Category	Number	Questions	Response (Yes, No, Short Answer)
IDENTIFY			
	1	Do you conduct an inventory of all hardware?	Yes
	2	Do you conduct an inventory of all software?	No. Each laptop has a standard install of Office 365, Nord VPN, and Zoom. Most have Matlab installed as well. Plus a number of folks have TikTok installed to share office memes. However, employees can install other software if they want to.
	3	How often do you update the inventory?	It is updated every 6 months, or if major purchases are made.
	4	Do employees undergo a background check when hired?	Yes. A standard background/credit check is completed for hiring.
	5	Do employees require ID badges?	They are given badges, but all employees are recognized by everyone else since we are a small organization.
	6	Do visitors require ID badges?	There are red visitor badges. In addition, anyone visiting the engineering spaces must be escorted for life-safety reasons.
	7	How often do you do a security audit or assessment?	This is the first one.
	8	Is it possible to obtain previous assessment reports?	N/A
PROTECT			
	9	How often are laptops and workstations updated?	They are set to automatically update.
	10	How often are network devices updated?	If there are critical issues, PITA patches them on their next trip over. This has happened 2-3 times. Otherwise, they are not regularly updated.
	11	Do your laptops and workstations have antivirus installed?	They use Microsoft Defender
	12	Do your laptops and workstations have firewall software installed?	They use Microsoft Defender as their firewall
	13	Does your network have a firewall installed?	Yes. There is a Juniper SRX firewall.

	14	How often are backups performed?	Every few weeks
	15	Are backups stored on site, or off site?	There are hard drives that are stored in the server room for on-site backups. PITA also does some kind of offline backup. (I will request more information.)
	16	How are laptops protected when not in use?	They are kept on desks in the office, or taken home by employees.
	17	Do you use encryption (password protect) the data on the laptops (may be called BitLocker) or workstations?	Yes. BitLocker is enabled on the laptops.
	18	Are backups encrypted (password protected)?	No.
	19	Do passwords have to be changed on a regular basis?	They are changed on an annual basis for the Windows login.
	20	Do passwords have to be a particular length, and use different kinds of characters (lower, upper, digit, etc.)	Yes. They follow NIST guidelines to be 8 characters long, with at least 3 types for upper, lower, number, or symbol
	21	Do employees use their personal devices (phones, home laptops, etc.) to access NARO resources?	Yes. They can log in through the VPN, or they can access their email and work documents through the Office 365 portal.
	22	Do you have written cybersecurity policies?	There are some written policies, but they are not comprehensive.
	23	How often are the policies updated?	They get updated approximately every year.
DETECT			
	24	Do you have a way to detect attacks against your network and systems?	Microsoft will notify if there are malicious emails or attachments. Google also scans files when they are transferred via Google Drive.
	25	Do you log system and network activity?	Yes. They are forwarded to a central logging system.
	26	How often are the logs reviewed for malicious activity?	PITA looks at the logs when they come on site.
	27	Do you conduct internal assessments/audits to identify any issues?	N/A
RESPOND			
	28	Does your company have an incident response plan?	Yes.

	29	How often is the incident response plan updated?	It has not been updated since it was created 18 months ago.
	30	Have you every used the incident response plan?	Yes. It has been used a few times, and PITA has used it as well when something has happened.
	31	Do you ever conduct an “after action review” after an incident?	Just informal discussions. It is usually accidentally clicking on a phishing email.
	32	Do you every update policies based on an incident.	No. However, reminders are often sent out to employees to not click on things, etc.
	33	Do you have remote monitoring of systems, including the ability to remotely delete any information on the laptops?	Yes.
RECOVER			
	34	Have you ever had to restore data from your backups?	Yes. Several times. Usually through accidental deletion – or dropping of a laptop.
	35	Do you keep spare laptops on hand in case one is stolen or damaged?	There are 1-2 older laptops that still work kept in a storage cabinet.
	36	Do you carry cyber insurance?	No.
TRAINING			
	37	Do your employees receive cybersecurity training, such as detecting phishing emails?	Yes. When employees are hired, they are required to take multiple cybersecurity training courses from LinkedIn Learning.
	38	Do you conduct any phishing email training?	No.
	39	Do you brief employees on cybersecurity policies?	Yes. They are all briefed during their on-boarding process.