DATE: December 6, 2002

In Re:

SSN: ----------

Applicant for Security Clearance

ISCR Case No. 01-18445

DECISION OF ADMINISTRATIVE JUDGE

JOHN G. METZ, JR.

APPEARANCES

FOR GOVERNMENT

Marc E. Curry, Esquire, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Although Applicant's unauthorized use of a personal external drive and disk to download unauthorized material from a Government computer was isolated, infrequent, and not recent, his misconduct was significant, not caused by inadequate or improper training, or authorized, and he did not act promptly to correct the action. Evidence of recent actions demonstrating a positive attitude toward discharge of security responsibilities did not overcome adverse inference of his misconduct where Applicant did not convincingly explain what he was doing in May 1999, and why. Clearance denied.

STATEMENT OF THE CASE

On 10 July 2002, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, stating that DOHA could not make the preliminary affirmative finding[(1)] that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. On 7 August 2002, Applicant answered the SOR and requested an administrative decision on the record. Applicant responded to the Government's File of Relevant Material (FORM)--issued 6 September 2002; the record in this case initially closed 2 October 2002, the day Department Counsel entered his objection to the last page of Applicant's response. The case was assigned to me on 16 October 2002. I received the case the same day to determine whether clearance should be granted, continued, denied or revoked. On 29 October 2002, I received a second response from Applicant, which I referred for comment to Department Counsel. Department Counsel responded on 6 November 2002, at which point the record closed.

RULINGS ON PROCEDURE

On 2 October 2002, and again on 6 November 2002, Department Counsel objected to the same document submitted by Applicant.[(2)] Department Counsel originally objected on the grounds that the document was unsigned and undated, not a character reference like most of the other documents, and of unknown provenance. Department Counsel objects to the resubmission--which differs from the original submission only because the questioned document is now signed, but not

dated, by Applicant--as being an inadequate attempt to authenticate the original submission. Department Counsel's points are well taken, but go more to the weight to be accorded the questioned document and not to its admissibility. Consequently, while I consider the document may be entitled to little weight, I will consider it as appropriate in assessing this case.

FINDINGS OF FACT

Applicant denied the allegations of the SOR.

Applicant--a 36-year old employee of a defense contractor--seeks renewed access to classified information. He held a clearance as late as May 1999, but it is not clear from the record whether he currently has access. He served on active duty with the U.S. Navy from 1984 to 1996, reaching paygrade E-5 as an Aviation Technician. He had a clearance during most of his active duty. After leaving the Navy, Applicant obtained associate's and bachelor's degrees in computer technology (Item 4).

In May 1996, Applicant went to work for a government contractor. In November 1996, Applicant was granted an interim clearance; Applicant submitted a formal clearance application (Item 4) in April 1997, which was presumably granted.[(3)]

Sometime before October 1998, Applicant went to work for another government contractor.[(4)] On 1 October 1998, Applicant acknowledged receipt of--and agreed to comply with--the company's Security Practices and Procedures (SPP) (Item 5),[(5)] specifically his understanding of his personal responsibilities for obtaining advance approval from the security office before bringing prohibited articles into the facility and his responsibility to safeguard classified information, sensitive material, and company private and proprietary material (Item 6). The same day, he acknowledged receipt of a detailed list of his reporting responsibilities to the security office (Item 7). He also acknowledged reading and understanding the company briefings detailing his responsibilities for: keeping his records clean, need-to-know, reporting responsibilities, prohibited articles, adverse information reporting, and foreign collection activities.[(6)]

