**

*DEPARTMENT OF HOMELAND SECURITY*

*SCIENCE AND TECHNOLOGY DIRECTORATE*

Next Generation Cyber Infrastructure (NGCI) Apex Program Management Plan

Version [1.2]

TBD, 2016

**APPROVALS**

PMP Approvals:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Eric Harder

Next Generation Cyber Infrastructure (NGCI)

Apex Program Manager Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Greg Wigton

Next Generation Cyber Infrastructure (NGCI)

Apex Deputy Program Manager Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Douglas Maughan, Ph.D. Date

Cyber Security Division Director

Homeland Security Advanced Research Projects Agency (HSARPA)

U.S. Department of Homeland Security (DHS),

Science & Technology (S&T) Directorate

**Record of Changes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Figure # or Section #** | **A/M/D\*** | **Description of Change / Rationale** |
| 1.0 | 08/2015 |  | A | Initial Draft of PMP |
| 1.2 | 10/2016 |  | A | Added Silicon Valley Innovation Program Initiative |
| 1.4 | 04/2017 |  | M |  |
|  |  |  |  |  |
|  |  |  |  |  |

\* A-Added, M-Modified, D-Deleted

**Contents**

[1 Program Summary 2](#_Toc467154454)

[1.1 Background and Purpose 2](#_Toc467154455)

[1.2 Customers and Stakeholders 2](#_Toc467154456)

[1.3 Other Transaction Authority (OTA) 2](#_Toc467154457)

[1.4 Silicon Valley Innovation Program (SVIP) 2](#_Toc467154458)

[1.5 Deliverables 2](#_Toc467154459)

[1.6 Schedule and Budget Summary 2](#_Toc467154460)

[1.7 Program Organization 2](#_Toc467154461)

[1.7.1 Federal Government Participation (Level 1) 2](#_Toc467154462)

[1.7.2 Cyber Apex Review Team (Level 2) 2](#_Toc467154463)

[1.7.3 CART + Cyber Apex Consortium Contractor (Level 3) 2](#_Toc467154464)

[1.7.4 Functions of DHS S&T PMO 2](#_Toc467154465)

[1.7.5 Functions of Cyber Apex Consortium Contractor 2](#_Toc467154466)

[1.8 Program Benefits 2](#_Toc467154467)

[1.8.1 New Capabilities/Technologies 2](#_Toc467154468)

[1.8.2 New Intellectual Property (IP) 2](#_Toc467154469)

[1.8.3 Public Access of Federally Funded Scientific Research 2](#_Toc467154470)

[1.8.4 Data Management 2](#_Toc467154471)

[2 Requirements 2](#_Toc467154472)

[2.1 Requirements Management Plan 2](#_Toc467154473)

[2.2 Customer Engagement 2](#_Toc467154474)

[2.3 Customer Requirements 2](#_Toc467154475)

[2.4 Key Functions and Desired Performance Requirements 2](#_Toc467154476)

[2.5 Project Effort Metrics 2](#_Toc467154477)

[3 Technology and Innovation 2](#_Toc467154478)

[3.1 Core Technology 2](#_Toc467154479)

[3.1.1 Cyber Apex Consortium Approach 2](#_Toc467154480)

[3.1.2 SVIP Cyber Apex Approach 2](#_Toc467154481)

[3.1.3 Logistical Considerations 2](#_Toc467154482)

[4 Program Management 2](#_Toc467154483)

[4.1 OTA Project Effort Execution Process 2](#_Toc467154484)

[4.2 SVIP Cyber Apex Project Effort Execution Process 2](#_Toc467154485)

[4.3 Scope Management 2](#_Toc467154486)

[4.3.1 Scope Control Plan 2](#_Toc467154487)

[4.4 Schedule Management 2](#_Toc467154488)

[4.4.1 Milestones/Deliverables 2](#_Toc467154489)

[4.4.2 Schedule Control Plan 2](#_Toc467154490)

[4.5 Cost Management 2](#_Toc467154491)

[4.5.1 Cost Estimate 2](#_Toc467154492)

[4.5.2 Cost Baseline 2](#_Toc467154493)

[4.5.3 Cost Control Plan 2](#_Toc467154494)

[4.6 Status Reporting 2](#_Toc467154495)

