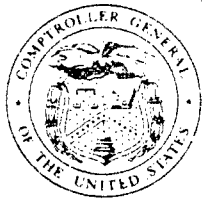


Worrell  
PH

15296

**DECISION**



**THE COMPTROLLER GENERAL  
OF THE UNITED STATES**  
WASHINGTON, D.C. 20548

FILE: B-198305

DATE: October 29, 1980

MATTER OF: Federal CSS, Inc.; Martin Marietta **DLG 05410**  
Data Systems

DIGEST:

1. Procuring agency's exclusion of proposal based on analysis of supervised benchmark test concluding that six major deficiencies were present is incorrect. Accordingly, protest is sustained and recommendation made that all or a portion of the benchmark test be rerun, if deemed necessary by the Navy in light of our decision.
2. No basis for protest arises when agency advises offeror that its proposal is technically unacceptable, and at the same time, gives offeror opportunity to demonstrate that determination was in error--thus showing contingent nature of determination. Rather, basis for protest arises only when agency responds (or refuses to respond) to offeror's demonstration.
3. Procuring agency's determination to exclude proposal because offeror's system could not complete benchmark test cannot be questioned.

Federal CSS, Inc. (Federal), and Martin Marietta Data Systems (MMDS) protest the Department of the Navy's Automatic Data Processing Selection Office **DLG 05412** (Navy) determination that their respective proposals, submitted pursuant to request for proposals (RFP) No. N66032-79-R-0012, were technically unacceptable after "benchmark" testing of their data processing systems.

[Protest Against Determination That Proposals Were Unacceptable]

~~012615~~

113647

Based on our review, we recommend that the Navy allow Federal another benchmark test; we deny MMDS's protest.

### Background

The RFP solicited data processing services, under the General Services Administration Teleprocessing Services Program, in support of the Naval Automated Civilian Management Information System (NACMIS) for the Naval Civilian Personnel Command. Primarily, NACMIS is a recordkeeping information system which collects, manipulates and stores civilian employee data for transaction and periodic reporting. Each activity maintains its own data base which is used by NACMIS to automatically transmit reports to the Personnel Automated Data System, to print Standard Form (SF)-7's and SF-50's (personnel forms), and to generate various reports. The system maintains for each activity an employee data base which can be used or "accessed" only by that activity or the NACMIS Project Office in the case of emergency or for maintenance. NACMIS's main purpose "is to provide cost-effective automated civilian personnel management through a system that would be common to over 140 activities."

The RFP required each of the offerors to submit the output from their own benchmark along with their proposal. If found technically acceptable, the next step was to be a Navy supervised benchmark, the requirements of which were set forth in section D.3 of the RFP. The supervised benchmark was a benchmark conducted by the Navy personnel in the presence of offerors' representatives. The final step concerning the benchmark requirements was a second test, a "blind" benchmark--run only after successful completion of the supervised benchmark--also performed by Navy personnel but not witnessed by the offerors' representatives. This test was an unannounced rerun of a portion of the supervised benchmark. The Navy's determinations of technical unacceptability were made when Federal was judged to have failed the supervised benchmark demonstration and when the Navy was unable to complete the blind benchmark demonstration on MMDS's system.

### Federal's Protest

The Navy advises that in Federal's first supervised benchmark demonstration there were two major failures or deficiencies. As a result, Federal was allowed an opportunity to correct the deficiencies in a second benchmark.

In the second supervised benchmark, which included eight separate tests, the Navy states that it found six major deficiencies, two of which in one submission the Navy characterizes as critical failures, while in enclosure 13 of its June 20, 1980, report the Navy characterizes all six as fatal. Our Accounting and Financial Management Division performed a technical review of the six major deficiencies. Based on this review and the record before us, Federal's protest is sustained.)

#### Deficiency #1 - Escape into Operating System

The Navy's position is that test 2 of the second benchmark (March 14, 1980) demonstrated that Federal's proposal failed to meet three of the RFP's mandatory requirements relating to security against unauthorized access into the operating system. The three requirements are:

"F.2.2.8: Access Security. The system shall provide for protection from unauthorized read and write access of user programs, the operating system, and the areas in which their code resides. This includes protection from writing and reading by programs not in NACMIS and any other interference caused by software or hardware.

"F.2.6.1.(37): (The offeror is required to) capture user interrupts (suspends) and process them within NACMIS; however users shall not be allowed direct access to the operating system in order to access their own local software for compiling or modification.

