Technical Requirements for Cyber Security

1. A process to identify risks. (7.3.3)
   1. Need to be more specific about phase (7.2.2 in current proposal?)
   2. Record and dedicate environments for the storage and execution of aftermarket software e.g., apps. (7.3.5)
2. A process to identify and manage dependency on suppliers. (7.2.2.3)
3. A process to manage/mitigate the risks during the design of the vehicle. (7.3.2)
4. A process to validate that the risks are managed as intended. (7.3.3)
5. A process to monitor for cyber attacks. (7.2.2.2)
6. A process to respond to an identified cyber attack. (7.2.2.2)
7. A process to restore any capabilities impaired by a cyber attack.
   1. Need to clarify that applies only to functions covered by regulation/certification/type approval etc.
   2. Time element – is this still true after 15 years, etc.
8. A process to evaluate all processes to ensure they are kept current. (7.2.2.2)