SECTION J

ATTACHMENT J-3: INFORMATION SYSTEM SECURITY PLAN TEMPLATE

Insert Company Name

Information System Security Plan

This document is a template and should be completed per guidance provided by the requirements listed in Section 2 below. Areas in italics or highlighted must be completed.

Review and Approvals

REVIEWED BY:

______________________________           __________________________
Information System Owner         Date
Typed First/Last Name

______________________________           __________________________
EMCBC Information System Security Manager (ISSM)         Date
John Muskoff

______________________________           __________________________
WVDP Federal Project Manager         Date
Typed First/Last Name

APPROVED BY:

______________________________           __________________________
EMCBC Authorizing Official Designated         Date
Representative (AODR)
Ward E. Best, EMCBC ADIRM
System Security Plan

1. **Purpose:**
The purpose of the System Security Plan (SSP) is to define system components, operational boundaries, and roles and responsibilities for managing the system.

2. **Requirements and Guidance:**
   - Federal Information Security Management Act (FISMA) 2002
   - OMB Circular 130-A, Management of Federal Information Resources
   - NIST Special Publication 800-53, Rev 4 – Security and Privacy Controls for Federal Information Systems and Organizations
   - DOE Cyber Security Program, DOE O 205.1B
   - NIST Special Publication 800-61, Rev 2 – Computer Security Incident Handling Guide
   - NIST Special Publication 800-30, Rev 1 - Guide for Conducting Risk Assessments
   - NIST FIPS-199 Standards for Security Categorization of Federal Information and Information Systems

3. **Information System Name/Title:**
   - *ABC Company, Inc.* General Support System (GSS)

4. **Information System Type:**
   - Indicate if the system is a major application or a General Support System. If the system contains minor applications, list them in Section 9. General System Description/Purpose. *(This should be a General Support System comprised of several individual stand-alone systems.)*

<table>
<thead>
<tr>
<th>Major Application</th>
<th>General Support System</th>
</tr>
</thead>
</table>

5. **Information System Categorization:**
   - Identify the appropriate system categorization using FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. *(Categorizations below are examples and should be changed as necessary.)*
6. **Information System Owner:**
   - Position with responsibility for the information system. *(Note: This document should only reflect roles by position, not individual names. Assignment of roles by name is done through an Appointments Memorandum, which can be changed without a formal review process, unlike the SSP.)*

7. **Authorizing Official:**
   - EMCBC Authorizing Official Designated Representative (AODR):
     Ward E. Best, EMCBC Assistant Director, Information Resource Management (ADIRM)

8. **Assignment of Roles and Responsibilities:**
   - List roles and associated responsibilities *(Contracting Officer’s Representative (COR), Authorizing Official (AO), Information System Security Officer (ISSO), Information System Security Manager (ISSM), Information System Owner (ISO), and other roles as applicable per NIST SP 800-18 Rev 1. This table is only a reference and can be removed or modified as necessary.)*

<table>
<thead>
<tr>
<th>Title</th>
<th>Assigned To</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Contracting Officer’s Representative   | COR         | Agency Project Manager providing direction and guidance to Contractor  
| (COR)                                  |             | Assists COR with regard to contractual matters                                                                                              |
| DOE Authorizing Official (AO)          | AO          | DOE official approving system security plans,  
|                                        |             | Authorizes operation of an information system,  
|                                        |             | Issues an interim authorization to operate the information system under specific terms and conditions, or  
|                                        |             | Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist. |
| Information Owner                      | CIO         | Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),7  
|                                        |             | Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides,  
|                                        |             | Decides who has access to the information system and with what types of privileges or access rights, and |
West Valley Demonstration Project
Development of a Supplemental Environment Impact Statement
Draft Request for Proposal No. DE-SOL-0009226

9. **General System Description/Purpose:**
   - Describe the function or purpose of the system and the information processes.
10. **System Boundary:**

- Provide a general description of the technical system. Include the primary Hardware and Software (items listed in table are examples only and should be modified as needed).