"F.2.6.1.(38): Field users logging on to NACMIS shall automatically be placed in an application program controlled by NCPC. The field user shall exit the applicable programs only by being automatically logged off."

During test 2, one of the test operators "deviated from the script" (that is, departed from the prescribed test format) and "escaped into" (entered) Federal's control program, which Federal calls "VP," and which the Navy considers to be part of Federal's operating system. This occurred when an erroneous command was entered into the computer by the operator 23 times resulting in 23 computer responses consisting of requests for a social security number. On the twenty-fourth time the response was "VP entered, request please." Then, we note that the operator in making certain requests received further responses advising that invalid VP requests were being entered by the operator. The Navy argues that once in VP the operator "has the ability to modify the entire computer system (not just [the] NACMIS [program])." This, the Navy contends, violates the aforementioned requirements which essentially "require that the operator be limited to performing within the NACMIS program."

Federal, while admitting that there was entry into the VP level, argues that "this does not mean that the operator had managed to 'escape into the operating system.'" Federal explains that "[its] proposed computer system consists of two basically unique and distinct parts, the VP program and the CSS system." Federal submits that the operating system is the CSS system. In addition, Federal states:

"\* \* \* The CSS operating system contains and controls the files and compilers (i.e., the data content of the computer system and the programs pertinent to the access and modification thereof). \* \* \* The VP control program, on the other hand, by itself has no capability to access or modify the data and/or the software content of the computer system. Rather, the VP program is analogous to both a traffic cop and a security guard with respect to the CSS operating system. \* \* \* That is, the VP program

allocates the various hardware resources required by the CSS operating system, and checks all users for the appropriate privileges (e.g., ensures compliance with the specified logon, password, and access procedures). \* \* \* A potential user seeking access to the CSS operating system can only do so by first passing through the VP program by 'satisfying' such program that the user in question possesses (and has properly so demonstrated) the requisite privileges, employing the proper command and protocol procedures."

Federal believes the VP level functioned correctly, not allowing access to the operating system, since "the operator elicited no commands or responses from the CSS system."

The solicitation's Glossary of Terms, 1.45, defines "operating system" as follows:

"The totality of all control software, such as executive routines, call routines, loading routines, working routines, together with priorities, associated data, and related software to permit total system operation; including necessary arrangements for assignment of available hardware, storage, and central processing unit allocation, control of queuing, input/output operations, receipt and transmission, and general control of data flow."

Under this definition, VP is technically part of the operating system. Nevertheless, the only functions available to the user when working within VP, as it was configured for this benchmark, were to log off or restart NACMIS, as was done. Therefore, VP, although part of the operating system, was a "rigidly controlled environment." Appendix I-Security Facilities of Federal's VP/CSS manual supports this conclusion.

The intent of the solicitation with respect to security, from a functional standpoint as seen in the requirements stated above, is to prevent the modification of the NACMIS system and data and unauthorized access

to the NACMIS data and other user programs. VP satisfies the intent of the instant solicitation even though it technically is a part of the operating system. As noted above, there was entry into VP. However, as also noted, everything the Navy operator entered once in VP resulted in the "response-invalid" command. If, on the other hand, the operator entered that portion of the operating system which was the object of the Navy's concern, the operator would have been no longer restricted by the system. Rather, the hardware would have been his only restriction. The record indicates VP prevented access to the NACMIS data.

While the Navy was in VP, the record indicates that there was no attempt by the Navy to access the NACMIS system files. In other words, there was never an escape from the "controlled environment."

Our review of the evidence before us supports Federal's position that in VP you are essentially "on the front porch" where you still must use a key (password) to enter the house (data). In VP the user has no access to files, is unable to perform the writing of data, and either can log off or restart NACMIS. Accordingly, Federal's VP satisfies the intent of these specifications even if VP is considered to be a part of the operating system; consequently, this alleged deficiency should not have resulted in the rejection of the proposal.

Deficiency #2 - Failure to Validate  
Password and Library Name

The Navy contends that Federal's system did not comply with the solicitation's mandatory requirements-- "preventing network access by a user who does not submit a valid password and library name." The provisions emphasized by the Navy are:

1) Section F.2.2.2(b)--

"The required library sharing arrangements are shown in Figure 1. The arrangements and type of sharing are subject to modification during the life of the contract as library functions change, at the authorization of headquarters personnel. The protective features provided

by the Contractor shall include two basic functions: first, the validation tests permitting only valid users to access the network; second, the appropriate permissions for use of the library. On a request basis, the complete library sharing profile shall be readily available to ensure that only the desired sharing arrangement and type is in force."

