DOS Connectivity Requirements

1. The Department of State (DOS) Sponsoring Bureau, along with DS/CTS/CMO and DS/IS/IND are responsible for ensuring that the below listed requirements are adhered to during the life of the contract;

2. The DOS Sponsoring Bureau must ensure that an ISSO and an Alternate On-Site ISSO are designated for this connection;

3. The Contractor facility must be secured for the protection of SBU data in accordance with the Foreign Affairs Manual and Physical Security Standards for Department of State Domestic Occupied Space;

4. All hardware and software used for this connection must be IT-CCB or local CCB approved and configured and managed in accordance with 12 FAM 620 and all applicable Department of State (DOS) computer security configuration guidelines. These documents are available on OpenNet at:

   - http://irm.m.state.sbu/sites/bmp/grp/sm/ITCCB/Pages/ITCCBHome.htm,
   - http://a.m.state.sbu/sites/gis/dir/fam/Pages/12FAM/12FAM.aspx and,
   - https://intranet.ds.state.sbu/DS/SI/CS/ESS/SCM/SCM%20Final%20Documents/Forms/AllItems.aspx.

Questions regarding the IT-CCB or local CCB can be sent to ITServiceCenter@state.gov. Questions regarding 12 FAM 600 and the security configuration guides can be sent to AskCTS@state.gov;

5. Citizens of specifically designated Human and/or Technical Intelligence Threat Countries may not develop, modify or perform maintenance on software developed for use on DOS computer systems, or on systems connected to DOS systems, without approval from DS/CTS/CMO;

6. The DOS network extension will have no other network connections;

7. IRM/OPS/ENM must ensure that network equipment:

   a. Have access restricted to only authorized personnel in IRM/OPS/ENM or other Department of State (DOS) cleared personnel authorized by IRM/OPS/ENM;

   b. Is secured to preclude tampering in:

      i. An approved server room; or

      ii. Mounted in an enclosure box with a DS-approved lock.

      iii. If applicable, servers used for this extension must be located in a server room that is constructed and secured in accordance with 12 FAH-10, Information System Security Controls and Procedures; and Physical Security Standards for Department of State Domestic Occupied Space;

DOS Connectivity Requirements

8. All Contractor personnel that have unescorted physical and/or logical access to DOS network workstations, servers and/or encryptors must be eligible for contract performance and meet the personnel security requirements as documented in the DD Form 254 Contract Security Specification Classifications and/or the contract document. The minimum of a Moderate Risk Public Trust certification conducted by the Bureau of Diplomatic Security is required for access to the network extension space and workstations;

9. Contractor personnel may not perform software development or maintenance on their DOS network workstations. OpenNet is a production environment and software application development and maintenance is prohibited;

10. Personnel (e.g. cleaning staff, building maintenance staff) that have not been cleared as described above, but require physical and/or logical access to DOS network workstations and/ or the room housing the server and/or encryption equipment, must be escorted at all times by a cleared Contractor employee;

11. The IT Service Center or responsible IT office must ensure that individual PKI card/PINs are issued to authorized users in accordance with 12 FAH 10 H-130.

12. All Contractor personnel with physical and/or logical access to DOS network workstations, servers and/or encryptors must be given a briefing by the ISSO to ensure that each employee understands their obligations and requirements to adhere to established DOS security policies concerning the use of Automated Information Systems;

13. The Contractor must agree that the DOS network connection is subject to on-site and remote auditing, scanning and testing by DS/SI/CS and recurring inspections by DS/IS/IND as deemed necessary by DS. Audits, scans, testing and inspections will help to assess the compliance of this DOS network connection with DOS requirements;

14. All media (e.g. hard drives, CDs) used on workstations and/or servers connected to DOS network must be returned to the Sponsoring Bureau when: (a) the contract has terminated; (b) the media is no longer needed; or (c) the media is inoperative. The Sponsoring Bureau may reformat the media for continued use within the Bureau or have the media destroyed;

15. All personnel with access to the DOS network must report any security incidents to the Contractor Facility Security Officer (FSO) in accordance with 12 FAM 553, Reporting of Security Incidents, and 12 FAM 590, Computer Security Incident Program. 12 FAM 553 incidents are reported to DS/IS/APD. 12 FAM 590 incidents are to be reported to the designated ISSO for reporting to the DS CIRT and DS/IS/APD. 12 FAM 632.1-7 incidents are to be reported to the designated ISSO. Contractor FSO must promptly provide a report of any security incident or violation to DS/IS/IND and DS/SI/CS;

16. Approval for a DOS network extension is valid for up to one year from the date of the original DS/SI/CS Approval Memo. The DOS Sponsoring Bureau must request annual extensions for the Contractor, as necessary, a month ahead of time and provide immediate notification to DS/CTS/CMO and DS/IS/IND if the requirement for OpenNet ceases, or the contract ends before the year is up;

DOS Connectivity Requirements

18. Any changes to the configuration of this extension (e.g., adding additional workstations, relocating existing workstations) or any changes to the physical structure of the space require prior approval by DS/CTS/CMO and IRM/IA.

19. DOS network connectivity approval is only for the Contractor location stated in this OpenNet request. If the Contractor performance location changes, the DOS Sponsoring Bureau must submit another request to DS/CTS/CMO for the new location. If at any time DS finds that the above listed security requirements are not being met, the connection will be subject to termination.