AF252-D010: AI/ML-Enhanced Risk Management Framework

ADDITIONAL INFORMATION

N/A

TECHNOLOGY AREAS:

Information Systems

MODERNIZATION PRIORITIES:

Advanced Computing and Software | Advanced Infrastructure & Advanced Manufacturing | Integrated Network Systems-of-Systems | Integrated Sensing and Cyber | Trusted AI and Autonomy

KEYWORDS:

RMF; Risk Management Framework; AI/ML

OBJECTIVE:

Develop a software application that employs AI/ML or similar methodologies to automate the Risk Management Framework (RMF) process which is required to achieve Authority To Operate (ATO) for software and hardware products on government networks.

DESCRIPTION:

The current RMF process relies heavily on manual efforts and human expertise, which can result in delays, inconsistencies, and potential oversights. As the DoD continues to adopt advanced technologies and faces increasingly sophisticated cyber threats, there is a pressing need to streamline and automate the RMF process to ensure the timely and effective management of risks. AI and ML technologies offer promising solutions to address these challenges by enabling data-driven decision-making, predictive analytics, and automated risk assessment. USAF CIO, USSF, MAJCOM/A6s, and program offices are highly interested in the development of an AI/ML-powered RMF platform that integrates with existing DoD systems and processes. The ideal platform will leverage advanced algorithms and techniques, such as natural language processing, graph analytics, and deep learning, to automate and optimize various aspects of the RMF process.

PHASE I:

It is expected that proposers provide evidence of sufficient prior work and feasibility study to apply AI/ML or similar methodologies to the Risk Management Framework.

PHASE II:

Provide a prototype software application which employs AI/ML or similar methodologies to automate the RMF process. Provide a demonstration of the prototype evaluating an example product which has already been through the manual RMF process within the last two years (achieve TRL 6 maturity).

PHASE III DUAL USE APPLICATIONS:

Provide a software application which employs AI/ML or similar methodologies to automate the RMF process. Provide proof of effectiveness by evaluating an example product which has not been through the manual RMF process (advance from a TRL 6 to TRL 9 maturity). Add the functionality of continuous monitoring after initial Authority To Operate approval. Implement proper User Interface/Experience (UI/UX) concepts to ensure end users can efficiently and effectively operate the tool. If successful, this technology will have broad application and significant impact across DAF, DOD, and USG.

REFERENCES:

1. Graubert, Richard and Bodeau, Deborah. "The Risk Management Framework and Cyber Resiliency." Case #16-0776. The MITRE Corporation. 2016.
2. DoDI 800.01 "Risk Management Framework for DOD Systems."
3. NIST 800-37 "Guide For Applying the Risk Management Framework for Federal Information Systems."

TOPIC POINT OF CONTACT (TPOC):

TPOC-1: Matthew Hays
PHONE: 7193333399
EMAIL: matthew.hays@afacademy.af.edu

TPOC-2: Duncan Stewart
PHONE: 7193333399
EMAIL: duncan.stewart@afacademy.af.edu