2) Section F.2.2.2(c)(2)--

"Security Controls - Access to the network shall be limited to the user's own library of files and to those other libraries of files which he has been authorized to share. Two controls are required for access: 1) an assigned library name (which is a library of files) and 2) a password selected and maintained by the user. The user shall be able to change the password."

3) Section F.2.2.5(a)--

"\* \* \* Such controls shall enforce the network access and determine what facilities each authorized terminal user may access and how much of the resource he may consume."

It is the Navy's position that during test 5 (March 14, 1980) Federal's system allowed network access for several of the operators after they inadvertently entered an incorrect library name into the system. The correct library name was "ACT" and a numeral from 1-7. An operator typed "A" without waiting for a prompt (a response from the system telling the operator that the system is ready to begin operations) from the system and, therefore, the system, which reads only after prompting the operator, read the library name as "CT2." The Navy says that after this the system "allowed access to the program 'CTLMOD' which is the NACMIS control module" before automatically shutting off.

The Navy argues that the requirements, stated above, provide that the operators be logged off the system, which was not accomplished until after CTLMOD was printed. Instead, the Navy states that the system accepted the invalid library name and improperly allowed "access to the network"--meaning, CTLMOD.

Federal's position is essentially that until an operator properly enters the necessary information the operator will not have access to the files or accounts. Federal submits that the operator's error, failing to wait for a prompt, resulted in an incomplete logon and then the operators were logged off. Moreover, Federal points out that the benchmark test proceeded without further incident once the operators repeated their entries, after receiving the system's prompt.

Before considering the deficiency, we will examine some of the concepts involved.

Under the RFP, the validation of the password and appropriate permission for library use are described as separate steps. The validation test is the taking of information supplied by the user and comparing it to a list of data (i.e., correct or valid responses). The user is allowed entry past this point in the system only if the password used is included in the list. Permission for use is a different function, implemented in a variety of ways. In the instant situation, once a correct library name is typed in, that library is available for the session. Validation of the library occurs at the time of access to the library, i.e., when it is called up. When a user logs on, the user has allowable access to several libraries and the library name entered only informs which particular library, out of the entire permissible group, the user needs at that time.

Here, the problem arose when the operator started typing in the library name prior to receiving a prompt after the computer had typed its message (A/C Info) in response to the correct password. After the library name was believed to be typed in, nothing happened (other than the printing of CTLMOD) except that the system responded that the library did not exist and the operator was logged off. This occurred since Federal's VP does not validate



the library name at its initial entry. Rather, the VP remembers (stores) the library information and then gives the operator another prompt (e.g., requests that the operator advise the system of the next operation). When the operator types in the operation code, VP then validates the library name before allowing the operation to proceed with the scheduled tasks. This is what did occur when the Navy ran test 5 for the second time.

While we note that Federal's system accepted an invalid library name, "CT2," this does not mean that Federal's method of library sharing is defective. This method was established by Federal's "Profile and Protect Exec" files, which are security features designed to protect unauthorized access to programs and data. These files are associated with the user ID and establish which libraries the user has access to. Once the library is brought forward (e.g., is able to be accessed by the user), the NACMIS procedures (programs) begin and the user proceeds to the controlled environment and can only do what the NACMIS programs allow.

Furthermore, the RFP does not require the validation of the library name, as it does the password, at the time it is initially typed by an operator. As a matter of fact, the RFP does not specify the time for validation of the library name. Moreover, if the Navy wanted a validation routine for the entering of bad data (e.g., an improper library name), as occurred here, then one should have been specified in the RFP. In this circumstance, Federal's system complied with the RFP requirements concerning password validation and library access.

Although the Navy argues that there was an "access to the network" since the system printed CTLMOD--the major NACMIS control program--our review of the original benchmark logs did not disclose successful access to any library to which the user was not permitted access and the system automatically logged off after the program was printed.

The Navy has also suggested that, had CTLMOD been programmed as it will in actual operation, access, through a library, might be obtained to a high speed printer which then might be improperly used. Our review shows that this suggestion is incorrect because Federal's system, in fact, will not allow access to an unauthorized library as was shown in this test.

Thus, we conclude that the alleged deficiency does not conflict with the intent of these specifications.

