agency in May 2004 based on information that he (1) modified a line of programming on a classified computer (between 2001 and 2003) as a prank so that a co-worker's computer would beep at start-up; (2) accessed a classified computer network at a U.S. government facility abroad on three separate occasions without authorization; (3) accessed a U.S. government facility's e-mails from the account of a co-worker (not logged off at the time) while working at a facility abroad; (4) inadvertently carried classified computer disks in his briefcase in either 1992 or 1993 from one classified facility to another; (5) viewed adult pornography on his office computer and masturbated in his office and in the company restroom, for two hours a day on average between 1995 and 1996; masturbated while driving his vehicle to and from work three times a year prior to about May 2003; (6) used a chastisement device to discipline his children between 1997 and 2004 that left bruises on his children's legs; and (7) continued working on a secure security system after being notified in October 2003 that he was no longer authorized to access this system.

For his answer to the SOR, Applicant admitted to modifying a line of programming on a classified computer system, but denied any exercise of questionable judgment. Applicant admitted

sending one or two e-mails from the account of a co-worker while working at a U.S. facility abroad. Applicant also admitted to working on a computer system without authorization in 2003, but only on few occasions. Applicant denied the remaining allegations: some *en totale*, and others in part, and added explanations.

FINDINGS OF FACT

Applicant is a 43-year-old software developer who seeks a security clearance. The allegations covered in the SOR and admitted by Applicant are incorporated herein by reference and adopted as relevant and material findings. Additional findings follow.

While employed as a contractor for another agency (NSA) between 2001 and 2003, Applicant was twice granted conditional certification of access (CCA) in 2003 to access SCI. He was first granted access in March 2003 and then debriefed after his employer withdrew his sponsorship in June 2003 (*see* ex. 3). Following his employment by a new employer in July 2003 (O corporation), this employer successfully sponsored him for CCA. His CCA was rescinded, though, in February 2004 when he was unable to successfully complete his security processing.

Applicant was interviewed by an NSA investigator in October 2003 as a part of the agency's background investigation to determine his suitability to access SCI (ex. 4). During this interview, he disclosed computer-related information that NSA interpreted to entail security violations, sexual misbehavior, and abusive child disciplining (*see* exs. 4 and 5).

In or about 1992 or 1993, Applicant inadvertently carried classified unused computer disks in his briefcase from one classified facility to another on multiple occasions. According to Applicant, these disks had never been used in a classified system: "They were just blank floppy disks," according to Applicant (R.T., at 38). However, Applicant did not expressly retract his statements given to an NSA investigator in October 2003 when asked about the disks by Department Counsel (R.T., at 72-75). In this interview, Applicant, acknowledged, carrying secret level computer disks in his briefcase from one DoD secret facility to another, discovering them on his return to the facility's unclassified location, and then taking steps to ensure the disks were properly secured in the proper classified facility by the close of business (*see* ex. 4). With the clarification that the disks in question were unused blank floppy disks, Applicant's statements made to the NSA investigator in October 2003 about these disks are accepted and incorporated anew.

While working for at a U.S. Government facility in Australia (between 1997 and 2001), Applicant remotely logged into a classified TS/SCI level network in Great Britain in an effort to resolve software problems, or other errors he was experiencing with the network in Australia (*see* exs. 3 and 4). After successfully logging in, he accessed the director of systems logs and proceeded to analyze the logs. He recollected taking these actions on three separate occasions during this 1997-2001 time period without obtaining authorization (R.T., at 71). He subsequently acknowledged this was likely incorrect action, since he was not authorized. Applicant assured that he never attempted to "crack" passwords on another user's system. Nor was it necessary to surreptitiously enter the other user's system, inasmuch, as he had not logged off of his system or engaged his screen saver during Applicant's interventions.

During his period of employment in Australia, Applicant also recollects sending one or two e-mails from the account of a co-worker who had not yet logged off her own computer. Applicant ensures he meant no harm by his intrusive actions and only intended the activity as a prank (*see* exs. 3 and 4).

