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

**Helpful Resources:** [**NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**](https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final)

[**Federal Trade Commission: Cybersecurity Basics & Small Business Resources**](https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics)

|  |
| --- |
| **Summary of assets on your network that store/process/transmit Controlled Unclassified Information:** |
| **FAR 52 204-21 Basic Safeguarding of Covered Contractor Information Systems** |
| DESCRIBE HOW YOU MEET EACH REQUIREMENT. ATTACH SUPPORTING EVIDENCE AS APPROPRIATE: |
| 1. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). |
| 1. Limit information system access to the types of transactions and functions that authorized users are permitted to execute. |
| 1. Verify and control/limit connections to and use of external information systems. |
| 1. Control information posted or processed on publicly accessible information systems. |
| 1. Identify information system users, processes acting on behalf of users, or devices. |
| 1. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| 1. Sanitize or destroy information system media containing Federal Contract Information (or Controlled Unclassified Information) before disposal or release for reuse. |
| 1. Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. |
| 1. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices. |
| 1. 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. |
| 1. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. |
| 1. Identify, report, and correct information and information system flaws in a timely manner. |
| 1. Provide protection from malicious code at appropriate locations within organizational information systems. |
| 1. Update malicious code protection mechanisms when new releases are available. |
| 1. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. |

     \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date: Signature** (President/Owner or accountable cybersecurity representative)

*This report may be shared with the Dept. of Energy (DOE), National Nuclear Security Administration (NNSA), and with other DOE/NNSA operating subcontractors.*

|  |  |  |
| --- | --- | --- |
| **For NTESS/Sandia Internal Use Only** | | |
| Reviewed by: | Organization: | Date: |
| **Status** | | |
| Approved: | Conditional: | Not Approved: |