Deficiency #3 - Test 8 Data

Pursuant to test 8, the offerors were to demonstrate that their proposed system was capable of supporting input/output (I/O) operations on data files created by either "COBOL or FORTRAN" programs. Test 8 required the printing of SF-50's, used to document federal civilian personnel actions for seven fictitious employees. Federal's system failed to print the "Clint Eastwood" SF-50 in the batch printout. In addition, test 8 required that one summary report should be printed for each request for printing SF-50's. Our review of this report indicates that "Clint Eastwood" was not included in the list of SF-50's printed.

The Navy's position is that "[Federal's failure] to print all the names entered is a fatal flaw which if accepted would defeat the Navy's intent to acquire a reliable system to handle personnel actions." Moreover, the Navy states that Federal was printing more than one report for various accounts. This, the Navy believes, demonstrates Federal's lack of system control.

With respect to the "Clint Eastwood" SF-50, Federal argues that the reason for its failure to print is based on the terminal 2 test operator's error--the entering of an incorrect social security number--which occurred during test 2. Alternatively, Federal argues that the "Clint Eastwood" account was not entirely missing. Rather, the account was in the system but "the file [data base] in question had not yet been closed by the updating program." Concerning the multiple printing of the summary report, Federal contends that "the cause of this 'discrepancy' may be traced directly to the Navy." Federal points out that "the printouts in question were produced by the Navy's Datapoint 5500 bulk terminal, in response to the direction of Federal's software and computer." Federal believes that had the Datapoint terminal been configured, as specified in the RFP, in accordance with Standard IBM 2780 protocol, the Datapoint terminal would have automatically sent a message to Federal's computer

that the data was printed and Federal's computer would have proceeded to print the next block of data. In any event, Federal posits that this multiple printing "demonstrates an important 'failsafe' in Federal's proposal which is designed to prevent the accidental loss of printout transmissions."

Our review of the terminal logs demonstrates that terminal 2 test operator's error referred to by Federal was corrected after the "mix up" occurred. In addition, the record makes it clear that this correction occurred approximately 1-1/2 hours prior to the running of test 8. This, in addition to the fact that Federal's VP/CSS Manual, appendix C, page C-4, paragraph 6, provides that Federal has the capability for immediate updating, leads us to believe that the updating program was closed at the running of test 8.

What actually occurred during test 2 was that the Navy terminal 2 operator was accessing (using) data base "ACT 2" rather than "ACT 1," the correct data base (library). Consequently, when the terminal 2 operator was performing test 2 he was updating (adding a new employee--"Clint Eastwood"), the wrong data base. Even though, as noted above, the problems which occurred were subsequently corrected, the corrections were made on the wrong data base. In order to validate all of test 2, the Navy was using the SF-50's produced by terminal 1, library "ACT 1," account UY0001. The result was the printing of the six SF-50's which were correctly entered into "ACT 1." Thus, because of this test 2 error, "Clint Eastwood" was missing in test 8. Consequently, Federal may not be faulted for the missing "Clint Eastwood" file.

In regards to the multiple printings, this circumstance relates to the Navy's use of a Datapoint 5500 bulk terminal during testing. For the same reasoning as set forth under our discussion of Deficiency #5, below, which also relates to this terminal, it is also our view that this circumstance is a minor problem, easily remediable.

Deficiency #4 - Failure to Identify  
and Run All Jobs for Processing

Test 5 was utilized to demonstrate the ability to submit jobs using varying priorities which are established

by the terminal operator. The original log with respect to the terminal 4 operator exhibits that a mistake as to entry was made and then correction was accomplished. It appears that the proper entry was then made (time 14:52:41), but the job was not printed.

Federal's response is essentially that it is unsure as to why the job was lost. The Navy's position is that the resubmission of approximately 4 percent of all job requests is "no small matter, especially where, as here, the Navy is being charged for both the additional \* \* \* operator time incident to resubmission." Furthermore, the Navy dismisses operator error as the basis for Federal's submission since the computer acknowledged the job ("Time Job Submitted:14:52:41"). The record before us does not indicate why the job was lost.