The following system categorization is based on FIPS-199.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Compile and create reports</td>
</tr>
<tr>
<td>Firewall</td>
<td>Protect systems from external sources</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>Operating System</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td></td>
</tr>
<tr>
<td>McAfee</td>
<td>Anti-virus protection</td>
</tr>
<tr>
<td>Adobe Acrobat Reader</td>
<td>Read portable document format (.pdf) files</td>
</tr>
<tr>
<td>Java</td>
<td>Mobile code for viewing WWW content</td>
</tr>
<tr>
<td>Adobe Flash Player</td>
<td>Multi-media Software</td>
</tr>
</tbody>
</table>

- Include a network diagram that illustrates how the stand-alone systems connect to the Internet and share information.

11. **System Configuration Management:**

- The Center for Internet Security (CIS) has established benchmarks for various operating systems and tools for assessing these benchmarks. The ISSO will establish minimum baseline requirements with respect to the CIS benchmarks and obtain approval from the ISSM. *(CIS is listed as an example, any baseline standard may be used.)*

- System Updates (identify how HW and SW is updated)
- System Back-ups (describe the system and data back-up procedures)

12. **System Interconnections/Information Sharing:**

- **Interconnections are not authorized.** Describe how information is shared (e.g., via email, CD/DVD, etc.).

13. **Minimum Security Controls:**

- The following minimum security controls have been selected for the information systems processing work under contract *(insert contract number)*. The contractor will perform a self-assessment on these controls and report to the Contracting Officer’s Representative (COR) and the ISSM.

1. General Policy Control: This document, and any documents associated with or supportive of this document, is reviewed and updated annually.
2. Access Control:
   a. Separate Account Types
i. Standard user accounts will be used for the routine use of the information systems
ii. Administrator accounts will be established for performing tasks requiring elevated privileges (e.g., installing and updating third-party software)

b. Establish a policy for disabling accounts upon termination or transfer of personnel that will ensure data integrity

3. Security Awareness & Training:
   a. All users will take annual security awareness training
   b. Training records will be maintained

4. Audit & Accountability – not applicable

5. Security Assessment & Authorization:
   a. The EMCBC will determine security controls
   b. The EMCBC will evaluate security controls periodically
   c. The Plan of Action & Milestones (POA&M) will be established to track issues identified as non-compliant with the SSP

6. Configuration Management:
   a. Apply CIS benchmark recommendations to obtain a minimal score of 80%
   b. Software must be approved by the Information System Security Officer (ISSO) prior to installation

7. Contingency Planning:
   a. Establish a methodology for performing data back-ups
   b. Annually test or validate data back-ups and validate that back-ups are being performed

8. Identification & Authorization:
   a. Users have unique accounts (shared accounts are not authorized)
   b. Passwords must be at least 12 characters and meet complexity requirements in accordance with Microsoft’s local group policy (upper case letter, lower case letter, special character and number)
   c. Passwords must be changed every 180 days
   d. The last 5 passwords cannot be re-used
   e. Account will be locked out after 5 consecutive invalid logon attempts. Lock-out duration is 15 minutes and the lock-out timer reset is 2 hours.

9. Incident Response:
   a. Incidents will be reported to the EMCBC Information System Security Manager (ISSM)

10. System Maintenance:
    a. Maintenance performed by vendors will be approved by the ISSO

11. Media Protection:
    a. Media will be marked appropriately based on content

12. Physical & Environmental Protection:
    a. Laptops shall be accounted for and assigned to individuals
    b. Conduct annual inventory of all equipment

13. Security Planning:
    a. Establish Rules of Behavior and ensure all users acknowledge

14. Personnel Security:
    a. Establish personnel sanctions for individuals who violate security policy
b. No foreign nationals shall be granted access to the system or information without the express written approval of the AODR

15. Risk Assessment:
   a. Review and verify risk categorization annually
   b. Re-establish configuration benchmarks annually as prescribed in Item 6, Configuration Management

16. System & Services Acquisition:
   a. Obtain documentation for the information system, system component, or information system service that describes secure configuration, installation, and operation of the system, component, or service

17. System & Communication Protection:
   a. System shall be protected by anti-virus software
   b. System shall be protected by a software firewall (e.g., Microsoft)
   c. Ensure most recent software patches and updates are installed on the Operating System
   d. Ensure most recent version of third-party software is installed (e.g., Adobe Flash, Acrobat Reader, McAfee, etc.)

18. System & Information Integrity:
   a. Shall provide for SPAM protection filtering
   b. Shall provide for malicious code protection through the use of anti-virus software