

**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: Bobby Lee Welding – Prototype Design and Fabrication**

**Site Name and Address: BLW Associates, 200 Wolf Road Hiram, GA**

**Point of Contact this Location: Bobby Lee**

**Contact Phone & Email: 770-381-9229, bobbylee@blw.net\_**

**Total number of employees at this site: 15**

**Total number of employees with remote access to this site: 2**

**Short Description of Business Activities:**

Bobby Lee Welding (BLW) began as a simple manual welding job shop. After upgrading to computer-controlled welding units, BLW was able to enter the more lucrative business of fabricating high precision components for DOD and aerospace applications. With the purchase of ACME Design Solutions, LLC, BLW is now able to modify and produce either single examples or small lots of high precision components.

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. Bobby Lee \_\_\_\_\_\_\_Compliance Officer – able to sign and adopt policies
	2. Bobby Lee \_\_\_\_\_\_\_Human Resources Manager – able to hire and train staff
	3. Bobby Lee \_\_\_\_\_\_\_Operations Manager – authorized to operate physical plant
	4. Tommy Lee \_\_\_\_\_\_IT Manager – able to install and manage data handling equipment
	5. \_\_N/A\_\_\_\_\_\_\_\_\_\_\_IT Consultant – resource for difficult technical issues
2. For this site, is a current Network Topology Diagram available, (Y). If yes, please attach. (Note: the free software program LibreOffice has a Visio clone drafting program that makes it 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. List of employees:

Owner: Bobby Lee

IT Manager: Tommy Lee

Administrator: Sarah Lee

Remote workers: Brandon Lee (accountant) and Jimmie Lee (Tech Crew)

Production: Mike Evans, Matthew Evans, Luke Hunter, Chris Smith, Billy Morrison, James Tyler

Design: Cindy Wells, Johnny Hughes, Lucas Granger, George Shaw, Will George, Riley Mortar

1. 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?

i. \_9 Windows, Win 10 workstations with Office 365

ii. \_6 Linux, welding machine controllers

iii. 0 Mac

iv. \_17 Android phones with full device encryption and Office 365

v. \_0 iOS

1. Software Summary – major software packages

MS Office

Quickbooks

AutoCad

WeldPro

1. 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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Fortinet WiFi 50\_\_\_\_\_\_

b. If Yes, Summarize Recent experience

Number of Days in Dataset \_\_\_\_\_\_\_\_\_30\_\_\_\_\_\_

Total Number of Intrusions \_\_\_\_\_\_\_\_\_4\_\_\_\_\_\_

Total Number of Alerts \_\_\_\_\_\_\_17\_\_\_\_\_\_\_\_

Total Number of Warnings \_\_\_\_\_\_\_\_\_\_120\_\_\_\_\_

Total Number of Virus Detections \_\_\_\_\_\_\_\_\_\_3\_\_\_\_\_

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

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

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

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

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

12. Staff Experience

 Total Number of People with Access to Protected Information \_\_\_\_17\_\_\_\_

 Total Number of People with Access and < 1 year Experience \_\_\_\_\_1\_\_\_



Network Security Auditing at Bobby Lee Welding

Auditing of network and computer functions is a major part of the DFARS cybersecurity program. Security auditing for the Bobby Lee Welding computer network shown at right involves two basic tasks;

1. Perimeter monitoring using a Fortinet Unified Threat Management (UTM) device.
2. Windows™ 10 monitoring using the built in Windows™ security policy (secpol.msc) and event viewer functions (eventvwr.msc).

Perimeter monitoring is straightforward using the Fortinet reporting tools. The UTM logs attempted viruses, intrusions, warnings and alerts. This data is used as part of the ACRMS™ auto calculated NIST 800-30 risk assessment required as part of the DFARS 252.204-7012 System Security Plan (SSP).

To set a security policy on a windows 10 machine click Windows™ key + R and enter secpol.msc. Clicking on “Local Policies” brings up a large number of options, as shown below. Audit Policy gives useful information about various events and functions.



Periodic review of the audited policies is best done using the built-in Windows 10 Event Viewer. Click on Windows™ + R and enter eventvwr.msc.



Open the “Windows Logs” tab as shown below.



Typically the security logs and application logs will be of most interest.