However, what the Navy fails to recognize is that the system alerted the operator that the batch job was not accepted. This "warning" should have been evident since after the system's message indicating the time the job was submitted the usual affirmative message, such as "Batch job will be run priority 6," did not appear on the screen. At this point, the Navy operator should have queried the batch job queue to determine if the job was actually entered into the system rather than having entered the next request. If the job was listed in the batch queue, then he could have proceeded to the next request. If, however, the job was not in the queue, then the operator should have returned the job submission to determine why it was lost. Since this was not done, we cannot say with any certainty what occurred. Notwithstanding, we do not believe that this "deficiency" in and of itself is sufficient to support the Navy's determination that Federal's proposal is technically unacceptable because the Navy operator acted unreasonably.

Deficiency #5 - Failure to Printout Entire  
Batch Output on One Call to the System

Federal argues that the cause of this "deficiency" was the Navy's use of a Datapoint 5500 bulk terminal, which was not configured to emulate "a standard IBM 2780," as

required by the RFP, and, therefore, operator intervention was required. Federal's position is that had the Datapoint terminal been configured as specified in the RFP, section "c," paragraph 33, the system would have functioned as specified. Section "c," paragraph 33, provides in pertinent part:

"Communicate asynchronously with the network's host computer for interacting, updating and construction job streams, using IBM 2780 and IBM 3780 protocols, ASCII code.

\* \* \* \* \*

"Error detection is that available under the IBM 2780 and IBM 3780 communications protocol."

The Navy admits that the RFP specified that the Datapoint terminal would be configured in accordance with Standard IBM 2780 protocol procedures. Furthermore, the Navy states that "the terminal had a Datapoint Standard 2780 configuration." In addition, the Navy advises that "instead of the bulk terminal operator being able to obtain printouts of an entire batch of processed files, only one file was printed for each request." Moreover, Federal had to set up a second terminal (interactive) which directed the files to be printed at the bulk terminal. It is the Navy's position that this violated the following RFP provisions:

F.2.6.1(16)--

"Allow a user to submit a task for deferred processing from either the bulk terminal or from an interactive session. Conversely, permanent data file outputs and print outputs, including control language job stream outputs from a batch job, shall be made available to an interactive session."

F.2.6.1(20)--

"Provide service to all local, remote, and interactive input and output devices on a demand basis without the requirement for operator intervention."

It is our view that the Navy, by using the Datapoint emulator, misled offerors to believe that it would be able to emulate an IBM 2780. It is clear that the Datapoint 2780 emulator is not identical to an IBM 2780. The Navy agrees that the "Datapoint configuration varies slightly from the IBM configuration." However, the Navy submits:

"Several offerors in addition to FCSS had problems with the bulk terminal. Offerors, including FCSS, all were directed to work these problems out with Datapoint. [The Navy] expressly informed each offeror that it had the option of using a different 2780 or reconfiguring the Datapoint 2780 to meet the needs of its own equipment. FCSS was the only offeror that failed to work with Datapoint to solve its problems. FCSS therefore, should be held accountable for any problems resulting from its deliberate inaction."

It is our view that the Navy's advice to each offeror, as noted above, would not be sufficient to put any offeror on notice that the Datapoint 2780 emulator would not be configured identically as a Standard IBM 2780. We believe that the cause of this deficiency resulted either from the Navy's failure to be explicit in the RFP as to how the Datapoint terminal was actually configured or from failure to allow a communications test. A competing offeror should be given the opportunity to examine the emulator and terminal equipment. Such examination or test is the best method for the offeror to determine if its system can be used, giving the offeror the opportunity to resolve communication problems, if any. To not allow such an examination, in certain instances, is to give the incumbent, who by its position has a communications test everyday, an unfair advantage. It is our view that, in the instant circumstance, failure to allow a communications test was a Navy error. The fact that the other offerors solved their problems by contacting Datapoint does not alter our view that in this procurement no offeror should have been essentially forced to check with Datapoint. In any event, we believe that this

deficiency is easily rectifiable in that the differences between the Datapoint and IBM emulators with respect to the capability to print batch output on one call are minor.

In addition, the Navy questions Federal's lack of keyboard support for the Datapoint terminals. However, we note that the Navy admits that the IBM 2780 emulator does not have keyboard support which the Navy contends was an implied RFP requirement. Since Federal's system was anticipating the IBM 2780 emulator, as specified in the RFP, the configuration for the benchmark test did not provide keyboard support. In this circumstance, we find that the Navy's position is inconsistent with the RFP requirements implied or otherwise. If the Navy desired keyboard support, the Navy could have specified such in the RFP and utilized the IBM "HASP" workstation emulator which is included in the communications software supplied for the Datapoint terminals and provides keyboard support.