While working for a prior defense contractor for a period in 2001, Applicant encountered a specific office need for system administrator access to modify a line of programming on a classified network (*see* exs. 3 and 7). On this particular occasion during this 2001 time frame, Applicant used his own system administrator privileges to gain access to a female co-worker's system profile. The modification caused his coworker's computer to beep at start-up; it was intended as a prank, and apparently did not cause any disruption in the network (*see* ex. 4; R.T., at 62-63). Applicant acknowledged, though, that "he was not supposed to access other people's e-mail" (R.T., at 72).

Following his employment as a NSA contractor in September 2003, Applicant began working in NSA facilities (*see* ex. 5). Shortly after his start-up with NSA, he was given root access passwords to the secure computer system in his office to facilitate his performing his assigned system administrator duties. Unbeknownst to him at the time, his supervisors had submitted his name for privileged access to classified information (PRIVAC). In October 2003, he was notified that he was denied PRIVAC and could no longer work on classified systems. After being told he did not have PRIVAC and couldn't administer classified systems without it, he continued performing his system administrator duties without supervision three times a week (*see* ex. 5; R.T., at 64-65, 86-87). Two months later (in December 2003), Applicant discontinued his unsupervised access to his classified computer system. By this time he had been notified of a scheduled second interview and polygraph examination with NSA and knew that gaining access to NSA's classified computer system without PRIVAC was against NSA policy. Knowing that he would likely be asked about his continued working on the classified computer without PRIVAC would likely be explored in the scheduled interview and polygraph, he ceased his unauthorized access (*see* ex. 5; R.T., at 88).

Over a two-year period between 1995 and 1996, Applicant viewed adult pornography on his unclassified office computer, in addition to masturbating in his office three to ten times and in the company restroom on three to ten occasions (never completely shielded from potential public observation). He estimates that on average he viewed pornography in his office computer for two hours per work day, and at times, as much as four hours per workday (*see* exs. 3 and 4; R.T., at 76-80). It is not clear whether there were specific guidelines in place with his employer at the time that proscribed deliberate accessing of pornography on an office computer (*compare* exs. 3 and 7). Nonetheless, the NSA's SCI findings reflect drawn inferences that it was at the very least a disfavored company practice. During this same contemporaneous period, and for a number of years thereafter, he occasionally masturbated while driving his vehicle to and from work. His last reported act of masturbation while driving was in May 2003 (exs. 3 and 4; R.T., at 79). Applicant insists he never had any fear of detection or repercussions at work over the conduct (R.T., at 81).

For over seven years spanning 1997 and 2004, Applicant used a 12-inch cloth-covered ruler known as a "chastisement device" (a device designed to change a child's behavior by means of administering corporal punishment) to discipline his children. He was introduced to this practice through a course that consisted of meeting with other couples, exchanging ideas, and watching two videos on child rearing that were produced by an identified Christian organization (*see* ex. A; R.T., at 50-51). He purchased the chastisement device from his course hosts (R.T., at 52). When first

interviewed by NSA in October 2003, he described his chastisement practice in which a child is "swatted a number of times equivalent to their age plus an additional one to two times" (ex. 4). Describing his practice as one that is done "effectively and lovingly," he acknowledged that he "swatted his daughter too many times and two hard," which resulted in bruises on his daughter's leg (ex. 4). He admitted to causing bruises on his daughter's legs once or twice, while making every effort to avoid applying the chastisement device on his children's bare posterior. Applicant also acknowledged his use of the chastisement device on his younger son once daily, which he attributed to his son's need for daily disciplining (*see* ex. 4).

In a second interview with NASA (in January 2004), Applicant elaborated some on his use of the chastisement device. He traced his initiation of chastising his children to very early ages and classified his use frequency of the device on his children as "regular" (s*ee* ex. 5). He acknowledged for the first time to unintentionally leaving bruises on the backs of his children on a few occasions (possibly once a year) when the disciplined child moved during his striking action. He stated in this interview that he last left a bruise on his youngest son in 2003 (*see* ex. 5). Applicant indicated he had never been questioned by authorities over the manner in which he disciplined his children and believed his actions were not excessive.

