April 29, 2022

Comments of HERE Technologies on the
NIST AI Risk Management Framework: Initial Draft

HERE Technologies ("HERE") respectfully submits these comments in response to the National Institute of Standards and Technology ("NIST") request for comments related to the initial draft of its Artificial Intelligence Risk Management Framework ("Framework" or "RMF"), published on March 17, 2022.

HERE is a global leader in location platform services, enabling people, enterprises, and cities to harness the power of location. By making sense of the world through the lens of location we empower our customers to achieve better outcomes - from helping a city manage its infrastructure or an enterprise optimize its assets to guiding drivers to their destination safely.

HERE has a direct interest in this matter, as our customer base includes many of the world's leading automotive manufacturers, transportation and logistics companies, and government agencies, all of whom demand secure, high-quality handling of the location data we process on our platform. HERE employs Artificial Intelligence ("AI") technologies in the collection and processing of the massive amounts of data we require to develop our location products and services. HERE has had a positive experience with NIST's Cybersecurity and Privacy Frameworks and believes that the proposed AI RMF can similarly help entities better manage and reduce their risks from using AI systems.

HERE appreciates NIST's effort to create a flexible and voluntary RMF that will help identify and address risks in the design, development, use, and evaluation of AI products and services. As noted, we believe that the RMF will provide valuable assistance and guidance to entities that use AI systems. As an overall observation, we suggest that the RMF should focus more on the quality and sources of data for AI systems as they are both the input and output for such systems. With that general statement, HERE offers the following specific comments, observations, and suggestions on the Framework.

AI Stakeholders

On lines 15-21 of page 4, the RMF describes the types and functions of "Operators and Evaluators" AI stakeholders. While HERE generally concurs with this description, we believe that because the use of AI is a serious consideration involving the curation and management of data from its raw format into its final transformed state, there should be an explicit mention of senior leadership within a technology organization that can bear the risk that 1) data quality is high enough to use AI, and 2) the decision to implement AI systems is in line with the organization's goals. Using AI is often a costly undertaking and needs direct decision making from leadership.

Challenges for AI Risk Management

As noted above, we believe that the RMF should emphasize should focus on what we think is the most pivotal facet of AI – data. The “Challenges for AI Risk Management” section beginning on page 6 does not adequately address the issue of data quality. Data is central to the quality of AI and is the earliest point where risk can be reduced. Bucketing data into the technical risks category, as defined starting on page 8 line 16, does not underscore the risk well enough as it is both the input and output of any AI agent. A specific area where this could be improved is figure 3 on page 8 by adding a bullet to the effect of “Data quality”.

While we believe that statistical validity and other technical characteristics are aptly covered in this section, the suggestion that AI needs to include tests ‘of robustness to adversarial attack’ is not pragmatic for many of the risks facing the AI domain today. Data quality, coverage, and model design are much more likely to disrupt a model than a specific attack. An attack against an AI model could be impacted non-distinctly from ransomware or other e-crime. Referencing NIST’s RMF and the capacity to protect AI models in line with other organizational systems risk capacity would be a more fitting conclusion to section 5.1.

Interpretability

On page 11 the RMF discusses the difference between interpretability and explainability. Interpretability can be articulated with industry standard terminology related to knowledge-based AI methods. Frames, scripts, and explanation-based reasoning graphs and learning trees can provide a more standard means of relaying model concepts that both serve to articulate an agent’s purpose and document ‘how’ something works for non-experts. Using industry-standard terminology would bridge the separation of interpretability and explainability for a broader audience while standardizing common methods of documentation.

Finally, as noted above, we appreciate NIST’s effort to develop the Framework for AI stakeholders to identify and reduce risks when developing and using AI systems. We think it would be sensible for NIST to provide a reference definition of AI in the Framework to ensure that stakeholders that turn to the Framework for guidance have a common basis for applying it.

HERE is pleased to submit these comments on the RMF and we would be happy to provide additional information or to answer any questions NIST staff might have.

Andrew Anderson
Senior Risk Assurance Manager
HERE Technologies