Therefore, these deficiencies are not sufficient to support the exclusion of Federal's proposal.

Deficiency #6 - Failure to Print Priority  
Prior to Commencing the Next Operation

It is Federal's position that the alleged deficiency here--an "overlap" caused when its system acknowledged receipt of a batch job submission during the entering of data stage for the next job--"is clearly not a violation of the RFP and, indeed, is the direct result of the performance characteristics required by the Navy itself." Federal states that its system "processes batch jobs asynchronously to prevent delays which might occasionally occur during peak use of the computer system." Consistent with the requirement of interactive operation, Federal argues that its "system returns (i.e., remains 'open') to the terminal to permit the operator to proceed with the next request while the computer is processing the prior batch request." Moreover, Federal submits that "this permits the most efficient use of all terminals and terminal operators, but also means that, on occasion, an individual terminal operator may commence entry of the next request before the computer completes processing his or her first batch request."

The Navy argues that overlapping messages create problems of identification. As the Navy explains:

"Once a job is entered, it is assigned a priority. This priority determines how soon a job will be executed. Once assigned, the priority is confirmed on a printout."

The Navy believes that the priority of the first job appearing in the middle of the next job is a problem.

The Navy, in support of its position, points to one example during test 8 where after the system responded to terminal 7 operator's request "23," the system printed out "request" which indicates simultaneously that the job is complete and inquires whether there are any further jobs. At that point, the operator replied "STOP" indicating that there were no more jobs. The Navy contends that the computer should have logged off. However, it then proceeded to print out the remaining portion of the report, in response to request "23," which supposedly was already completed. This, the Navy believes, will cause problems since the portions of the various reports will have to be identified and assembled into complete reports. Notwithstanding, the Navy does not point to any provision in the RFP which requires Federal to complete one batch job request prior to the submission of a new batch job request. Rather, the Navy posits that the "requirement is inherent in the context of the RFP when read as a whole."

Our review of Federal's system indicates that an operator can initiate a job request and control is immediately returned to the operator. At this point, while the system separately indicates the job, the operator can initiate a second job request. This is unlike the incumbent's system with which the Navy is familiar. Under such system, the sequence of events is (1) operator initiates a job request, (2) the system processes the request, (3) the system initiates the job, and (4) the system returns control to the operator. Under this system, descriptive data is received after the system indicates the first job and, then, the operator can proceed with the second job. The Navy's position



is not so much that Federal's system is wrong, but that the system is confusing. However, an agency cannot expect all systems to be identical and should assume, at least initially, that the new system may be confusing. It is our view that when the RFP is read as whole, the requirement to essentially conform to the incumbent's system concerning priority printing is not clear in the RFP. In any case, even though such is not a specific requirement in the RFP, this situation appears to be one that could be easily rectified (by RFP amendment) or the protester could easily convert to the "initiate job-receive-data-initiate second job" system. Under these circumstances, it is our opinion that the Navy was unreasonable to downgrade Federal for this deficiency.

Based on the foregoing, we find that the Navy's evaluation of the supervised benchmark was not reasonable. Therefore, we recommend that the Navy disregard the disputed test results and rerun all or a portion of the test in the supervised benchmark for Federal's system to allow Federal the opportunity to demonstrate the performance capability of its system.

Our recommendation of rerunning those portions of the benchmark when the Navy deems such necessary is based on the fact that the Navy is in the best position to determine the procedures needed at this stage in the procurement. For example, we note that under Deficiency # 1 the Navy objected to what it termed unauthorized access into the operating system. Whether in light of our findings, that access to the operating system did occur but such did not breach the intent of the RFP's security specifications, the Navy would desire to rerun test 2 and attempt to access the NACMIS system files or simply reevaluate test 2 must be left to the discretion of the Navy. Another example is found in Deficiency # 2 where the Navy maintained that network access occurred when an incorrect library name was entered into the system. Here again, we note that the Navy is faced with various alternatives. These include, for example, re-evaluating test 5 without rerunning it or rerunning test 5 and either entering an invalid and nonexistent library, as occurred, or entering an existing library which the user is not authorized to access and in both instances attempt to access the NACMIS data files.

Accordingly, Federal's protest is sustained.

