Automated, Artificial Intelligence (AI) – Enabled Traffic Generation

(AI Traffic Generation)

Cyber Innovation Challenge (CIC) #5

Assessment Event

Request for Solutions (RFS)

09 SEP - 13 OCT 2025

Submit NLT 13 OCT 2025
at or before 11:59 PM ET
U.S. Citizens Only

Background/Synopsis

This RFS solicits innovative solutions via a white paper submission in Vulcan for the development of an automated, advanced Artificial Intelligence-enabled traffic generation capability, sometimes referred to as user emulation, for the Persistent Cyber Training Environment (PCTE). The primary objective of this innovation challenge is the provision of user traffic and artifacts so realistic that the PCTE trainees experience situations that match the network traffic seen in real-world missions they will face upon deployment.

PCTE Overview

The PCTE provides the Department of Defense (DoD) Cyberspace Workforce and Allied partners with a secure, configurable, and real-time virtual environment for cyber training and mission rehearsals across all classification levels. PCTE is a distributed capability to DoD Cyberspace Workforce and its International Partners to "train as they fight" in a relevant, configurable, and real-time virtual environment. Through this ability to standardize, simplify, and automate the training management lifecycle seen by the Cyber Mission Force (CMF) operators, PCTE supports United States Cyber Command (USCC) mission readiness priorities.

PCTE Platform and Architecture

PCTE consists of a suite of Commercial-Off-The-Shelf (COTS) software products that are hosted on a fleet of geographically dispersed data centers managed by the Government with bespoke hardware architecture. At the highest level, a PCTE system, referred to as an Enterprise Compute and Storage node (ENT), is divided into the Control Plane (CP) and one or more Event Plane(s) (EP):

- CP: Logically isolated cluster of servers hosting the security-hardened and accredited applications/services that provide the core user-facing functionality of PCTE. The CP hosts applications and services such as the training portal, Help Desk ticketing service, chat application, platform monitoring dashboards, and more. From the CP, the PCTE Platform provisions computing resources in the EP to support individual, team, and force-level training.
- EP: Logically isolated cluster of servers hosting virtual machines, containers, and software-defined networking components that make up the dynamic "ranges" for cyber training environments. The EP is unaccredited which grants users total flexibility to incorporate vulnerable systems, upload malicious software, and design their environments however needed to conduct cyber training and rehearsal. Virtual machines and containers deployed within the EP are unable to reach the outside internet or network transports to ensure that potentially malicious artifacts cannot escape the training environment.

Compute, storage, and networking resources are provided by COTS hardware and do not currently integrate with cloud-based storage or compute resources. Of note for this contract, ENT systems do not currently have any Graphics Processing Unit (GPU) resources available. CP applications are hosted as virtual machines on a vCenter hypervisor or as containers on Tanzu Kubernetes Grid (TKG).

Users access PCTE via a web browser over the unclassified internet as well as on classified networks. Users authenticate via RedHat Single Sign On (SSO) and access each PCTE application based on assigned permission roles.

Current PCTE Tools Related to Help Desk Operations

PCTE currently offers a COTS tool to provide traffic generation within cyber ranges. The AI-enabled traffic generation solution proposed is expected to augment and/or replace some of these capabilities.

The PCTE traffic generation current state has the following capabilities:

- A configurable user profiles and activities
- GUI for setting and monitoring high level actions within a collective event
- Users execute activity on full stack VMs and can be monitored via console
- Users can support Windows and Linux operating systems
- Limited traffic and user generation

Key Technologies

The following table lists some of the specific technologies utilized in the PCTE platform today. This list is provided to aid prospective future developers in integrating their capabilities into the platform.

Capability	Technology Used	Purpose
Kubernetes	VMWare TKG	Containerization platform for hosting software applications
Identity Manager	Red Hat Identity Manager (IDM)	Source of truth for user attributes and credentials
Single Sign-On (SSO)	Red Hat (SSO)	Authentication tool utilizing OpenID Connect (OIDC) to allow users to sign into the platform once and access all applications (based on platform roles)
Hypervisor	VMware vSphere	Hosting virtual machine clusters that serve the infrastructure and services in ENT systems and that dynamically deploy virtual machines for cyber ranges
Software-Defined Networking	VMware NSX-T	Dynamic networking tool that logically isolates Range Deployments and provides the networking infrastructure within each Range Deployment
Firewalls	F5 products	User-facing firewall that controls access to the PCTE platform from the open internet and firewall that isolates the EP

Solution Constraints

The proposed solutions must adhere to the following:

- NIST, ISO 27001, FedRAMP, etc. cyber security standards compliance
- No dedicated AI/ML GPUs in existing infrastructure (but program can adjust as needed)

Purpose

The Cyber Fusion Innovation Center (CFIC), in collaboration with the Program Executive Office Simulation, Training and Instrumentation (PEO STRI) invites qualified industry partners to submit solutions in the form of a white paper for the development of an automated, advanced Artificial Intelligence-enabled traffic generation capability for the Persistent Cyber Training Environment (PCTE). The intent of the RFS is to identify, evaluate, and select capable companies through the CIC #5 contract vehicle – CFIC, who will be the B2B contracting entity. Aligned to address emerging United States Cyber Command (USCC) operational priorities, this RFS seeks candidate prototypes across best-of-breed AI-enabled traffic generation solutions amongst various companies to incrementally integrate into the PCTE platform through its agile acquisition methodology, to improve realistic user activity and network traffic in the training environment.

