N251-019 TITLE: Neuro-Symbolic Artificial Intelligence (AI) Agents for Cybersecurity Authority To Operate (ATO) Development

OUSD (R&E) CRITICAL TECHNOLOGY AREA(S): Integrated Network Systems-of-Systems;Integrated Sensing and Cyber;Sustainment

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: Research, design, and develop an innovative automated software toolset to assist the Cybersecurity workforce personnel in developing and maintaining Authority to Operate (ATO) packages under the Risk Management Framework (RMF) process.

DESCRIPTION: The DoD leverages the RMF to guide cybersecurity processes and requirements [Refs 3, 5, 7, and 9]. Further, program offices have experienced a dramatic increase in the man-hours required to produce a cybersecurity ATO package and maintain that package throughout the lifecycle of the system or systems supported. This increase has put a strain on budgets and increased schedules.

One outcome from Deep Neural Network (DNN) experiments into what are called large language models (LLMs; e.g., GPT3 or Lambda) is the ability for analysis of large data sets and the capability of system composed documents based on user requests [Refs 1 and 2]. For example, one might say, “Write me a paper about ‘Logistics issues in Africa’”, and the system can then automatically produce a document that may sound reasonable. It has classified or categorized information about both logistics and Africa. It may even have found areas of overlap. The system is trained to understand, identify, and replicate patterns of what a paper should look like, how it might be organized, and the structure of paragraphs and sentences. There is a chance, therefore, that the paper actually conveys real information. There is, however, a significant chance that the paper is utter nonsense (i.e., a pattern borne out of mimicry rather than substance). The use of the LLM approach may be less viable as one moves towards novelty. That is, if a paper that describes a new concept, device, method, process, or strategy is desired, LLMs are unable to provide much help. In one sense they are merely sophisticated search algorithms that can find existing patterns and sometimes combine those patterns to useful effect.

An ATO is by its very nature a novel problem. So, one might argue that the LLMs are not going to add much value. This, however, is only true if they are used in isolation. This SBIR topic seeks a technical approach that leverages one or more technology type, such as LLMs, and capabilities offered by Artificial Intelligence (AI) and/or Machine Learning (ML) [Refs 4 and 8]. For example, approaching this challenge as an applied engineering discipline, focusing on applying a myriad of AI Techniques such as DNN to identified AI reasoning tasks with an understanding that most expertise is found in the heads of subject matter experts (SMEs) rather than in large data repositories, is expected to maximize the efficiency and effectiveness of the capability and maximize return on investment. The desired outcome of this SBIR topic is to develop technology and a methodology to work with SMEs to capture their expertise and mental models on the RMF and ATO process. From here, the technical approach should leverage these mental models to generate bias DNN classifiers and provide a way to represent an organization’s specific expertise and content.

Expected outcomes include:

- Efficiency Gains: Significant reduction in time and manpower required for ATO drafting.
- Consistency and Compliance: Standardized ATOs that adhere to Department of Defense (DoD) Cybersecurity regulations and policies.
- Scalability: Potential application across various DoD acquisition entities, enhancing overall efficiency of the Cybersecurity workforce.

Work produced in Phase II may become classified. Note: The prospective contractor(s) must be U.S. owned and operated with no foreign influence as defined by 32 U.S.C. § 2004.20 et seq., National Industrial Security Program Executive Agent and Operating Manual, unless acceptable mitigating procedures can and have been implemented and approved by the Defense Counterintelligence and Security Agency (DCSA) formerly Defense Security Service (DSS). The selected contractor must be able to acquire and maintain a secret level facility and Personnel Security Clearances. This will allow contractor personnel to perform on advanced phases of this project as set forth by DCSA and NAVAIR in order to gain access to classified information pertaining to the national defense of the United States and its allies; this will be an inherent requirement. The selected company will be required to safeguard classified material during the advanced phases of this contract IAW the National Industrial Security Program Operating Manual (NISPOM), which can be found at Title 32, Part 2004.20 of the Code of Federal Regulations.

PHASE I: Design and develop a system that captures and organizes cybersecurity hardware/software configuration information and can automatically write an ATO for a given system leveraging that information. Develop a hybrid solution that integrates the capabilities of large language models, leveraging the mental models of experts and past ATOs into the ATO creation process. The Phase I effort will include prototype plans to be developed under Phase II.

PHASE II: Develop, test, and validate prototype software toolset proof of concept. Recognizing that initial generated ATOs will lack quality, develop and engage in an iterative test cycle, design and development software refinement, and document proposed concept of operations for employing technology. The goal is to capture and adapt knowledge over time, which incrementally improves the process through feedback from experts.

Work in Phase II may become classified. Please see note in the Description section.

PHASE III DUAL USE APPLICATIONS: Mature technology and seek approvals for deployment on DoD systems. Extend capability to more advanced capabilities for higher level security documentation. Investigate solutions to automated sustainment of underlying knowledge models. Consider additional modular capabilities to extend utility and use throughout the ATO process.
Cybersecurity is an issue for commercial sector organizations beyond DoD such as banking, medical, and civil infrastructure (e.g., power, water, GPS, and internet). As technology use has continued to increase, individual considerations for protections increase as well. The commercial sector will likely benefit from similar technology within these industries, as well as means for commercial products used within households to increase certification/guarantees to consumers.

REFERENCES:

1. Kitchin, R. “Big Data, new epistemologies and paradigm shifts.” Big data & society, 1(1) , 2014. https://doi.org/10.1177/2053951714528481
2. Fan, J.; Han, Fang and Liu, Han. “Challenges of big data analysis.” National Science Review, 1(2), February 5, 2014, pp. 293-314. https://doi.org/10.1093/nsr/nwt032
3. “Risk Management Framework.” https://rmf.org/

4. Snoek, J.; Larochelle, H. and Adams, R. P. “Practical bayesian optimization of machine learning algorithms.” Advances in neural information processing systems, 25, 2012. https://www.cs.princeton.edu/~rpa/pubs/snoek2012practical.pdf
5. Takai, T. M. “DoDI 8510.01 Risk management framework (RMF) for DoD Information Technology (IT).” Department of Defense, March 12, 2014. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300
6. Ellett, J. M. and Khalfan, S. “The transition begins: DoD risk management framework.” CHIPS, April-June 2014. https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=5015
7. AcqNotes. (n. d.). “Risk management framework (RMF).” AcqNotes: Defense Acquisitions Made Easy. http://acqnotes.com/acqnote/careerfields/risk-management-framework-rmf-dod-information-technology
8. Defense Innovation Board. (n. d.). “AI principles: Recommendations on the ethical use of artificial intelligence by the Department of Defense.” Department of Defense. https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF
9. “Risk Management Framework (RMF).” National Institute of Standards and Technology. https://csrc.nist.gov/projects/risk-management/rmf-overview
10. “National Industrial Security Program Executive Agent and Operating Manual (NISP), 32 U.S.C. § 2004.20 et seq. (1993).” https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2004

KEYWORDS: Automated Software; Cybersecurity; Authority to Operate (ATO); Risk Management Framework (RMF); Deep Neural Network (DNN); Generative Artificial Intelligence