MMDS Protest

A. Timeliness Issue

On March 26, 1980, the Navy notified MMDS that its proposal was unacceptable for failure to complete the blind benchmark test. MMDS representatives, on March 27, 1980, visited the Navy and requested the computer outputs for their own evaluation. They were advised that the Navy would not alter its position "unless MMDS could demonstrate that the original decision was in error." On March 31, 1980, MMDS presented the results of its review of the computer outputs. The Navy, by letter dated April 2, 1980, advised MMDS that the original decision was reaffirmed. Subsequently, MMDS filed a protest with the Navy by letter dated April 16, 1980. Then, on April 25, 1980, MMDS was advised by the Navy that "it was unable to commit to a firm and expeditious date for resolving the MMDS protest." Consequently, MMDS on May 1, 1980, filed a protest with our Office.

MMDS argues that its protest to the Navy on April 16 and its protest to GAO on May 1 are both timely. The Navy disagrees, stating that on March 26, 1980, MMDS was notified that its proposal was technically unacceptable. Moreover, on March 27, MMDS was, once again, advised of the decision and was given information that supported the Navy's determination. Accordingly, it is the Navy's position that a protest should have been filed no later than 10 working days from March 27, 1980.

While it is clear that on March 27, 1980, the Navy did advise MMDS that its proposal was determined to be technically unacceptable, it is also unmistakable that the Navy gave MMDS an opportunity to demonstrate that the Navy's determination was in error by furnishing the company with the computer outputs. Essentially, the Navy advised MMDS that unless MMDS could show that the Navy was wrong, the Navy was going to reject MMDS's proposal. At this point in time, there was no basis for protest since MMDS was given the opportunity to review the computer outputs and explain why it believed that the problems encountered by the Navy were not caused by MMDS's system. It was only after the Navy's response

to the MMDS presentation that the basis for protest was known. This response was a letter, dated April 2, 1980, which essentially advised MMDS that the problems encountered by the Navy were caused by MMDS's system and, therefore, its proposal was unacceptable.

Thus, this situation is unlike the circumstances in Brandon Applied Systems, Inc., 57 Comp. Gen. 140 (1977), 77-2 CPD 486, cited by the Navy, where the procuring agency gave no indication that its position was contingent on the protester's review of technical materials. Since no contingency existed, the position should have been reasonably considered to have been final unlike the inference to be drawn from the facts here.

MMDS filed its initial protest with the Navy on April 16, within 10 working days of receipt of the April 2 letter, as prescribed by our Bid Protest Procedures, 20 C.F.R. § 20.2(b)(2) (1980). Accordingly, its initial protest to the Navy was timely. Furthermore, MMDS's protest filed with our Office on May 1, 1980, was also timely since MMDS had been advised by the Navy on April 25 that the protest to the Navy had not been resolved and the Navy could not make a firm commitment as to when it would be resolved.

#### B. Conduct of Benchmark

The Navy could not complete MMDS's blind benchmark test because of alleged "MMDS system problems." Therefore, the Navy excluded the company's proposal.

MMDS, through its submissions, focuses its protest on one issue--MMDS's belief that its blind benchmark demonstration was conducted unfairly. At the outset, MMDS concedes that "it is difficult to determine what caused the MMDS system to perform improperly." As a matter of fact, MMDS advises that "without direct evidence MMDS must resort to circumstantial evidence, the computer console logs, and operator's memory to ascertain the cause of the failure."

MMDS states that the elements of a "fair unsupervised [i.e., blind] benchmark" test are:

1. "The operators should have had adequate (more than minimal) training in the logon procedures and operating characteristics of the MMDS system and the nature of the benchmark."
2. "The Navy should have had technical personnel present during the blind benchmark to correct operator errors and provide technical assistance as needed."
3. "The terminal equipment used during the benchmark should have been that which was specified in the RFP and used by field operations."

It is MMDS's position that the Navy failed to satisfy the three elements stated above. MMDS argues that since there were numerous operator errors, especially logon errors, e.g.--failure to a) restore the files, b) hit the "carriage return" key, and c) enter correct account number--one conclusion has to be that the operators participating in the blind benchmark did not participate in the supervised benchmark. Moreover, MMDS alleges that the operators failed to follow correct procedures when an incorrect account number was entered. The number of errors and failures to follow correct procedures lead MMDS to believe that there was "either a low level of competency or inadequate training or inadequate supervision." At the same time, MMDS maintains that the errors and failures demonstrate "the criticality of the need for qualified and supervised operators to conduct the benchmark test." In addition, MMDS states that the Computer Devices, Inc. (CDI), terminal used, which was not specified by the RFP, had an APL-type keyboard. MMDS contends that "the APL keyboard has a different keyboard and function keys than the terminal prescribed for the benchmark tests." MMDS objects to the use of a special keyboard since the benchmark test was intended to represent conditions at field activities and MMDS believes that this APL keyboard is "not normally used in the field." MMDS requests that its system be given another opportunity to complete the blind benchmark.