The company which hired Applicant was a Government contractor providing services to the user agency at that agency's facility, under circumstances where contractor personnel may work side-by-side with Government employees in executing the contract. The main focus of the computer work Applicant and his associates performed was on the information security of Government computers and information. On 5 May 1999, an employee, (**A**), of Applicant's company was performing routine end-of-day security checks in company-designated spaces within the agency facility, a room approved for open storage of secret material. Inspecting Applicant's cubicle, **A** discovered that Applicant's computers were on, with the monitor turned off.[(7)] **A** turned the monitor on and discovered that the classified computer had its password-protected screen saver enabled, as required. However, the screen saver on the unclassified computer was not enabled; several Windows processes were running and the display screen was frozen on an internet Window for another Government agency in a different state. When **A** was unable to conduct an orderly shutdown of the system, because the operating system was not responding, he called another company employee, (**B**), over from where he had been conducting end-of-day security checks himself to enlist his help in sorting out the problem with the unclassified computer. When they were unable to shut the computer down normally, they decided to restart the computer, which they did successfully. While the computer was rebooting, **A** noticed an external drive (zip) powered-up and attached to the unclassified computer. Neither **A** nor **B** knew anything about the external drive, because it was not the standard issue zip drive in use in this office. **A** and **B** conducted a preliminary examination of the external drive and discovered a 1.0 gigabyte disk. They examined the disk and concluded that it contained information taken from the classified global security directory. They then secured the disk in **B**'s locking storage compartment in his cubicle (Item 9, 10).[(8)] Later that evening, **B** contacted the Government manager of the project and they agreed to discuss the situation with Applicant the next morning.

On 6 May 1999, Applicant approached the Government manager and asked about his computer being shut down and two missing disks. Applicant informed the Government manager that the external drive and disks were his personal property, and asserted that the disk contained no classified information. However, when the Government manager confronted Applicant with the fact that it was against policy to connect personal equipment to Government systems,

Applicant agreed, stated he had business elsewhere, and left (Item 9).

The Government manager and **B** spent much of the rest of the day conducting a detailed examination of the disk contents,[(9)] and advising successive levels of management and security officials, both Government and company, of the results of their investigation. They also examined Applicant's email account from a central computer and discovered no email activity by Applicant. By the time they returned to Applicant's cubicle, the unclassified computer had been "scrubbed," nearly all programs removed from the desktop (Item 9).

On 7 May 1999, the company security director conducted an interview with Applicant at the company's local facility, with a conference connection to the Government facility. Between the two locations, most of the management and security officials who were briefed on 6 May 1999 listened to the interview. The adverse information report submitted by the company security director on 10 May 1999 (Item 11), summarized the interview:

. . . During the interview, [Applicant] stated he brought the disk to the [Government building] on 5 May. He said he didn't see anything wrong with bringing his personal drive into the [Government building] because nobody told him he couldn't. When asked if he remembered signing the Security Awareness Statement on 14 October, he said I guess so. He also stated this was the first time he had ever brought personal software into the [Government building]. All questions about how the classified material got on his disk were answered with "don't remember", "I don't know", "I don't recall", and I have no idea how the classified got on the disk". He stated he never brought any proprietary information from previous employers and answered "no" when asked if he ever mishandled classified information. He also said "no" when asked if he ever handled information for which he was not authorized. When asked why he left the disk on the computer when he went home on 5 May he said because he wasn't finished downloading. Many questions, no matter what the topic were answered with "All I know is the disk and the black book were going to [**A**]." [Applicant] terminated employment with [the company] on 7 May. He did not wish to identify his new employer and had no idea whether his new job required a security clearance.

After describing ongoing followup actions, the director of security observed that Applicant's motives for his actions remained unclear.[(10)]

On 23 May 2001, Applicant was interviewed by an agent of the Defense Security Service (DSS) about the May 1999 events. Applicant stated he had been hired by the company to work on a short-term (45 days) basis until the company found a permanent employee for the position. He signed, but did not read, the briefing documents he had acknowledged in October 1998. He expanded on his statement during the 7 May 1999 interview that he was downloading programs (but not classified information) at the behest of **A**, so that **A** could continue work on the project once Applicant left the job. Applicant also stated his understanding that **A** expected to be promoted into the job that Applicant was filling on a temporary basis. He reiterated his earlier statements that he did not believe he had done anything wrong in bringing in his personal external drive and disk.

