HIGH PERFORMANCE COMPUTING MODERNIZATION PROGRAM

RESEARCH PROJECT #: HPCMP-HIP-25-045

Commercial Solutions for Classified (CSfC) Investigation for the Defense Research and Engineering Network (DREN) Network of Opportunity Rapid Deployment Kit (NORDK)

About HPCMP:

The DoD High Performance Computing Modernization Program (HPCMP) provides an HPC ecosystem of centers, networking and software for DoD research, development, test, and evaluation as well as acquisition engineering missions. The Defense Research and Engineering Network (DREN) is a component of the HPCMP and provides wide area networking support between HPCMP users and centers. DREN connects over 200 DoD and DoD contractor sites across the US including Alaska and Hawaii. DREN offers a high bandwidth, low latency, low jitter, full service wide area network solution. DREN also offers an ideal platform for next generation network protocol and cyber security research.

RESEARCH LOCATION: Wright-Patterson AFB, OH

PROJECT DESCRIPTION:

The DREN NORDK kit is a mobile equipment stack meant to be deployed to remote US military locations and be connected back to DREN using any circuit of opportunity including geosynchronous or Low Earth Orbit (LEO) satellite services. The NORDK equipment stack currently includes an NSA Type 1 encrpytor. Because NORDK is deployed in remote locations, it can be difficult to ship COMSEC accountable equipment and key material where it is needed. This project will build on the lessons learned from the HIP internship in FY24. This project will implement capabilities not previously completed (such as implementation of management tools for red/gray/black zones) and investigate additional capabilities that are required by NSA (such as full packet capture/storage and automated security log reviews).

Develop potential options for full CSfC implementation in the DREN NORDK environment to be used at remote US military locations. Demonstrate a potential end-to-end solution in the laboratory suitable for deployment in real-world situations. If time permits, investigate/recommend CSfC endpoint and back-end solutions that can be used by DREN staff not in SCIF locations for remote access to SDREN resources. Availability, usability, cost, and performance are critical evaluation factors when considering CSfC devices used by the DREN staff.

Additional questions to be answered through this research and demonstration project:

- How should the management of a CSfC solution be implemented for the red/gray/black zones at an enterprise network level?
- What technical solutions exist to implement 30 days of full packet data capture and automated security log reviews?
- What approved turn-key solutions exist to support remote access to SDREN resources by DREN staff not in SCIF locations? What CSfC endpoint and backend systems are recommended?

Under the guidance of a mentor, the intern will:

- Understand Commercial Solutions for Classified (CSfC) requirements and internship project results from FY24.
- Re-implement as necessary the test bed created in the FY24 internship project.
- Investigate, explore, and demonstrate solutions for management of CSfC red/gray/black zones.
- Research and implement in the testbed technical solutions for 30 days of full packet data capture.
- Research and implement in the testbed technical solutions for automated security log reviews.
- Investigate and recommend approved turn-key solutions to support remote access to SDREN resources by DREN staff.
- Prepare appropriate documentation including reports, presentations, posters, etc. as needed.

This internship will benefit the intern through involvement in a professional HPC work environment and the opportunity to contribute to a meaningful professional project. The intern will also benefit from professional mentorship and the opportunity to improve communication skills through written reports and oral presentations. The intern will get a sense of work in a DoD environment and potential future opportunities for a professional DoD career.

ANTICIPATED START DATE:

May 2025 – Exact start dates will be determined at the time of selection and in coordination with the selected candidate.

QUALIFICATIONS:

The ideal candidate will be enrolled as an undergraduate student in Computer Engineering, Electrical Engineering or Computer Science. Coursework or experience in data networking, Internet fundamentals, cyber security, data encryption, and Windows or Linux configuration is desirable.

ACADEMIC LEVEL:

Degree received within the last 60 months or currently pursuing:

- Associate's
- Bachelor's

DISCIPLINE NEEDED:

- Computer, Information, and Data Sciences
- Engineering
- Science and Engineering related