Based on the record before our Office, we believe that another opportunity would be inappropriate. As can be seen from the discussion that follows, we believe that MMDS has not refuted the Navy's position and, therefore, has failed to affirmatively prove its case.

With respect to MMDS's allegations concerning the terminal operators, we note that two operators encountered problems while attempting the blind benchmark runs. The Navy advises that these operators ran the blind benchmarks for all the vendors. Moreover, one of the operators "was a regular operator at the supervised benchmarks and conducted multiple training sessions for regular operators and alternates." The record indicates that there was no instruction except for logon and backspace procedures necessary for the supervised benchmark. Since the operators were familiar with these instructions, no additional instructions were given for the blind benchmark. In addition, the Navy submits that approximately 2,300 entries, containing three key strokes each, or 6,900 inputs, were made during the benchmark and only 23 errors, about a 1-percent error rate, were counted. The Navy insists that all these errors "were corrected and the test continued" until the perceived MMDS system failures required that the tests be ended before completion of all test requirements. We are not in a position to question the Navy's position that these errors were corrected.

As to the allegation that there was inadequate supervision from technical personnel, the Navy advises that the operators were supervised by a Navy computer specialist, having "13 years' experience in computers/teleprocessing." The Navy indicates that its specialist received instructions from MMDS personnel and was also in charge of running the supervised benchmark. Moreover, "she performed the identical function(s) for all offerors participating in this acquisition." In addition, we note that on March 18, MMDS's technical benchmark personnel were allowed by the Navy, "as a special favor," to observe one of the attempts to run the blind benchmark test. Thus, we cannot question the adequacy of the personnel supervision or that the attempts to complete the benchmark were terminated by properly authorized Navy employee(s).

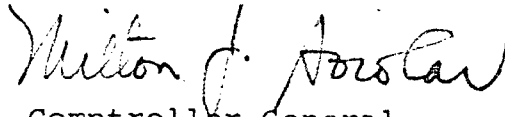
Concerning the terminals used for this blind benchmark, here, again, we find that the Navy's position has not been refuted by MMDS. We note that, contrary to MMDS's belief, two terminals, a CDI terminal and Texas Instruments (TI) terminal, encountered problems using two phone lines. However, we note that the RFP, section "D," paragraph 3.4.1, provides that "TI silent 700-series terminals would be supplied by the Navy and does not mention the CDI terminal." While the use of the CDI terminal was not expressly authorized by the RFP, we find no prejudice to MMDS, as both terminals were used for the other vendors' blind benchmark and the terminal specified by the RFP also encountered problems. Furthermore, at the time of the benchmark demonstrations, the Navy states that these terminals were currently in daily use and that they had no trouble prior to, during, or subsequent to the benchmark demonstrations. Moreover, the Navy submits that both operators were "fully familiar with the terminals in question because they are maintenance programmers."

MMDS also complains that the records of testing show that the Navy operators improperly allowed terminals to be dormant for 20-minute periods, resulting in proper automatic logoffs rather than system failures. The Navy denies that any terminal was dormant for a period up to 20 minutes. We must conclude that MMDS has failed to show that the Navy's position is in error.

In summary, the record shows that MMDS was given two opportunities to have Navy personnel verify the results of the supervised benchmark test--in other words, run the blind benchmark. The Navy refers to the period of March 10 to 18 as one opportunity and March 20 to 27 as the second opportunity. However, we note that within the former time period the Navy made two attempts to perform the blind benchmark but encountered several problems which prevented the completion of the test. The Navy advised MMDS of the problems and gave it a "second opportunity." During the latter opportunity, the Navy made three more attempts on different days but was still unable to complete the test. Some of the problems encountered were: terminals being logged off by the MMDS's Orlando operator, the mass storage was inoperable and there was no backup, files were not set up and the reinstatement of files took an extended period of time.

Thus, there appears to be no reason to question the rejection of MMDS's proposal.

Accordingly, MMDS's protest is denied.

A handwritten signature in cursive script, reading "Milton J. Forster".

For the Comptroller General  
of the United States