

**CUI Cybersecurity Site Data Summary**

**General Directions:** Please answer questions with whatever information is readily available. Typically, data will not be available for all questions. Do not delay the project for unavailable data but do provide as much information as can be readily obtained.

**Company Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Site Name and Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Point of Contact this Location: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Contact Phone & Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Total number of employees at this site: \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Total number of employees with remote access to this site: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Short Description of Business Activities:**

Initial Information–Where information requested is unavailable, mark “unknown”.

1. Identify personel that will be available for onsite assistance for completing the risk management program. One person may fill multiple roles.
	1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Compliance Officer – able to sign and adopt policies
	2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Human Resources Manager – able to hire and train staff
	3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Operations Manager – authorized to operate physical plant
	4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_IT Manager – able to install and manage data handling equipment
	5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_IT Consultant – resource for difficult technical issues
2. For this site, is a current Network Topology Diagram available, (Y / N). If yes, please attach. (Note: the free software program LibreOffice has a Visio clone drafting program that makes is simple to turn a pencil drawing into a useful diagram. A youtube video detailing the process is at <https://www.youtube.com/watch?v=4laWj95PimI> )
3. Create Device Inventory of all devices connecting to the network or accessing protected information (PI) *(i.e. PCs, Smart phone, Mobile Device, etc.)* Please append Inventory to this form.
	1. How many and what type of computers or servers or other devices?
		1. \_\_\_\_Windows,
		2. \_\_\_\_Linux,
		3. \_\_\_\_Mac
		4. \_\_\_ Android
		5. \_\_\_ iOS
		6. \_\_\_Other
4. Software Summary – major software packages
5. Network Details - Are computers part of an Active Directory domain? (Y / N)

7. Firewalls, including next-generations Firewalls (NGFW) and/or Intrusion detection/intrusion prevention systems (IDS, IPS)? (Y / N)

a. If Yes, Manufacturer / Model \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b. If Yes, Summarize Recent experience

Number of Days in Dataset \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Total Number of Intrusions \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Total Number of Alerts \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Total Number of Warnings \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Total Number of Virus Detections \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Do you allow remote access? If so, how? (Check all that apply)

1. \_\_\_ Virtual Private Network (VPN)
2. \_\_\_ SSH
3. \_\_\_ Terminal server
4. \_\_\_ Other

9. Cloud-based servers (Y / N) Manufacturer / Type \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. Cloud-based storage (Y / N) Manufacturer / Type \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11. Cloud-based applications (Software as a Service) (Y / N) Manufacturer / Type \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12. Staff Experience

 Total Number of People with Access to Protected Information \_\_\_\_\_\_\_\_

 Total Number of People with Access and < 1 year Experience \_\_\_\_\_\_\_\_