9 September, 1986

STAT [redacted]

John Holmes
Management Science America, Inc.
61 S. Paramus
Paramus, N.J. 07652

Dear Mr. Holmes:

Attached is a memo from my systems programming shop denoting their concerns with MSA security. This should be a good jumping off point for discussions with your systems people. If you could get comments from your folks on each of these points, we can get the dialogue underway.

STAT For more information, you may call me at [redacted]

Sincerely,

STAT [redacted]

CC: Bob Hunt

31 August 1986

STAT

MEMORANDUM FOR:

FROM:

SUBJECT: Draft- Questions for MSA

STAT

The following are a draft set of questions we would like to present to MSA to help clarify and correct any concerns we have with their packages. Some of these questions are related to our general concern with security and others relate to our ability to integrate their software packages into our environment.

1. There is an apparent lack of auditing capabilities with the MSA applications software. Will MSA provide audit trails, or at the very least exits that we could use to implement our own audit trails?

2. The need for a separate logon ID and logon process to MSA applications as distinct from the VM and IDMS/R is contrary to our intended direction. We would like a user to be authenticated only once, when signing onto the host operating system (VM), and that all subsequent authentications (IDMS/R or MSA) be performed by a 'trusted method' automatically such that a user only sees one signon process. We have the necessary exits in IDMS/R to perform a trusted signon, but it is not apparent that MSA provides the same capability. Does MSA provide exits during the logon process that we could take advantage of ?

3. There are no provisions within MSA software to provide security for Batch jobs. How can we get these required features? or, How do we disable this batch capability if it is not required?

4. The Information Expert (IE) component has job submission capability that must be integrated into our systems in secure manner. We must get a commitment from MSA to work this issue. It is not at all clear how we would do this at this time. Without solving this problem we introduce a significant security hole into our systems. It would be appear currently, that all jobs submitted via this mechanism would assume the same security characteristics and therefore we could not differentiate between users having distinct security profiles.

5. We have a major concern at this time that MSA does not consistently use IDSM/R to access data. Some MSA components, for example, issue their own OPEN macros to data files by-passing IDMS/R control all together. This by-passes any controls that we have built into the Central Version for IDMS/R. Can MSA define all instances in which they directly access data owned by IDMS/R? Does MSA do any type 1 SVC calls? What if any user exits are provided to audit data that is accessed directly ? What if any capability is there for security checking of data that is accessed directly?

6. The security architecture used by MSA requires that applications be provided with rather wide access to subchemas within systems in which a transaction is to run. Security is then provided with the online MSA software which narrows the view of data to the user. We have two significant problems with this approach:

   a. Any defined MSA user will be given rather broad access to data which is only narrowed when accessed using the MSA online software. Should the user gain access to the IDMS/R system with other packages (ie CULPRIT) he now has the broader view of data. How does MSA propose to provide consistent access of the data ? In our environment we need to limit access to the data regardless of the tools used to access it?

   b. It also appears that MSA user are provided read/write access of the MSA security rules. How does MSA propose to provide a secure environment if any can access and change the online security rules?

7. Interfaces to the Agency's print network will need to be developed. We need to have MSA commitment to provide the appropriate exits so that they can be developed. Can MSA identify to us the locations within their code wich generate print? Do they have a standard print exit that we can take advantage of?

8. Is MSA willing to provide system programing suppot to the Agency so that some of these issues can be resolved?

STAT