Appendix U Protective Security Measures for Applications and High Sensitivity Protocol

1. NYSHIP Decision Support System (DSS) Security Measures

The DSS Security Measures document is a supplement to the Department of Civil Service (Department) Information Security Policy requirements that includes detailed requirements specific to the DSS Project. The following protocol identifies detailed requirements for the DSS.

1.1 Assumptions

1. The DSS will comply with all requirements in the Department Information Security Policy, dated October 1, 2007.
2. The DSS application is classified with the following sensitivity ratings:

- Confidentiality = High
- Integrity = High
- Availability = High

1.2 Account Management

1. The DSS will integrate with the Department authentication and authorization infrastructure.
2. Shared privileged accounts will not be used.
3. Privileged account names will not reveal privilege level.
4. Privileged account passwords must be changed every 90 days.

1.3 Log Data

1. Lockout data must be logged.
2. Additional data that must be logged includes authentication events or unsuccessful resource access events. Data to be logged for each of these categories is:

   i) Authentication Events. All authentication events must be logged. Authentication events can be either successful or unsuccessful. The data to be logged for authentication events is:

      (1) account or User ID;

      (2) the type of event;

      (3) an indication of success or failure of event;

      (4) the date and time of event;

      (5) identification of the source of event such as location, IP address, terminal ID or other means of identification.

   ii) Unsuccessful Resource Access Events. The data to be logged must include:

      (1) account or User ID;

      (2) the type of event;

      (3) the date and time of event;

      (4) the resource;

(5) identification of the source of event such as location, IP address, terminal ID or other means of identification.

iii) Privileged Account Use:

(1) Account ID

(2) date/time

(3) successful/unsuccessful

(4) identification of the source of event such as location, IP address, terminal ID or other means of identification

iv) System starts and stops

v) Hardware attachments and detachments

vi) Successful and unsuccessful access to log files. The data to be logged must include:

(1) account or User ID;

(2) the type of event;

(3) an indication of success or failure of event;

(4) the date and time of event;

(5) identification of the source of event such as location, IP address, terminal ID or other means of identification

1.4 Log Requirements

1. Syslog logs are preferred.
2. Logs must be protected from alteration by any user.

1.5 Backup and Restoration

1. The location of both the application backup media and the data backup media must be off-site.
2. Backup media must be encrypted.
3. The backup restoration method must be tested and validated to enable all the technical processes of the restoration to be completed within 24 hours of all of the technology being in place.
4. Changes to the technology require a re-test of the restoration process.

1.6 Network Protections

1. The required connectivity method is via the Internet to a Department-approved or Department-provided Virtual Private Network (VPN) device.

2. Strong encryption will be used while data is in transit.
3. The DSS will deploy antivirus and an intrusion prevention software.
4. All servers at the DSS will be uniquely identifiable by a static IP address. The ITS data center will use Civil Service provided IP addressing, or be capable of using Network Address Translation.
5. The vendor will work with the Department to provide a seamless and secure interface to the vendor's application from the Department's web site.
6. The firewall and any related security systems for the DSS will be subject to audit by Civil Service.
7. The DSS will submit network drawings and data flow diagrams for all systems. The firewall and DMZ policies will be subject to Civil Service review and approval.