Applicant spoke in greater depth and detail about his chastising of his children in his third and last interview with NSA in March 2004 (*see* ex. 6). In this interview, he confirmed his chastising his four-year old daughter two to three times per week for "pushing her six-year brother's buttons" (ex. 6). He reaffirmed his chastising his younger son on a daily basis between 2000 and early 2004, and thereafter three to four times a week for bullying his four-year-old sister and lying (an automatic reason for chastising). He indicated that his chastising of his other two daughters varied: from no chastising for the past year with his nine-year old daughter to once a month chastising of his oldest daughter for exhibiting a bad attitude and "saying mean things" to her siblings (ex. 6). Applicant repeated his leaving inadvertent bruises on his children once a year between the years 1997 and 2004 and to occasionally striking the backs of their legs when any of the children moved while he was administering the chastise device. At hearing, he insisted he had no intention to bruise or harm his children with his chastising actions.

After talking with co-workers following his March 2004 NSA interview, Applicant enrolled in a parenting course in April 2004 (*see* exs. 7 and D; R.T., at 59). This class was administered by a state department of social services, was entitled "Dads works" (ex. 7), and involved weekly sessions with fathers seeking to learn about parenting skills (R.T., at 59). From this parenting course, he gained fresh tools and ideas for non-physical punishment of his children and, thereafter threw the chastise device away. Since taking his parenting course, Applicant insists he has not used a chastisement device to discipline his children (R.T., at 59-60).

Based on all of the information compiled from NSA interviews covering Applicant's security-related activities and his personal practices involving his personal behavior over a 12-year period, NSA denied Applicant access to SCI in May 2004 (ex. 3). After weighing all of the available information necessary to make an informed whole person assessment, NSA determined that Applicant did not meet the DCID 6/4 standards for access to NSA/CSS SCI (*see* ex. 3). Applicant elected not to appeal NSA's eligibility denial for SCI access (R.T., at 88).

Applicant was interviewed by OPM in December 2006 in connection with his application for a collateral clearance (*see* ex. 7). The interview covered the same areas of inquiry developed by NSA during its SCI investigation, and entailed considerable qualifications and minimizing of the actions he acknowledged in previous NSA interviews. For instance, when he was asked about his continued use of a classified computer system without oversight in 2003 after being advised he did not have PRIVAC, he indicated he did so only after he could not find a team member with PRIVAC, and used the computer system for the limited purpose of repairing system errors. Asked to address his prior chastising of his children in this OPM interview (s*ee* ex. 7), he retreated on his previous acknowledgments made to NSA interviewers. In this interview, he assured that he did not use the chastise device often and always applied it over the child's clothes, "never against bare skin" (ex. 7). Further, he indicated "the children were not bruised due to the use of the chastise belt" (*see* ex. 7). Applicant indicated he did not enjoy disciplining his children with "the chastise belt" (ex. 7).

Asked at hearing about bruising his children with his chastisement device, Applicant did recall one possible inadvertent experience with his younger son (R.T., at 56-57), but otherwise denied ever inflicting any bruises on his children from his chastising. Applicant did admit to one instance of intentionally striking his youngest daughter on her bare skin while she was bathing (R.T., at 57).

In his 2006 OPM interview, the OPM investigator also explored Applicant's previously acknowledged viewing of adult pornographic material on his office computer. For the first time he recounted a cause and effect association between his viewing of pornographic material and his withdrawing to his employer's restroom to masturbate (*see* ex. 7). At the same time, he trimmed his previously admitted admissions of masturbating while driving: in this interview; in this interview, he admitted to just one instance of masturbating while driving (ex. 7).

Applicant's FSO and project manager together credit Applicant with avoiding any security violations and incidents between August 2004 and April 2007 (*see* exs. B and C). Applicant is well regarded by a coworker familiar with him. This coworker describes Applicant as honest and trustworthy and one who possesses a high sensitivity to guilt (R.T., at 26-27).