In his undated response to the FORM, Applicant asserted, for the first time, that he was hired by the company initially to work at a different Government facility, but was prevailed upon by the company to work at the other Government facility temporarily because the company was going to lose the contract if they did not have Applicant to fill in a vacant position. **A** was unhappy with this arrangement because he expected to get the position, but showed great interest in everything Applicant was doing on the contract. When the company was unwilling to move Applicant to the other Government facility as they had promised, Applicant began looking for a job elsewhere, and was eventually hired by his current employer.[(11)] According to Applicant, he advised his company that he was leaving, and **A** requested Applicant record the various programs for his use after Applicant's departure. Applicant believes that **B** discovered the disk and **A** denied knowing anything about it.

Applicant submitted eight character references with his response to the FORM, all of whom work with Applicant at his company, one of whom also has personal contact with Applicant. All his references consider Applicant an excellent information security professional who follows company regulations and possesses great honesty and trustworthiness. Although he apparently does not have a security clearance, and thus cannot work on security-related projects for the Federal Government, he has performed similar work for state and local governments and corporate clients.

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines to be considered in evaluating an individual's security eligibility. The Administrative Judge must take into account the conditions raising or mitigating security concerns in each area applicable to the facts and circumstances presented. Each adjudicative decision must also assess the factors listed in Section F.3. and in Enclosure (2) of the Directive. Although the presence or absence of a particular condition for or against clearance is not determinative, the specific adjudicative guidelines should be followed whenever a case can be measured against this policy guidance, as the guidelines reflect consideration of those factors of seriousness, recency, motivation, *etc*.

Considering the evidence as a whole, the following adjudication policy factors are most pertinent to this case:

GUIDELINE K - SECURITY VIOLATIONS

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

[1st] Unauthorized disclosure of classified information;

[2nd] Violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

[2nd] Were isolated or infrequent;

[3rd] Were due to improper or inadequate training;

[4th] Demonstrate a positive attitude towards the discharge of security responsibilities.

GUIDELINE M - MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying also include:

[1st] Illegal or unauthorized entry into any information technology system;

[3rd] Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

[4th] Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

Conditions that could mitigate security concerns include:

[1st] The misuse was not recent or significant;

[3rd] The introduction or removal of media was authorized;

[4th] The misuse was an isolated event;

[5th] The misuse was followed by a prompt, good faith effort to correct the situation.

GUIDELINE E - PERSONAL CONDUCT

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Conditions that could raise a security concern and may be disqualifying also include:

[5th] A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;

Conditions that could mitigate security concerns include:

None.

Burden of Proof

Initially, the Government must prove controverted facts alleged in the Statement of Reasons. If the Government meets that burden, the burden of persuasion then shifts to the applicant to establish his security suitability through evidence of refutation, extenuation or mitigation sufficient to demonstrate that, despite the existence of disqualifying conduct, it is nevertheless clearly consistent with the national interest to grant or continue the security clearance.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. Where facts proven by the Government raise doubts about an applicant's judgment, reliability or trustworthiness, the applicant has a heavy burden of persuasion to demonstrate that he or she is nonetheless security worthy. As noted by the United States Supreme Court in *Department of the Navy v. Egan*, 484 U.S. 518, 531 (1988), "the clearly consistent standard indicates that security-clearance determinations should err, if they must, on the side of denials."

CONCLUSIONS

The Government has established its case under Guidelines K, M, and E, and the Applicant has not mitigated the conduct. On 5 May 1999, Applicant connected an unauthorized personal external drive with high-volume disk into a Government computer system, and used it to download classified files, Government-licensed software programs, and company proprietary information. He did so despite the fact that it was against company policy to bring unauthorized external media into his office and to connect personal equipment to Government systems. Applicant asserted that he did not read the security briefings that he signed in October 1998, but his conduct and statements belie that claim. On 6 May 1999, he acknowledged to the Government manager that he knew that his use of his personal external drive and disk was unauthorized. His unclassified computer was later found with its programs scrubbed from the desktop. Further, the violations alleged are basic security precautions, particularly for a highly-skilled information security specialist (with a Navy background in a highly technical field) such as Applicant. Applicant attempted to lay the responsibility for his actions on **A**, suggesting that **A** either deliberately set him up or simply failed to own up to his request to Applicant to download the information found on the disk.. However, the most detailed assertion of this theory comes only in response to the FORM. Applicant's recorded responses during the 7 May 1999 interview (reported by the individual who conducted the interview, and not either **A** or **B**) are evasive on why and what he was downloading. Although Applicant did have job offer to start work with his current company, that detail did not appear in the initial reports of the security violation or in Applicant's sworn statement to the DSS. In addition, it appears that the events of 5 May 1999 prompted Applicant to terminate his employment well before his projected start date with the new employer.

