Next Generation Cyber Infrastructure Apex Program

Homeland Security
Science and Technology

PROTECTING THE NATION'S CYBER INFRASTRUCTURE

Cyberattacks on the necessary, every day services that make up critical infrastructure can seriously threaten national security. The Department of Homeland Security Science and Technology Directorate (S&T) has identified three major challenges:

- Adversaries are infiltrating critical infrastructure systems and networks without our knowledge.
- Understanding of the cyber situation is inaccurate, incomplete, or only achieved forensically and after the infiltration has occurred.
- Network owners/operators lack strong methods to respond to and mitigate the impact of attacks while maintaining adequate operating capacity.

NGCI APEX PROGRAM FOCUS

S&T's Next Generation Critical Infrastructure (NGCI) Cyber Apex Program aims to identify vulnerability gaps within critical infrastructure sectors and develop new technologies. The Cyber Apex Program is currently focused on topics related to the nation's financial sector, though the tools and technologies developed will later be adapted for other sectors.

- **Network Characterization** provides real-time understanding of a network, including the internal communication patterns of connected assets, to enable immediate anomaly detection and rapid response to cyber incidents.
- **Data Protect** ensures confidentiality, integrity, and availability of sensitive data at all times.
- **Advanced External User Authentication** focuses on non-password-based, multi-factor authentication for external users, such as customers, business partners, and third-party suppliers.
- **Dynamic Defense** changes external and internal network layouts so they are harder for adversaries to probe, breach, and exploit.

CUSTOMER AND STAKEHOLDER ENGAGEMENT

S&T's Cyber Apex Program has established Cyber Apex Review Teams (CART) to define and prioritize requirements and evaluate tools that can reduce risk and vulnerabilities by improving the security and defenses of the financial services critical infrastructure.

The CART is composed of the Department of the Treasury as well as chief information security officers and cybersecurity experts. Financial services organizations can request to join the CART by contacting CyberApex@hq.dhs.gov.

To identify the most promising technology solutions, the Cyber Apex Program work is with a consortium of vendors able to provide solutions to the financial sector. For more information about joining the consortium, please contact info@cyberapexsolutions.com.

APPROACH

The Cyber Apex Program leverages existing federally funded and private sector programs to conduct a variety of research efforts:

- Developing a sector-wide understanding of needs for each topic area.
- Analyzing identified needs and recommending relevant metrics.
- Researching current and emerging technologies relevant to each topic.
- Developing a solicitation to the Consortium with project requirements. Vendors within the Consortium can then submit proposals.
- Reviewing and selecting the proposals with which to move forward.
- Testing selected solutions in a representational/ operational environment and evaluating the results against the project requirements.