

<https://sam.gov/workspace/contract/opp/b6b00811ee9a49f1b4c32965c89dd696/view>

Persistent Cyber Training Environment (PCTE) Cyber Range Development Software Application Project (Simulated Internet for Cyber Range Training Events)

Active

Opportunity

Notice ID

PCTERange-FY2026

Related Notice

(blank)

Contract Opportunity Type

Sources Sought

Contract Line Item Number

(blank)

Inactive Dates

Dec 31, 2026

Inactive Policy

Manual

Response Date

Jul 14, 2026 4:00 PM EDT

Published Date

Jun 22, 2026 10:11 AM EDT

Department/Ind. Agency

DEPT OF DEFENSE

Sub-tier

DEPT OF THE ARMY

Major Command

AMC

Sub Command 1, 2, 3

ACC

ACC-CTRS

ACC-ORLANDO

Office

W6QK ACC-ORLANDO

Classification

Original Set Aside

No Set aside used

Product Service Code

DA10 - IT AND TELECOM - BUSINESS APPLICATION/APPLICATION DEVELOPMENT SOFTWARE AS A SERVICE

NAICS Code

541519 - Other Computer Related Services

Place of Performance

(blank)

Initiative

None

Description

Request for Information (RFI)

Title: Persistent Cyber Training Environment (PCTE) Cyber Range Development Software Application Project (Simulated Internet for Cyber Range Training Events [Grey Space])

Issued By: Army Contracting Command Orlando in support of PEO STRI, PM CT2, PdM CRT PCTE

Issue Date: 18 June 2026

Response Due Date: 14 July 2026

Introduction

The Capability Program Executive Simulation Training, Test and Threat (CPE ST3), Program Manager Cyber Test and Training (PM CT2), Product Manager Cyber Resilience and Training (PdM CRT), Persistent Cyber Training Environment (PCTE) is seeking information from vendors and technology providers regarding a **simulated internet capability** (often called a Cyber Range or Grey Space Network). The purpose of this RFI is to explore available capabilities with a focus on realism, scale, and control.

This RFI is **not a solicitation** for proposals but rather a means to gather information for potential future procurement. Vendors are encouraged to provide detailed responses that address the requirements outlined below.

PCTE is built on a hierarchical, two-plane architecture: a **Control Plane (CP)** hosts hardened, accredited services (training portal, help-desk, dashboards, etc.) and provisions resources, while a logically isolated **Event Plane (EP)** runs virtual machines, containers, and software-defined networking to create dynamic cyber-range environments; the platform is deployed across regional compute/storage (RCS) sites and newer enterprise compute/storage (ENT) sites, leveraging VMware Cloud Foundation, NSX-T for SDN, F5 edge firewalls, and Red Hat SSO for authentication.

Objectives

The primary objectives of the simulated internet capability are:

To create a **realistic and highly scalable** cyber range environment / Grey Space Network for cybersecurity training and exercises.

To generate **realistic background traffic**.

Capture vendor specify platform's maximum throughput (Gbps) and concurrent session generation limits for background traffic. Assess vendor support for **advanced protocol states**, specifically: **Domain Name System Security Extensions** (DNSSEC) validation, Border Gateway Protocol (BGP) hijacking scenarios, **Hyper Text Transfer Protocol Secure** (HTTPS) inspection/decryption capabilities, and the simulation of localized, autonomous root-CA hierarchies.

To integrate with existing and future PCTE on-prem and cloud **security tools, network environments, and cloud infrastructure**.

To ensure high levels of PCTE functionality, **security, automation, and reporting capabilities**.

Concept of Operations

1. Purpose

The Simulated Internet within the Persistent Cyber Training Environment (PCTE) provides a realistic, controlled, and isolated network ecosystem that emulates the complexity and unpredictability of the real-world internet. Its primary purpose is to support persistent, scalable, and repeatable cyber training, mission rehearsal, and cyber operations experimentation for military and allied users, without risk to actual networks.

2. Objectives

Realism: Accurately mimic internet services, protocols, and user behaviors to provide authentic training scenarios.

Isolation: Ensure complete separation from live networks to prevent unintended impacts or data leakage.

Scalability: Support a wide range of training events, from small team exercises to large-scale, multi-organization operations.

Repeatability: Enable rapid reconfiguration and reset of the environment for multiple training iterations.

Observability: Provide robust monitoring, logging, and after-action review capabilities.

3. Operational Overview

3.1 Environment Composition

Core Internet Backbone: Simulated ISPs, backbone routers, and peering points.

Public Services: Emulated DNS, web, email, social media, and cloud services.

User Population: Automated user agents generating realistic traffic and behaviors.

Adversary Infrastructure: Simulated threat actors, botnets, and command-and-control (C2) servers.

Defensive Infrastructure: Blue team tools, sensors, and monitoring systems.

3.2 User Roles

Trainees: Blue, red, and purple team members conducting operations.

Instructors/Controllers: Scenario designers, exercise controllers, and observers.

Support Staff: System administrators and technical support personnel.

4. Key Functions

4.1 Scenario Generation

Dynamic Topology Creation: Automated deployment of network topologies and services based on exercise requirements.

Service Emulation: Realistic simulation of internet services (web, DNS, email, etc.) with configurable vulnerabilities and behaviors.