POLICIES

The revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (effective September 2006) list Guidelines to be considered by judges in the decision making process covering DOHA cases. These Guidelines require the judge to consider all of the "Conditions that could raise a security concern and may be disqualifying" (Disqualifying Conditions), if any, and all of the "Mitigating Conditions," if any, before deciding whether or not a security clearance should be granted, continued or denied. The Guidelines do not require the judge to assess these factors exclusively in arriving at a decision. In addition to the relevant Adjudicative Guidelines, judges must take into account the pertinent considerations for assessing extenuation and mitigation set forth in E.2.2 of the Adjudicative Process of Enclosure 2 of the Directive, which are intended to assist the judges in reaching a fair and impartial common sense decision.

Viewing the issues raised and evidence as a whole, the following adjudication policy factors are pertinent herein:

Personal Conduct

The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, 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.

Burden of Proof

By virtue of the precepts framed by the revised Adjudicative Guidelines, a decision to grant or continue an applicant's security clearance may be made only upon a threshold finding that to do so is clearly consistent with the national interest. Because the Directive requires Administrative Judges to make a common sense appraisal of the evidence accumulated in the record, the ultimate determination of an applicant's eligibility for a security clearance depends, in large part, on the relevance and materiality of that evidence. As with all adversary proceedings, the Judge may draw only those inferences which have a reasonable and logical basis from the evidence of record. Conversely, the Judge cannot draw factual inferences that are grounded on speculation or conjecture.

The Government's initial burden is twofold: (1) It must prove any controverted fact[s] alleged in the Statement of Reasons and (2) it must demonstrate that the facts proven have a material bearing to the applicant's eligibility to obtain or maintain a security clearance. The required showing of material bearing, however, does not require the Government to affirmatively demonstrate that the applicant has actually mishandled or abused classified information before it can deny or revoke a security clearance. Rather, consideration must take account of cognizable risks that an applicant may deliberately or inadvertently fail to safeguard classified information.

Once the Government meets its initial burden of proof of establishing admitted or controverted facts, the burden of persuasion shifts to the applicant for the purpose of establishing his or her security worthiness through evidence of refutation, extenuation or mitigation of the Government's case.

CONCLUSIONS

Appellant comes to these proceedings as a software developer who acknowledged security-related actions over a 10-year period that were neither authorized nor incidents that could be fairly determined to fall within his established parameters of responsible authority. While none of these specific actions admitted to in NSA interviews associated with his 2003 SCI application were ever investigated and found to reflect security violations meriting disciplinary actions, the cumulative effect of these repeated actions over an extensive period of time raise security issues. Although none of Applicant's cited irregularities with his computer or classified disks carried in his briefcase involved stored classified information, his actions certainly raised questions about his judgment, reliability and trustworthiness required for eligibility to access classified information.

Recurrent failures to adhere to established security procedures

Under the Directive's security violation guidelines in force, persons responsible for safeguarding classified information in their custody and control are required to adhere to established procedural requirements for operating classified computer systems and safeguarding classified disks, and to avoid actions that might place classified information under their custody and control at risk to compromise. Applicant's continued access to a classified computer system with the knowledge of being denied PRIVAC and his deliberate mishandling of his classified computer systems under his control (even for prank reasons) violated the procedural requirements of paragraph 5-100 of the NISPOM for accessing classified network systems without authorization. His actions warrant one of the disqualifying conditions (DC) of the Adjudicative Guidelines for personal conduct: DC 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*).

The importance of demonstrating sound judgment and willingness to comply with established rules and guidelines regarding the administering of classified equipment and safeguarding classified computer hardware and software cannot be overemphasized. Protecting the nation's security interests against the risks of foreign coercion and intimidation remains a core governmental responsibility that finds roots in our earliest Constitutional history and enjoys the sustaining force of the courts. *Cf. United States v. Curtiss-Wright Corp.,* 299 U.S. 304, 319-20 (1936). Applicant's continued accessing of a classified computer system after being advised he did not have PRIVAC, his failures to utilize his employer's trusted authorization procedures for accessing other computer systems, his misuse of a classified computer to cause a beep on a co-worker's computer start-up, and his carrying classified disks (even empty ones) to and from classified facilities in his briefcase over an extended time period increased the security risks for potential compromise of classified information. His actions, as such, reflect adversely on his judgment and trustworthiness for accessing classified information.