[4.6.1 Deliverable tracking 2](#_Toc467154496)

[4.6.2 Configuration Management 2](#_Toc467154497)

[4.7 Human Systems Integration (HSI) 2](#_Toc467154498)

[4.8 Security and Classification 2](#_Toc467154499)

[5 Risk Management 2](#_Toc467154500)

[5.1 Risk Management Plan 2](#_Toc467154501)

[5.2 Risk Identification and Assessment 2](#_Toc467154502)

[5.2.1 Technical Risks 2](#_Toc467154503)

[5.2.2 Programmatic Risks 2](#_Toc467154504)

[5.2.3 Operational Risks 2](#_Toc467154505)

[5.3 Risk Register 2](#_Toc467154506)

# Program Summary

This document contains the plan for managing the Next Generation Cyber Infrastructure (NGCI) Apex program.

## Background and Purpose

The United States critical infrastructure sectors have an immediate need for technologies that can adequately detect, defend, protect, restore, and respond, to sophisticated cyber threats. The Next Generation Cyber Infrastructure (NGCI) Apex program will identify, test, evaluate and deploy cutting-edge technologies to deter cyber-attacks against the financial sector. The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate has partnered with the Department of the Treasury and the U.S. financial sector, to deliver technologies designed to fill the existing functional and technological gaps in the sector. The NGCI Apex program includes the following objectives to be performed by the DHS S&T NGCI Apex Program Management Office (PMO), the Other Transaction Authority (OTA) contractor, and by vendors and supporting organizations:

**Objective 1**: Partner with financial sector critical infrastructure institutions to develop and integrate technologies that fill cybersecurity gaps; reducing risk through the improvement of security.

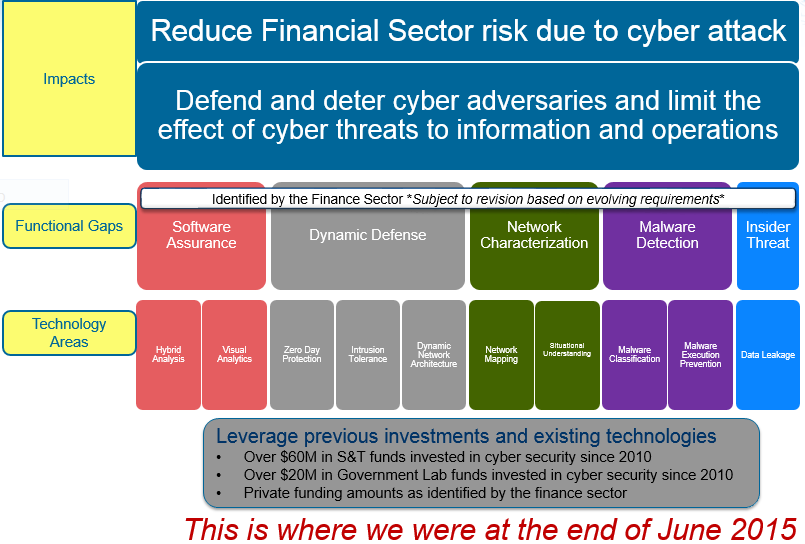
**Objective 2**: Test, evaluate, and integrate candidate technologies in both, representational and institution-specific (operational) environments using a build-test-repeat model.

**Objective 3**: Transition successful prototype technologies to private sector / commercial use.

The U.S. financial and banking industry is one of the sixteen national critical infrastructure sectors, as defined by Executive Order (EO) 13636[[1]](#footnote-1) and Presidential Policy Directive (PPD) 21[[2]](#footnote-2). The resulting cybersecurity risk-based framework, outlined in EO 13636, is defined by the National Institute of Standards and Technology (NIST) Cybersecurity Framework[[3]](#footnote-3). Figure 1 illustrates the five NIST core functions that underlie the NGCI approach. These framework functions are also referred to as Operational Functions in the Financial Services Sector (FSS). Figure 2 illustrates the capability gaps identified by the FSS. The NGCI Apex program will work to address the cybersecurity gaps affecting the FSS by utilizing the NIST Cybersecurity Framework.