User Simulation: Automated generation of benign and malicious user traffic.

4.2 Exercise Execution

Isolated Operations: All activities occur within the simulated environment, with no external connectivity.

Attack/Defense Play: Red teams conduct offensive operations; blue teams defend; purple teams coordinate and analyze.

Live Monitoring: Real-time visibility into network and host activities for both participants and observers.

4.3 Data Collection and Analysis

Comprehensive Logging: Capture of all network, host, and user activity for after-action review.

Performance Metrics: Measurement of trainee actions, response times, and mission outcomes.

Replay and Debrief: Ability to replay scenarios for learning and assessment.

5. Security and Isolation

Physical/Logical Segregation: Use of air-gapped or logically isolated infrastructure.

Access Controls: Strict authentication and authorization for all users.

Reset and Sanitization: Automated environment reset and data sanitization between exercises.

6. Scalability and Flexibility

On-Demand Provisioning: Rapid instantiation of new environments for concurrent exercises.

Modular Design: Ability to add or remove services, users, and adversary elements as needed.

Integration: Support for interoperability with other training systems and federated ranges.

Requested Information

Vendors should provide information on the following aspects:

Core Capabilities & Infrastructure

Describe your software capability cyber range / Grey Space Network's **architecture and scalability**. Include a description of the hardware that would best meet your software's architecture. Identify scaling limitations in your current architecture.

Does your solution support **on-premises, cloud-based, and/or hybrid deployment**?

How does the software solution **simulate realistic background traffic** (web browsing, email, IoT)?

What types of **network environments and protocols** does your platform support?

Does your system support **autonomous entities** that interact naturally with services?

Does your system replicate global routing tables and autonomous systems (ASNs)?

The PCTE current architecture has multiple Enterprise Platforms interconnected. Would your simulated internet solution be a standalone capability or could it be integrated into PCTE current architecture?

Describe your solution in terms of usage visibility (CPU, memory, and storage).

Provide data on the maximum number of simulated nodes and concurrent sessions.

Is your simulated internet solution compatible with VMware, Docker containers, and cloud providers?

Can your solution use public IP ranges without leaking traffic to the real internet?

Describe how your solution maintains strict isolation between its management/orchestration services (aligning to the PCTE Control Plane) and the actual traffic-generation/range nodes (aligning to the PCTE Event Plane) (reference Fig A-2).

Identify what functional components are included in the product's greyspace simulated internet capability, such as simulated social media platforms, online services, messaging tools, authentication infrastructure, email, web search or other web based services.

Security & Compliance

What security measures are built into the platform?

In terms of air-gapped execution, can your entire capability run completely isolated from the live internet?

How does your solution ensure **data integrity and confidentiality**?

How does your application securely execute, control, and contain malicious traffic and non-STIG-compliant grey space entities within the Event Plane without jeopardizing the security posture of the underlying container/hypervisor layer?

User Experience & Training Capabilities

Does your solution include a user-friendly, **interactive dashboard and reporting tools**?

Can the software application support **multi-user collaboration, remote access, and team-based exercises, using the PCTE Enterprise architecture (reference Fig A-1)**?

Integration & Compatibility

Is there an **API for custom integrations**?

Detail how your application integrates with the government-provided API Gateway and Message Bus. Is your solution natively capable of publishing and subscribing to Apache Kafka/RabbitMQ events (or similar standard message buses) to sync simulation state with external PCTE tools?

Cost & Licensing

What pricing models do you offer (e.g., subscription-based, software as a service, perpetual license, government purpose rights, are portions open-source)?

Are there any **hardware or infrastructure requirements or dependencies**?

What are the estimated costs for **scaling up the system, on-premises and in the cloud**?

Response Submission

Interested parties should submit their responses in **electronic format (PDF or Word document)** by **10 July 2026** to:

Contact Person:

ACC-O POC: Jaime Morrison

PCTE POC: Juan B. Orozco, PCTE Acquisition Product Lead

Alfredo Betancourt, PCTE Chief Engineer.

Email:

ACC-O POC: jaime.morrison.civ@army.mil

PCTE Acquisition: juan.b.orozco.civ@army.mil

PCTE Engineering: alfredo.o.betancourt.civ@army.mil

Phone:

ACC-O Phone Number, kurt.l.kleinlein.civ@army.mil, 321-235-7523

Responses should include a **company profile**, relevant **case studies**, and any additional **marketing materials or whitepapers** that provide insights into the proposed solution.

Disclaimer

This RFI is **for information-gathering purposes only** and should not be construed as a commitment by PEO STRI / PM CT2 to issue a solicitation or award a contract. No compensation will be provided for responding to this request.

Thank you for your interest in supporting the development of a next-generation **PCTE Cyber Range Software Application** Simulated Internet for Cyber Range Training Events. We look forward to your insights and responses.

Contact Information

Primary Point of Contact

Jaime Morrison

Email

jaime.morrison.civ@army.mil

Phone Number

520-714-5618

Alternative Point of Contact

Kurt Kleinlein

Email

kurt.l.kleinlein.civ@army.mil

Phone Number

(blank)

Contracting Office Address

12211 SCIENCE DR

(No Street Address 2)

ORLANDO, FL 32826-3224 USA

Attachments/Links

Links

No links have been added to this opportunity.

Attachments

No attachments have been added to this opportunity.