Statement of Need

PCTE's current method for emulating users during training scenarios has several challenges. Today, it is very easy to differentiate between what artifacts the red team left behind and what was auto generated. The current system does not provide the totality of network traffic required for realistic training desired by PCTE users including, network traffic, grey space user actions, system to system communication, etc. On the network side, emulated user traffic has a distinctive signature that is easy to filter out. Network traffic from emulated users is easily

differentiated from OPFOR and other actors because the lack of realistic behavior leads to a high level of detectability. Furthermore, activities performed, and text written by emulated users is unrealistic and/or completely random. In addition, emulated users are limited to a dedicated domain, a small number of operating systems, and have difficulty scaling beyond 50+ personas. This leaves limited choices for customizing user actions and it becomes increasingly difficult to configure and/or modify these actions.

PCTE is seeking the following features in solution proposals:

- Automated generation of varied and realistic users, network, services, and device traffic from varying nodes and network domains, so that the training audience has realistic network activity and red team traffic can be obfuscated and harder to identify
- Providing more realistic, dynamic and diverse network traffic that incorporate the "noise" and complexity of a realistic environment (e.g. – varied types of devices, varied frequency of network usage, varied points of origin or traffic routing, varied frequency protocols, etc.)
- User emulation and network traffic generation capabilities tailored for blue, red, and gray space, so that expected traffic within an event represents a realistic environment
- Traffic generation based on roles and associated account privileges producing a variety of user types and activity to include administrators, service accounts, human resource users, finance users, etc., so that the environment has variation in activity to make it difficult to differentiate between blue and red team operators and generated traffic
- Emulation of highly varied and diverse types of users, technologies, and protocols across information technologies (IT) and operational technologies (OT) domains
- Host-based user emulation capabilities that can perform a variety of tasks on hosts, to include login/logout, run processes, send emails, create files, change system configurations, so that the training audience has realistic host activity within the training environment
- Centralized monitoring and management interface for White Cell with the capability to oversee and traffic generation capabilities in real time
- Realistic user activity, email and traffic artifacts tailorable to specific scenarios
- Diversified, adaptive, and non-patterned user behavior
- Intelligent scenario generation and adaptation
- Intuitive user interfaces
- Flexible, dynamic, and highly realistic agents that adapt and react for events and activities on the network aware of the scenario details
- Ability to perform specific activities and action at specified time (or based on events) in the training scenario
- Support seamless integration of third-party tools

Potential Data artifacts to inform the AI model include:

- Open source data
- Network maps/configurations
- User-developed scenarios and/or background information
- Server Message Block (SMB connections

PCTE is seeking the following outputs as part of the solution proposals:

- Realistic documents with realistic names and tailored to each training scenario
- Realistic and tailored emails, including source, subject, content and attachments
- Seasoned traffic generation from, but not limited to the following areas:
    - Emulation: medical personnel, insider threat, standard user, Human Resources, workstation administrative user, Exchange administrative user, Active Directory user

- Active Directory: Federated services, organization units' creation scripts, AdminSDHolder, SIDHistory, Groups creation script, tiered administrative user creation script, tiered administrative groups creation script, Group Policy Object creation script, computer creation script, and user creation script
- Software: Git, LAPS, Active Client, nginx, Apache, Open Office, Python 3.x, PowerShell 7.5x, Wazuh, Elastic Stack, OpenEMR, Adobe Reader, Firefox, Chrome, Putty, Velociraptor, Office 2019

It is expected that, over time, the AI-enabled traffic generation capability will "learn" and increase fidelity in response to trainee actions.

Key Capabilities and Requirements

PCTE requires the implementation of traffic generation enhancements that use state-of-the-art AI technologies and techniques to maximize timeliness and accuracy of help to users of PCTE. PCTE acknowledges that this is a relatively new and emerging capability and therefore has separated the requirements into initially minimally viable requirements and additional requirements that may be added through iterative improvements. Companies should address all requirements in the whitepaper, including what is currently in the solution being proposed and the feasibility of adding the functionality in a reasonable time frame.

