COMPUTER SYSTEMS ACCESS REQUEST

(COMPLETE ONLY IF VISITOR NEEDS ACCESS TO MSFC COMPUTER SYSTEMS)

Name (Please Print) - (Last, First, Middle):	Date(s) of Proposed Visit	
	From:	To:

5. SYSTEM(S) TO BE ACCESSED

System Name	Location	Access Level*	NASA Line Manager

6. APPLICATION(S) TO BE ACCESSED ON ABOVE SYSTEMS

Application Name	Access Level*	Application Owner

7. JUSTIFICATION FOR ACCESS

Exact Nature of Job Assignment Requiring Access (Include Grant, MOU, Contract or Agreement Number):

8. DESCRIPTION OF ACCESS CONTROLS PROPOSED TO BE IMPLEMENTED DURING REQUESTED IT SYSTEM/APPLICATION ACCESS

Physical (escort, locks, etc.):	File and/or System (passwords, folder/file limits, etc.):

9. CERTIFICATION / CONCURRENCE

Approval is granted for access to the Information Technology System(s) named, at the access levels defined, subject to implementation of adequate access controls, for the purposes and time periods described in this request.

IT System Line Manager (Printed or Typed Name and Signature):	Date:

Adequate IT system technical controls will be implemented to restrict system and/or information access as described in this request.

IT System Administrator (Printed or Typed Name and Signature):	Date:

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Section 799, Title 18, U.S. Code; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts, and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Foreign Visitor's Signature:	Date:

10. * ACCESS LEVEL DESCRIPTIONS (For further information see MPG 2810.1a)

PRIVILEGED ACCESS: Can bypass or modify the technical or operational system security controls (system-administrator level access, root-level account, or maintenance-account level access to all system controls and resources).

LIMITED PRIVILEGED ACCESS: Can bypass security controls for part of a system or application but not the entire system or application (access to controls for certain system resources or applications, excluding root-level or maintenance-account level accesses).

NON-PRIVILEGED ACCESS: Cannot bypass any security controls (user-level accesses to applications and limited systems resources only).