In appraising the security significance of Applicant's history of misuse of classified computer systems and software (*i.e.*, the empty classified disks), some deliberate and some inadvertent, careful consideration was given to Applicant's full and open disclosure of his actions in the NSA interviews that preceded his denial of SCI access in 2004. While all of the developed information was based on Applicant's open disclosures to NSA interviewers, and not from any other developed sources, the information does reflect judgment lapses by an experienced software developer that are security significant. While Applicant has since minimized some of the events he recounted to NSA interviewers, the findings made in NSA's 2004 decision covering Applicant's application to access SCI is well supported by information furnished by Applicant in a series of NSA interviews and was never appealed by Applicant. Despite his efforts to further explain and to some extent minimize the events covered in NSA's 2004 decision, the findings are credibly based and are sustained.

Because the developed infractions of company procedures governing the administering of classified computer systems and software are derived from the guideline governing personal conduct, and not the guideline covering security violations, these infractions must be assessed against the backdrop of both the mitigating conditions of the new Adjudicative Guidelines and a whole person assessment. While a number of years have passed since the last reported infraction (in 2003), the actions themselves cannot be considered minor, infrequent, or aged, when considered as a whole,

and not in piecemeal. To be sure, any of these actions considered alone or in isolation could likely be mitigated, especially given his more recent clean record. It is their confluence that creates current security concerns over Applicant's demonstrated judgment. Given the circumstances in which these incidents were elicited (*viz.,* against the backdrop of a scheduled polygraph) and the absence of documented counseling and/or specific restorative initiatives (such as additional briefings on procedures for administering classified systems) to ensure his avoidance of recurrent incidents in the future, potential mitigation conditions under the personal conduct guideline are not available to Applicant. Without the benefit of applicable mitigating conditions to the covered conduct, successful mitigation is more difficult to demonstrate herein under the Guideline E guideline.

Evaluating Applicant's actions from a whole person perspective does not warrant any more favorable conclusions either. Even with credit accorded for his completing security training and avoiding any adverse incidents over the past three plus years, the covered incidents are too numerous and serious when considered together to warrant the application of any of the mitigating conditions of Guideline E in this proceeding. Collectively, these covered classified computer and software-related actions reflect a security significant pattern of judgment lapses that is too extensive and recent to be mitigated at this time under any of the cited mitigation conditions under the personal conduct guideline.

Applicant's other covered conduct

Pattern misconduct attributable to Applicant also includes his regular viewing of adult pornography on his office computer during a two-year period spanning 1995 and 1996 and his engaging in masturbation in his office, in the company's restroom, and while driving during this same contemporaneous period, and thereafter when driving his car (*i.e.,* to May 2003). Applicant's regular disciplining of his four young children through the corporal application of a chastisement device to their posteriors, and occasionally to their exposed legs and backs, over the course of seven years spanning 1997 and 2004, was confirmed by NSA in its 2004 SCI access decision and was never challenged by Applicant. Applicant's acknowledged sexual misconduct and harsh treatment of his children (some of which resulted in bruises and red marks on his children), reflect poorly on his respect for his office rules and internal guidelines and his children's well being and represent still additional examples of demonstrated poor judgment.

Aside from the physical bruises and red marks occasionally inflicted on his children, regular application of pain producing blunt instruments on children so young risks damaging their fragile esteem systems during their early development and exposes these children to potentially irreversible developmental deficits. It is not at all clear that Applicant considered these risks before settling on the discipline practice he chose after viewing a child rearing video with his hosts. His regular use of a chastisement device on his children in the way he recounted on multiple occasions to NSA investigators does cast reasonable doubt on his judgment and trustworthiness and his overall ability to demonstrate his current eligibility to access classified information.

