DHS Science and Technology Directorate

Next Generation Cyber Infrastructure Apex Program

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, the DHS Science and Technology Directorate's 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, incomplete, or only achieved forensically and after the infiltration has occurred, and
- Network owners/operators lack strong methods to respond and mitigate the impact of adversaries on our systems, while still allowing for the sector to maintain adequate operating capacity.

NGCI's Apex Program Description and Focus

The Next Generation Cyber Infrastructure (NGCI) Apex Program addresses these challenges by providing the financial services sector with the technologies and tools to confront advanced adversaries when they attack U.S. cyber systems and networks. NGCI will concentrate on delivering capabilities identified by the 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

Conducted in collaboration with the U.S. Department of the Treasury, the initial phase evaluates tools that can help the financial services sector defend itself from threats.

Working with sector chief information security officers, NGCI has established 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 leverages existing federally funded and private sector research efforts that provide the required capabilities. It uses a flexible, repeatable technology development approach with five distinct phases:

1. **Forage for candidate technologies**, based on requirements provided by the CART, including industry engagements, technology scanning, and Transition to Practice (TTP) candidates.
2. **Demonstrate, test, and evaluate candidate technologies** using a representational architecture the CART members 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, is highly encouraged.
4. **Integrate and refine technology products** as needed, based on test and evaluation results.
5. **Develop and implement appropriate transition or commercialization strategies** through 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 program 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 program, visit Homeland Security Science and Technology / or contact: Cyber Security Division (CSD), Next Generation Cyber Infrastructure (NGCI) Apex Program - email: CyberApex@hq.dhs.gov

2016–1–29