Reliable Energy Analytics, LLC (REA) is pleased to offer these comments in response to the NIST Call for Papers on Consumer Software Labeling.

REA is a Massachusetts based software vendor providing critical infrastructure industries with a Cyber Supply Chain Risk Management (C-SCRM) solution that implements a patent pending 7-step risk assessment process based on the NIST Cybersecurity Framework, V1.1, using NTIA supported Software Bill of Materials (SBOM) standard formats. The comments below describe an existing consumer labeling program, called SAG-STAR™, that has been implemented by REA, based on a Community Trust Model where consumers declare their trust in a vendor/product within the SAG-CTR™, Community Trust Registry. Products that achieve a critical mass of "community trust declarations" in SAG-CTR™ are eligible to display the SAG-STAR™ emblem, shown below:

Figure 1 SAG-STAR emblem (left) and SAG-CTR Logo (right)

SAG-STAR™ Program Description

The SAG-STAR™ program includes a combination of vendor-centric and product-centric evaluations that are performed by REA customers. The process begins with a set of vendor-centric evaluations, which an REA customer conducts on a software vendor. The North American Transmission Forum (NATF) Supply Chain Security Assessment Model provides the basis for all vendor-centric assessment activities that REA customers are expected to follow:

Figure 1: The Supply Chain Security Risk Assessment Lifecycle

All product-centric evaluation criteria is based on the Software Assurance Guardian™ (SAG™) patent pending process defined in the patent application titled "Methods for Verification of Software Object Authenticity and Integrity", which is implemented in the SAG™ Point Man™ (SAG-PM™) C-SCRM

software solution provided to the Electric industry in order to meet NERC CIP-010-3, software verification requirements. The SAG-PM™ software is the gateway by which a REA customer submits their "trust declaration" in the SAG-CTR™. During an execution of the SAG-PM™ C-SCRM risk assessment a statistically calculated trustworthiness score, called a SAGScore™ is produced, based on the results of the 7-step risk assessment process. REA customers are prompted by SAG-PM™, requesting if the customer wants to submit a trust declaration for the examined software product, within the SAG-CTR™.

If the customer answers Yes to this prompt, the SAG Evidence file from the SAG-PM risk assessment is sent to the SAGServer™, where it is inserted into the Trust Queue for processing. REA personnel evaluate all trust submissions and decide if the evidence data supports the inclusion of a trust declaration, by the filing customer, for the submitted product and vendor in SAG-CTR™. The customer is notified of the decision to pass/fail the trust declaration, along with findings supporting the decision.

Products with a critical mass of community trust declarations in SAG-CTR™ are eligible to proudly display the SAG-STAR™ emblem on their marketing and product materials. The process begins when REA notifies a Product Vendor that their product has received the required number of community trust declarations in SAG-CTR™ to be eligible to display the SAG-STAR™ emblem. The software vendor may choose to pursue this right by contacting REA indicating their desire to acquire the rights to display the SAG-STAR™ emblem.

The SAG-STAR™ program described above is currently in production use within REA's SAG-PM™ product offering.

REA thanks NIST for the opportunity to provide these comments, in response to the call for papers identified earlier in this document, for information regarding "*technical criteria needed to support validation of consumer software security assertions that reflect a baseline level of secure practices*".

s/*Richard Brooks*/
Richard Brooks
Reliable Energy Analytics LLC
CoFounder and Lead Software Engineer for SAG-PM™
https://reliableenergyanalytics.com/
email: dick@reliableenergyanalytics.com