

# DHS Science and Technology Directorate

## Next Generation Cyber Infrastructure Apex Project

### Protecting the Nation's Cyber Infrastructure

Cyberattacks threaten national security by undermining information-dependent critical infrastructure. The Department of Homeland Security (DHS) identified 16 critical infrastructure sectors designated in the Presidential Policy Directive (PPD-21) - Critical Infrastructure Security and Resilience. Subsequently, DHS's Science and Technology Directorate's (S&T) Cyber Security Division (CSD) and the financial services sector identified three major challenges:

- Adversaries are infiltrating our systems and networks without our knowledge,
- The sectors' understanding of the cyber situation is inaccurate, or only achieved forensically and after the infiltration has occurred, and
- Network owners/operators lack strong ways to respond and mitigate the impact of adversaries on our systems and still allow the sector to maintain adequate operating capacity.

### NGCI's Apex Project Description and Focus

The Next Generation Cyber Infrastructure (NGCI) Apex project addresses these challenges by providing the financial services sector with the technologies and tools to confront when advanced adversaries attack cyber systems and networks.

NGCI will concentrate on delivering capabilities identified by financial sector to address five primary functional gaps:

- ***Dynamic Defense:*** Present changing external and internal network layouts that are harder for adversaries to probe, breach and exploit, significantly increasing the economic costs for a potential attacker.
- ***Network Characterization:*** Provide 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.
- ***Malware Detection:*** Deliver improved ability to detect and prevent the execution of malware in all formats and to predict the likely evolution of malware code.
- ***Software Assurance:*** Decrease false positive rates and accelerating the analytic timeline to increase the likelihood of finding software defects in complex software code.
- ***Insider Threat:*** Deliver the capability to detect data exfiltration below the network level, as well as predict and model potential insider threats.

### Customer and Stakeholder Engagement

The initial phase evaluates developing tools that can help the financial services sector defend itself from threats, done in collaboration with the Department of Treasury, the DHS National Protection and Programs Directorate, and the U.S. Secret Service.

Working with sector chief information security officers, NGCI will establish the Cyber Apex Review Team (CART) to define prioritized requirements, plan and execute test and evaluation activities, and carry out the most appropriate methods of technology deployment and transition.

### Approach

NGCI will leverage existing federally funded and private sector research efforts that provide the required capabilities. It will use a flexible but repeatable technology development approach with five distinct phases:

1. **Forge for candidate technologies**, based on requirements provided by the CART. This will include industry engagements, technology scanning, and Transition to Practice (TTP) candidates.
2. **Demonstrate, test, and evaluate candidate technologies** using a representational architecture the CART institutions will help define.
3. **Further test and evaluate successful products in company-specific test environments.** Throughout the process, CART engagement and feedback, using a build-test-repeat model for system development and testing, will be highly encouraged.
4. **Integrate and refine technology products** as needed, based on test and evaluation results.
5. **Develop and implement appropriate transition or commercialization strategy** to be provided by the financial institutions' internal operations, managed security services providers, an entrepreneurial or venture capital-supported model, or open source options.

### Timeline

The first three years of the Apex project will focus on deployment and transition of cutting edge technologies to the financial services sector. In later phases, the tools and technologies developed for the financial sector will be adapted to address a broader set of sectors, including the government, energy, and communications sectors.



**Homeland  
Security**

Science and Technology

To learn more about the Cyber Apex project, contact:  
Cyber Security Division (CSD), Next Generation Cyber Infrastructure  
(NGCI) Apex Project - email: [CyberApex@hq.dhs.gov](mailto:CyberApex@hq.dhs.gov)