**Applying The NIST Cybersecurity Framework to Pen-Testing**

*From your readings of pages 1 - 21 of the NIST Cybersecurity Framework, what benefit can organizations gain from using this framework, and how would you use it at your future workplace?*

After reading about the NIST Cybersecurity Framework, it is clear there are many ways organizations can benefit from using the framework. Because the Framework is adaptable and can be used no matter if the organization is in the private or public sector—or even which country, for that matter—it is easy to implement. Although 2014 seems like decades ago in terms of cybersecurity, the functions can be applied in the same way, as they mentioned how the Framework is technology neutral. This would make it so the Framework can be used not only from one organization to the next but can also be applied to one specific area or department of an organization.

The jobs I am most interested in involve "in the field" work, such as a Penetration Tester. I decided to switch from the Computer Science program to Cybersecurity because I realized that I wasn't very interested in software development or similar roles. In the role of a pen-tester, the Framework would be a huge help in the way a problem is assessed and also in creating and executing a plan of action. The Framework would be useful in deciding which assets are the most critical to the organization. Once this is known, they can then begin the testing of hardware (such as workstations), software (such as firewalls), and the weakest link in any organization—the humans within the organization. After running tests and trying to do things like gaining

unauthorized access/privilege escalation, altering security settings, or phishing employees with critical access, the pen-tester could then use the functions Respond and Recover. By using these functions, it would be easy to see if the organization is set up to respond quickly and make sure that they have current backups in place, ready for a major incident that would encrypt or wipe critical data.

Using the NIST Cybersecurity Framework, anyone in any cybersecurity role can come up with a plan of action, both preemptively and reactively, to many situations. By applying different tasks to each function within the Framework, it would help with visualizing the plan from start to finish. Not only would this be a great way to make documenting your findings easier, but it also would look good to the organizations you would be working for.