# C-SCRM QUESTIONNAIRE

**SUPPLIER INFORMATION**

| | | |
|---|---|---|
| Company Name: | | |
| Address: | | |
| City: | State: | Country (if outside USA): |
| Name & Title of person completing this assessment: | | |
| Phone: | Email: | |

| | |
|---|---|
| **FAR 52 204-21 Basic Safeguarding of Covered Contractor Information Systems** | |
| DESCRIBE HOW YOUR ORGANIZATION DOES THE FOLLOWING: | |
| (i) | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). |
| (ii) | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. |
| (iii) | Verify and control/limit connections to and use of external information systems. |
| (iv) | Control information posted or processed on publicly accessible information systems. |
| (v) | Identify information system users, processes acting on behalf of users, or devices. |
| (vi) | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| (vii) | Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. |
| (viii) | Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. |
| (ix) | Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices. |
| (x) | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. |
| (xi) | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. |
| (xii) | Identify, report, and correct information and information system flaws in a timely manner. |

# C-SCRM QUESTIONNAIRE

| | |
|---|---|
| **FAR 52 204-21 Basic Safeguarding of Covered Contractor Information Systems** | |
| DESCRIBE HOW YOUR ORGANIZATION DOES THE FOLLOWING: | |
| | |
| (xiii) | Provide protection from malicious code at appropriate locations within organizational information systems. |
| (xiv) | Update malicious code protection mechanisms when new releases are available. |
| (xv) | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. |
| (xvi) | Verification of any security-related 3rd party evaluation and results of that evaluation. |

**Date:**

**Signature (person completing assessment)**

*This report may be shared with the Dept. of Energy (DOE) Office of Science as requested.*

| | | |
|---|---|---|
| | | |
| Reviewed by: | Organization: | Date: |
| | **Rating** | |
| Green: □ | Yellow: □ | Red: □ |