CORE REQUIREMENTS

The white paper solution submitted must address how the solution provides the following:

1. **Realistic, varied and relevant AI-enabled user persona and traffic simulations:** Deploy AI/ML-enabled traffic generation as described above, tailored to PCTE usage.
2. **Realistic emulation of user roles and associated traffic:** In order to obfuscate the action of emulated network activity from actual activity, ensuring that trainees do not identify artifacts as part of the training versus reality.
3. **Realistic, relevant, and varied artifacts:** To support realism, artifacts (e.g., files, emails, traffic) are complete, coherent, and relevant to the training.
4. **Adaptive User Actions:** Enriches system traffic and usage emulation while scenarios are underway with context-relevant, adaptation of user activity while training is ongoing.
5. **Management and Monitoring Dashboard:** Provides an interactive means for configuring, managing, and monitoring the usage and performance in user emulations.
6. **Data Assurance and Security:** Precautions and security controls are in place to ensure that any information retrieved by the AI system are secure in a Controlled Unclassified Information (CUI) - compliant environment.
7. **TS/SEC Air-Gapped Environment:** Consideration for the future ability to have all data, models, and processing contained within the secure local infrastructure, without reliance on external networks or cloud resources.

INTEGRATION REQUIREMENTS

PCTE includes multiple COTS and proprietary products and prototyped capabilities in the platform. The Stakeholder will work with the selected company(ies) to integrate the company's AI-enabled traffic generation solutions into the modular PCTE baseline. The candidate technologies will be embedded into the agile scrum integration processes whereby each company iteratively and incrementally enhances their capability within the PCTE platform. Accompanied by its agile scrum execution, companies are expected to demonstrate and deliver usable and shippable products at agreed to sprint increments that increase breadth and depth of capabilities within the PCTE ecosystem. This continued rapid development of the platform is necessary to meet the evolutionary and rapidly adapting delivery requirements and immediate user needs.

The Stakeholder intends to integrate the selected company's solution(s) into the modular PCTE baseline that currently includes other commercial and proprietary products. Integration will require technical data exchange, dialogue, and software/hardware integration of proposed solutions within the Stakeholder's DevSecOps environment. It is expected that a company may have to work directly with other companies under the Stakeholder's integration oversight to help establish and extend PCTE.

The white paper should address any integration considerations or requirements for the solution, such as:

- Integration into the PCTE enterprise
- Any hardware or operating environment requirements
- Scalability
- Ability, constraints, and technical approach for ingesting other data into the AI used for User emulation processing
- Identify any systems or services outside of PCTE platform that would need to be incorporated

Deliverables

The selected contractor(s) shall provide the following deliverables:

1. An incremental, functional prototype of the AI-enabled traffic generation capability
2. Documentation, including user manual, installation/configuration guides, and relevant API and architectural documentation needed for extensibility
3. A detailed report outlining the design and implementation of the AI algorithms, machine and/or reinforcement learning methodology used in the solution (i.e. RAG, Vector Search, conventional indexed search, etc.)
4. Periodic demonstration, as requested by the Stakeholder, of the platform's AI-enabled traffic generation capabilities and performance
5. Documentation of security controls in place to ensure Risk Management Framework compliance.
6. Software Product Licensing Cost Estimate Projection
7. Software Product Data Rights, Life Cycle Sustainment Terms and Conditions

Assessment Criteria

Solution white papers and demonstrations will be evaluated with consideration given to the vendor's ability to provide a clear description of the proposed solution aspects. Each criterion will be scored on a scale of 0 to 5 where 5 = Excellent; 4 = Good; 3 = Satisfactory; 2 = Marginal; 1 = Unsatisfactory; and 0 = Lack of applicable content.

#	**Criteria**
0	General Submission Quality
1	Operational Relevancy
2	Technical Approach
3	Development and Integration
4	Operations and Maintenance
5	Schedule and Price

What happens after white paper submission?

(Grading and downselect for a Virtual Assessment Event)
Prospective solutions will be evaluated by a team of the Stakeholder's choosing through a multi-phased process with the intent to competitively award one or multiple Other Transaction Agreements (OTAs) for prototype projects in accordance with 10 U.S. Code §2371b.

The Stakeholder will subsequently down select companies whose white paper solution has the highest value. Then, those companies will be invited to present and/or demonstrate their capability in a private, virtual pitch / demo session hosted through an online platform with stakeholders on a specific date.

Current Initiative Timeline

Phase 1: 04 June 2025 – Collaboration Event
Industry, academia, and government partners met in-person, in a workshop format, to identify current limitations and refine the definition of the topic areas for CIC #5. The AI-Enabled Help Desk capabilities discussed during that event have been used in formulating this RFS.

