From: Baumbach, George G (GRANT)
Sent: Wednesday, September 28, 2022 12:19:39 PM (UTC-05:00) Eastern Time (US & Canada)
To: aiframework <aiframework@nist.gov>
Subject: Playbook Feedback.

1) In MAP-2 replace "Classification" with "Categorization". Classification is a confusing word in this context since classification is 'class' (or category) of AI. This would also more closely mirror the NIST RMF.

2)I suggest a MAP-6 "Risks to AI Specific Cybersecurity Threats are mapped, modelled, and addressed".

This includes attacks like model extraction and robustness attacks. These attacks should be considered before deploying a model. The threats should be modelled and addressed like any other cybersecurity risk. It is important that the NIST AI RMF framework addresses AI specific attacks because they are not addressed by any other governing documents

AI needs a mapping to the NIST CSF "Identify threats, vulnerabilities, and risk to assets" because the CSF doesn't recognize AI as a unique kind of asset - a different kind of software - that requires its own controls.

I have spoken about these kinds of attacks to corporate, academic, and industry audiences - all of whom were unaware that these attacks are possible. The NIST RMF should bring these topics into the conversation.

verizon✓
Grant Baumbach