Examining the events of 5 May 1999 overall, Applicant's conduct was isolated, infrequent, and not recent. However, the misconduct was significant, was not caused by inadequate or improper training, or authorized (despite Applicant's claim to the contrary), and Applicant did not promptly act to correct the action. Indeed, he appears to have acted to remove

evidence of his action from his unclassified computer. While Applicant's favorable character references provide some evidence of actions that demonstrate a positive attitude toward discharge of security responsibilities, what Applicant has not done, is convincingly explain what he was doing in May 1999, and why. The position Applicant had then, has with his current employer's non-Federal clients now, and presumably seeks with the Federal Government, gives Applicant access to the "keys to the kingdom." The events of May 1999 may be a meaningless blip in Applicant's conduct, or not. However, Applicant had the burden to demonstrate its security insignificance, a burden he did not meet. Accordingly, I resolve Guidelines K, M, and E against Applicant.

FORMAL FINDINGS

Paragraph 1. Guideline K: AGAINST THE APPLICANT

Subparagraph a: Against the Applicant

Subparagraph b: Against the Applicant

Paragraph 2. Guideline M: AGAINST THE APPLICANT

Subparagraph a: Against the Applicant

Subparagraph b: Against the Applicant

Paragraph 3. Guideline E: AGAINST THE APPLICANT

Subparagraph a: Against the Applicant

Subparagraph b: Against the 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 a security clearance for Applicant.

John G. Metz, Jr.

Administrative Judge

1. Required by Executive Order 10865, as amended and Department of Defense Directive 5220.6, dated January 2, 1992--and amended by Change 3 dated 16 February 1996 (Directive).

2. Described by Department Counsel as "page 10," but not so numbered by Applicant and not the tenth page of Applicant's response as submitted to me originally, or in Applicant's resubmission. However, by process of elimination, I have deduced that the questioned document is a document, now signed by Applicant, purporting to describe Applicant's version of the events surrounding the SOR, albeit written in third person.

3. Item 11 reflects that Applicant was granted a clearance on 24 September 1998.

4. The record does not reveal whether Applicant remained with the contractor who nominated Applicant for his clearance in April 1997.

5. Specifically the portion prohibiting transmission of classified material by unauthorized means.

6. Item 11 also reports that Applicant received a security indoctrination by the Government on 14 October 1998, but the record contains no information on what this briefing contained, and no signed acknowledgment by Applicant.

7. The computer configuration for Applicant was typical for this Government agency: a classified computer and an

unclassified computer share a monitor, which is accessed by an A/B switch. However, the computers are not connected to each other (i.e., no inter-operability between them).

8. **A** completed an unsigned Memorandum for Record (MFR)(Item 10) on 6 May 1999. **B** completed an MFR (Item 9) on 6 May 1999, which he signed and dated on 10 May 1999.

9. Found to contain a classified company report, a summary of the report, filled-in data sheets for classified servers (classified when filled in), a company proprietary report on encryption, an entire directory from the classified local area network (LAN), reports on active and inactive account holders on the classified LAN (with classified email addresses), and installation sets for Government-owned software packages, with licensing agreements. The Government manager and **B** agreed that the reports and data sheet could only have come from the classified LAN, as they were not available from any other source.

10. However, there is no evidence in the record of the results of the follow-up actions underway at the time.

11. Applicant's response contains the first page of a 23 April 1999 letter from his current employer offering Applicant a job with the employer. The typewritten start date for the offer--10 May 1999--bears an inked change to 24 May 1999, but it is not clear who made the change.