Phase 2: 09 September - 13 October 2025 – Submission Window / Q&A and Response
The resulting RFS is distributed via the sam.gov website and Vulcan submission portal to notify any/all interested industry partners/companies so that they can submit whitepapers/responses. The white paper submission window will open, information will be distributed via the sam.gov website, CFIC website, and Vulcan submission portal, and then white paper documents will be accepted through the Vulcan portal for at least 30 days. Submitting companies MUST have a Vulcan account to submit.

Industry, academia, and government partners MUST submit a maximum 8-page submission response white paper document through this link – **CLICK HERE**. Submit NLT (No Later Than) 11:59 p.m. Eastern on 13 October 2025.

Q&A and Response: During the white paper preparation period, prospective respondents may submit clarifying questions to the Stakeholder through **this form**. The form will be open until 3:00 p.m. Eastern on 19 September 2025. An anticipated response to these clarifying questions will be sent out via email by CFIC on or about 25 September 2025. Please visit cyberfic.org to stay informed.

Phase 3: On or About 15 October - 29 October 2025 – Submissions Reviewed & Downselects
The Assessment Team (chosen and managed by the Stakeholder) will review and assess each submission using the requirements and assessment criteria defined herein for grading and making down-selects of those respondents/submissions they feel have the highest potential to satisfy the PCTE needs. Some number of favorably evaluated submissions will receive an invitation to attend Phase 4. The exact number of submittals receiving this invitation will be decided at a later date. Grading and downselecting will take place in the Vulcan system and be led by the Assessment Team. CFIC will facilitate notification to the downselected companies and assist in coordinating dates/times for virtual demos noted in Phase 4. Notifications are tentatively slated to be sent on or near 31 October 2025.

Phase 4: On or About 17 November - 20 November 2025 – Virtual Demonstration Presentations and Evaluation
Selected companies will conduct a virtual Solution Demonstrations for PCTE Stakeholders and the CIC #5 evaluation team. Within this evaluation phase, selected companies will have an allocated 1-hour timeslot to discuss their solution and conduct a demonstration, showcasing how it meets the operational requirements. It is expected that the demonstration will be recorded. The Stakeholder will complete their evaluations with

consideration given to the same set of evaluation criteria, as a reinforcement or clarification of the white paper response. Sample datasets for ingestion by the potential solutions may be provided by the Stakeholder prior to demonstrations to aid in evaluating capability effectiveness. Demonstration presentations will be held virtually through MS Teams. Each company will be notified of their presentation time by a member of the CFIC team.

Phase 5: Selection, Award, and Execution/Follow-On
Following review of initial submissions and solutions via virtual demonstrations, the Stakeholder may award one or more prototype project(s) to the company(ies) whose solution(s) is/are determined to be the most advantageous to the Stakeholder. The Stakeholder may elect to purchase all, some, and/or none of the solutions from Phase 4 for incorporation into PCTE, or for further projects. This may include the solution as an off-the-shelf solution or may include further incremental refinement to meet the needs of PCTE. The Stakeholder has several acquisition/contract vehicles (i.e., various IDIQ contracts, purchase orders, etc.) to potentially contract for the solution, and or further capability development for the solution, if operationally viable.

The Stakeholder reserves the right to award to a company that does not meet all the requirements but provides attributes or partial solutions of value.

How You Can Participate

Submissions will be accepted through the Vulcan platform – **CLICK HERE TO SUBMIT**.
White paper submission format and template are on our website – **CLICK HERE TO LEARN MORE & DOWNLOAD**.
Vulcan submission instruction sheet – **DOWNLOAD THE PDF**.

Teaming Opportunities: Interested in teaming with other companies for a whitepaper solution? Fill out **this form** NLT 5:00 p.m. Eastern on 22 September 2025. Your capabilities and information will be shared with other companies interested, as well. All information provided will be sent out on or about 23 September to any company filling out the form.

To learn more about how to use Vulcan, please refer to this information on the CFIC website - https://www.cyberfic.org/joinvulcan.

Questions?

For submission-related questions, please contact Brandon Sizemore at bsizemore@cyberfic.org and Amanda Green at agreen@cyberfic.org.

DISCLAIMERS:

An award under 10 U. S. Code, Section 2371b may result in award of a follow-on production in accordance with 10.U.S.C. 2371(f). Upon determination that the competitively awarded prototype project(s) has been successfully completed, and subject to the availability of funds, the prototype project(s) may result in the award of a follow-on production contract or transaction without the use of competitive procedures. Such awards may include multiple phases.

Non-Government advisors may be used in the evaluation of submissions and will have signed Non-Disclosure Agreements (NDAs) with the Government. The Government understands the information provided in this announcement is presented in confidence and may contain trade secret or commercial or financial information

and agrees to protect such information from unauthorized disclosure to the maximum extent permitted and as required by law. An organization's participation in any part of the selection process under this announcement indicates concurrence with the aforementioned use of contractor support personnel.