**EMCS2600: The Future of Cybersecurity: Technology and Policy**

Assignment: Module 6 Review Questions

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

Question 1: In at most 200 words contrast the different approaches taken by the FCC planning guide with the first reading by Bau and Mitchell.

The FCC Planning guide, in summary, is a walled garden/moat defense approach. They instruct organizations to identify what is valuable and “hide it” from threat actors. The steps outlined in the document can be summarized as inventory, identify and protect, control access, secure and back up. In contrast, the article by Bau and Mitchel is deeply concerned with modeling, which includes threat modeling, security modeling, network behavior modeling and other defenses that are based on understanding the methods of threat actors. The first approach proposed by the FCC is definitely the traditional way of approaching security derived mainly from the world of physical security. The article by Bau and Mitchel is a more modern approach that takes into consideration the countless ways that attackers are able to supersede the wall/moat type defenses. Neither these approaches take into consideration the serious risk that an organization creates when they knowingly or unknowing create homogeneous and biased engineering teams.

Question 2: What do you consider the three most important topics in the NIST Cybersecurity Framework (in at most 200 words)?

“Coordination of Framework Implementation” as outlined in section 2.4 in very important. Often in western thinking, people look for some “thing” whether it is a model, technology or policy to provide security. It is refreshing to see some recognition that coordination from different parts of the business is fundamental to the success of the security plan. Robotically implementing security without serious self-reflection is dangerously easy when the team implementing the system is not diverse. People with privilege tend to do this more often because unlike the people they oppress, they are often not forced to think outside of their own perspective. Coordinating is the first step in canceling out bias. Section 3.3, “Communicating Cybersecurity Requirements with Stakeholder” falls in alignment with section 2.4 and is immensely critical to a successful plan. If there is no common language that arises out of the coordination step, there will be no way to measure the effectiveness of the efforts put forth by the team Lastly section 3.6 is important because businesses should coordinate on protecting themselves but should also have an overarching interest in protecting our civil liberties, without which the freedom to operate a business might not exist.