APPENDIX E: FACTORS AND ISSUES FOR APPLICATION MIGRATION

30 Jun 2004

This appendix presents baseline factors and potential issues for applications migrating to the NMCI environment.

Factor	Issue
1. The NMCI user desktop is Windows 2000.	• Are desktop applications Windows 2000-compliant?
2. The NMCI desktop will be implementing Office 2000.	• Are there any interfaces to Office applications (Word, Excel) that might be affected by the Office 2000 implementation?
3. User desktops have dynamic TCP/IP addresses.	• Are there any issues with changing TCP/IP addresses at the desktop?
4. Servers moving into the NMCI network will have a different TCP/IP address assigned.	• Is there any hard coded logic based on TCP/IP addresses? • Is there hard code in script files, configuration files, parameters, and database entries? • Do external systems reference your server by TCP/IP address?
5. Printers within the NMCI network have a different naming scheme than currently used.	• Are there any hard coded printer names embedded in the application or application scripts? • Are there any unique desktop printing requirements (e.g., color, duplex, high speed, plotter, scanners, etc.)?

Factor	Issue
6. An NMCI user logs on to NMCI with a user ID that is different from the current user ID structure. For single sign-on NT domains, it may be more reasonable at this time (until the majority of users are transitioned) to prompt the user for the ID and password rather than creating a pass through security mechanism.	• Are there hard coded tables that reference user IDs? • Are database permissions by user ID? • Are external interfaces sensitive to user ID?
7. NMCI users will be dialing into the NMCI dial-up servers. The TCP/IP address from the NMCI dial-up is different from that currently used.	• Do any issues relate to using a different dial-up facility than is currently in use? • Is anyone using PC/Anywhere or similar products?
8. A standard software configuration product locks the NMCI desktop down.	• Does the application install anything on the desktop? • Does the application install and uninstall properly in the Add/Remove program?
9. Is your application in compliance with the Navy Marine Corps Firewall Baseline Configuration?	
10. Is all the desktop software available and configurable for standard software distribution?	
11. If this application runs under an emulator, are there any anticipated issues (keyboard mapping) when the standard NMCI emulator (Reflections) is used?	

Factor	Issue
12. Are there any other applications that interface with your application under NMCI?	• Does your application update any data used by another application? • Does your application run upstream or downstream from another application that it might effect? • Does your application share files, access shared files, or use drive mappings across workstations or servers? • Does the application depend on portable browser-initiated code? JavaScript and Java Applets are supported in the NMCI environment, but ActiveX components are not. Active X components used on the browser (client) for application access by users outside NMCI will not be allowed by the NMCI boundary. • Does the application rely on desktop plug-ins? • Does the application need any supporting applications (such as web browsers, ORACLE, PowerBuilder, 4th Dimension, runtimes)?
13. Does your application encrypt data during transmission or for storage? Does your application use encrypted data for input?	
14. Users do not have administrative rights to their local machines.	• Developers must test applications with an account that does not have administrative rights.
15. The NMCI gold disk includes common desktop applications.	• As these applications may change over time, developers should develop to standard protocols and avoid the use of proprietary APIs.