Q1. As you are aware, electric power is vital to all aspects of all life. The 2003 Northeast blackout is an example of its criticality. Use web resources and your imagination (state the assumptions) to describe the security services dimension of a desirable IA system for a power company.

When it comes to creating a well-rounded and desirable IA system for a power company it is vital to remember the CIA Triad. One of the major goals when it comes to an IA system is to ensure that processes are set in order to protect or meet the triad: confidentiality, integrity, and availability. One model that addresses such things is John McCumber's model where he highlights ways to protect information systems. When it comes to a power company it is safe to assume that these rules and frameworks can enhance its security. Preventing attackers or threat actors from degrading or hampering performance. In order to meet the CIA triad many things can be set in place and are set in place to deter threat actors. Such things can be access controls that limit the ability of unauthorized users to operate or interact with certain aspects of a business. This helps prevent any compromised credentials from being used to have full rain over a company. Preventing access and having strict access controls prevent insiders and outside attackers from having privileges they otherwise should not. Another major thing that should be implemented when it comes to power companies is physical security. This can prevent bad actors from tampering with machinery or systems that are critical. One major thing that would be wise to include in an IA system is an incident response plan. This would be valuable in an incident such as the 2003 blackout. If an incident response plan is set then it would make the princess of getting things back to working order more efficient. Understanding the political sphere and what policies interact with the power company is important to ensure that regulations are being abided by.

Q2. You have asked your system administrator to provide you with measures on organization's computer system availability and failures. The administrator reports to you that there were four failures and that the availability was satisfactory. What is wrong with these metrics? Use the material provided in the metrics papers and slides to critique---don't simply write some English sentences that anyone else could make. Instead, provide a good analytical critique using the material provided.

The metric lacks detail and further information that would support the metrics that were given. The issue with this metric is it doesn't establish a timeline or a length of time that has been measured. Which makes it hard to compare it to other metrics that may be gathered. It also fails to account for the length between each incident and if there was any downtime. The main point in having metrics is being able to use them to compare results or measurements that have been gathered. This involves having some form of

baseline or set perimeter when it comes to measuring. The metric given lacks surrounding measurements which makes the metric rather useless.

Q3. Using the web provide a list of ten organizations that are using CVSS to classify/quantify the potential effect of vulnerabilities on their information systems.

https://www.first.org/cvss/v2/adopters

1. Amazon
2. McAfee
3. HP
4. Oralce
5. IBM
6. Cisco
7. Microsoft
8. U.S. Department of Homeland Security
9. NIST
10. Skype