Like his computer-related conduct, Applicant's pornography and sexual based actions are not based on any specific guideline tailored to the specific conduct, but rather on the personal conduct guideline that covers acts indicative of poor judgment and unreliability. Specifically, this conduct is covered by DC 16(c) of the Adjudication Guidelines for personal conduct. Whether Applicant's collective actions can be mitigated due to age, infrequency, and/or unique circumstances

that are unlikely to recur cannot be resolved solely based solely on the application of any of the mitigating conditions**.**

Both Applicant's disciplining practices and his less recent accessing of pornography on his office computer and engaging in masturbating in public areas over a prolonged period preclude the application of the conjunctive provisions of MC 17(c) (*the offense is so minor, or so much time has passed, 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*) of the guidelines for personal conduct. Based on the counseling he initiated to reassess his disciplining of his children, he may take very limited application of two of the other mitigating conditions: specifically, MC 17(d) (*the individual has acknowledged the behavior and obtained counseling to change the behavior or taken 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 MC 17(e) (*the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress*). Applicant's counseling efforts and corrective steps he has taken in disciplining his children, while encouraging, are still too recent and uncertain, however, to accord considerable weight.

Recognizing that security clearance evaluations do not represent an exact science, some whole person assessments are necessary to supplement the specific requirements of the relevant mitigating conditions of the personal conduct guideline. Applicant's accessing of pornography and related masturbation in public areas (inclusive of his office and while driving on public highways) is now quite dated for the most part (primarily in the 1995-1996 time frame), and has not been repeated since his last reported incident of masturbating while driving in 2003. Even though the judgment lapses implicit in this acknowledged behavior reflect part of a pattern of judgment lapses manifesting in different areas and circumstances, this activity has unique characteristics and is one that can be fairly evaluated separately without turning the evaluation into a unsustainable piecemeal assessment. So, although application of the mitigating conditions may not be fully available to Applicant, without ignoring Applicant's history of serious indiscretions in other areas of the record, whole person assessment in these unique circumstances makes it highly unlikely that Applicant will ever again engage in any of these sex-related activities.

Less amenable to mitigation through either the mitigating conditions of the personal conduct guideline or a whole person assessment is Applicant's self-reported disciplinary use of a chastisement device on his children. To Applicant's credit, he took advantage of a parenting course following his last NSA interview. Whether his parenting course has resulted in permanent behavioral changes in Applicant is still uncertain at this point in time. Applicant provided no documentation of his course progress, his completion of the course, or what he learned from the course. His most recent OPM interview reflects some continuing denial of the ramifications of his regular use of the discipline practice on his young children and complicates the process of making predictive judgments about whether he can be expected to avoid recurrent use of the chastisement device in the future. Unlike his accessing pornography and employment of sexual relief actions in public places, his harsh disciplining actions are generally more recent and more likely to generate long term repercussions on the child recipients.

In balance, Applicant can safely be credited with mitigation of security concerns associated with his use of poor judgment in accessing pornography and engaging in masturbation in public

places and areas. More time is needed, however, to make fair and reasonable predictable assessments about his abstaining from inflicting the kind of corporal punishment on his children that he acknowledged to NSA investigators in 2003 and 2004. While Applicant is to be encouraged by his accounts of changing his disciplining practices since taking his parenting course, it is still too soon to mitigate the judgment lapses associated with his past actions. So, while favorable conclusions warrant with respect to the poor judgment allegations associated with his access of pornography on his office computer and his related engagement in sexually oriented activity in public areas, unfavorable conclusions are warranted with respect to the judgment allegations covering his disciplinary practices.

In reaching my decision, I have considered the evidence as a whole, including each of the E2 2.2 factors enumerated in the Adjudicative Guidelines of the Directive.

FORMAL FINDINGS

In reviewing the allegations of the SOR and ensuing conclusions reached in the context of the FINDINGS OF FACT, CONCLUSIONS, CONDITIONS, and the factors listed above, I make the following FORMAL FINDINGS:

GUIDELINE E (PERSONAL CONDUCT):	AGAINST APPLICANT
Sub-para. 2.a (numbers 1 through 5, 7 & 8):	AGAINST APPLICANT
Sub-para. 2.a (number 6):	FOR APPLICANT

DECISION

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue Applicant's security clearance. Clearance is denied.

Roger C. Wesley
Administrative Judge