1)

a) See Spreadsheet

b) See Spreadsheet

c) Ranking:

   i) Security Assessment
   ii) Identification and Authentication
   iii) Systems and Communications Protection
   iv) Access Control
   v) Asset Management
   vi) Personnel Security
   vii) Maintenance
   viii) Physical Protection
   ix) Recovery
   x) Incident response
   xi) System and Information Integrity
   xii) Risk Management
   xiii) Audit and Accountability
   xiv) Situational Awareness
   xv) Configuration Management
   xvi) Awareness and Training
   xvii) Media Protection

d) Explanation : I split the domains into three categories, with *threat prevention* being the most important domains, domains that I believe are a *threat response* follow in importance, and finally other controls that may fall into one of the proceeding categories, but are not important to SnowBe's operational needs. The first seven domains, Security Assessment through Physical Protection are all domains that I believe could help SnowBe prevent/protect against threats. These are most important because if they ideally, if they are perfectly implemented, there will never be any threats to respond to, making other domains null and void. The next five domains, Recovery through Audit and Accountability are all domains I feel help an organization respond to threats. These are important to help SnowBe remain operational and in business during and after and threats. Situational awareness is the first of the next set of domains because while I think it is an important threat prevention domain, I don't think it is as important as any of the other threat prevention domains, or the threat response domains. While configuration management is important, SnowBe currently seems to be managing with doing configuration and documentation as systems are built/need to be protected. Awareness and Training is something that SnowBe can focus on after getting their systems up and running and as SnowBe doesn't really have much media, this is the last domain in order of importance.

2)
   a) Domains one, three, five, and seven from ordered list above.
      i) Security Assessment
      ii) Systems and Communications Protection
      iii) Asset Management
      iv) Maintenance
   b) Capabilities for Domains in 2a
      i) C035 – Define and manage controls
      ii) C038 - Define security requirements for systems and Communications
      iii) C006 - Manage asset inventory
      iv) C021 - Manage Maintenance
   c) Domain, level, practice number for the state of each domain
      i) CA.2.157 – Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.
      ii) SC.1.175 - Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems.
      iii) AM.3.036 - Define procedures for the handling of CUI data
      iv) MA.2.111 Perform Maintenance on Organizational Systems.
   d) Next steps for each practice
      i) The first this SnowBe should do to meet this practice is identify and define system boundaries. The system scope will include, but is not limited to laptops, desktops, all servers, Firewall, Antivirus software, and RMM software. Connections between systems will need to be defined, as well as any external or third-party connections. Snow be will need to document system environments of operations, as well as map and document security requirements for SnowBe's organizational needs. Most important for this practice will be creating and maintaining system security plan documentation so that future security analyst will not only know SnowBe's systems, but how and why protections were implemented.
      ii) To properly monitor, control, or protect organizational communication, SnowBe will first need to identify and map their network boundaries. SnowBe has already deployed a firewall which will help protect communications, but that firewall will need to be regularly maintained.

Internal networks should be segmented with VLANs and a Zero Trust Policy should be implemented to ensure all internal communications are verified and logged. SnowBe should focus on protecting DNS and Email communications to meet this practice.

iii) To appropriately define procedures for the handling of Controlled Unclassified Information(CUI) data, the first thing SnowBe should do is identify and classify all information that SnowBe process on it’s systems. This will help SnowBe determine what data qualifies as CUI. Next, SnowBe should evaluate the requirements they need to meet to become/remain compliant with necessary regulations. After SnowBe both understands both the data they process and the regulations they need to meet, they can come up with clear procedures on how to store, access, transmit and dispose of CUI. In order to meet the practices for this level, procedures will need to be properly documented.

iv) To maintain organizational systems, the first thing SnowBe needs to do is come up with a schedule on which they will perform maintenance. This could include daily, weekly, monthly, quarterly, or annual maintenance, or some combination of them. Maintenance should include operating system updates for all Laptop and desktops which can easily be done using SnowBe’s RMM software. All applications and antivirus software that runs on SnowBe systems should also be maintained regularly. The AD server should also be maintained as this system influences other domains like Access Management and Identification and Authentication. User Accounts should be reviewed to remove inactive accounts, and groups membership should be verified to ensure it aligns with SnowBe policies.

3) The most important thing I learned this week while working on the CMMC task for this week is how to properly assess a companies security posture using the Cybersecurity Maturity Model Certification. I thought it was a little confusing ‘grading’ domains that did not have lower level exercises, but I was able to efficiently use the CMMC Assessment guide to rank the appropriate categories for SnowBe. Understanding the practices and different ways a company might impalement those practice to achieve mastery of the following level was great real world practice.