**Figure 1 - NIST Cybersecurity Framework Core Functions**



**Figure 2 - Financial Services Sector Capability Gaps (as of June 2015)**

## Customers and Stakeholders

The NGCI Apex stakeholders include representatives from the largest recognized U.S. financial & banking institutions, representatives from the Department of Treasury, and representatives from DHS. These financial institutions are members of the Cyber Apex Review Team (CART) along with DHS and the Department of the Treasury. CART members constitute the principal stakeholders of the NGCI Apex program. Additional stakeholders include the Security Industry and Financial Markets Association (SIFMA) and Financial Services Sector Coordinating Council (FSSCC).

## Other Transaction Authority (OTA)

The NGCI Apex program will leverage an Other Transaction Authority (OTA) agreement, authorized under Title 10 USC § 2371, for the majority of the work to be performed. OTA refers to an agreement that is used by DHS for research or prototype projects, and is not a procurement contract, grant, or cooperative agreement. Because such agreements are primarily defined in terms of what they are not (i.e., are defined in the negative), OTAs can take an unlimited number of potential forms. This authority, when used selectively, is a vital tool that will help DHS S&T to rapidly achieve the goals of the NGCI Apex program. Benefits of this approach include:

* Federal funding can be obligated quickly
* An OTA is not a contract, grant or cooperative agreement. As a result, an OTA is not subject to the Federal Acquisition Regulation (FAR) or its supplements
* Government rights to intellectual property are generally minimal and negotiable
* The Government is allowed to openly discuss requirements and to collaborate with contractors to obtain the best approach for developing technology

The Secretary of DHS is authorized by statute to enter into transactions other than procurement contracts, grants, and cooperative agreements in carrying out activities that:

* Support basic, applied, and advanced research and development (R&D) that would promote homeland security
* Advance the development, testing, and evaluation of critical homeland security technologies
* Accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities

Responsibilities of the OTA and PMO are covered in more detail in sections 1.6.4 and 1.6.5.

## Silicon Valley Innovation Program (SVIP)

In addition to the Cyber Apex Consortium contractor, the NGCI Apex program will leverage the recently launched DHS S&T Silicon Valley Innovation Program (SVIP) to broaden the search for innovative technology solutions from technology startups and vendors. One of the key differences between SVIP and NGCI Apex is in the approach to technology acquisition/transition. The NGCI Apex OTA “Cyber Apex Consortium” will place significant emphasis on testing and evaluation (T&E), whereas, the SVIP Cyber Apex arrangement focuses more on technology development. SVIP is designed to accelerate the transition of innovative technologies and solutions into DHS programs and the Homeland Security Enterprise (HSE). SVIP makes smaller, incrementally funded awards to start-up companies using a four-phased approach[[4]](#footnote-4).

Leveraging the SVIP will enable the NGCI Apex program to canvass a larger quantity of startup / vendor candidates for technology solutions capable of addressing cyber vulnerability gaps within the financial sector. Benefits of this approach for the FSS include:

* Spark FS cyber innovative technology solutions from technology startups and vendors
* Increase quality and quantity of companies than typical contract vehicles
* Emphasis on developmental technologies (less mature technologies)
* Only government employees can review solutions throughout the selecting, prototyping and testing phases
* Technology solutions will transition to FSS Partner(s) for additional piloting. On occasion, some solutions may transition to the Cyber Apex Consortium OTA for additional testing

## Deliverables

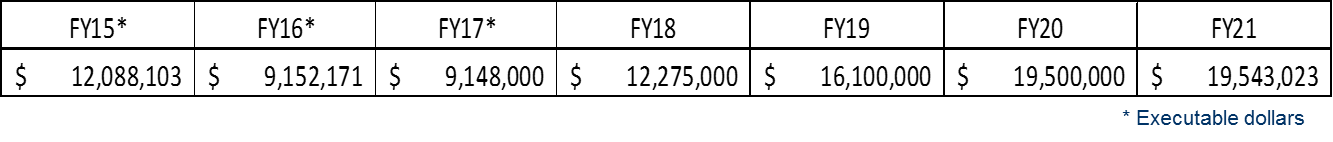
See section 4.4.1

## Schedule and Budget Summary

The high-level program schedule shown in figure 3 is an example of the NGCI Apex program schedule. The five-year budget summary is given in Table 1.



**Figure 3 - High-Level NGCI Apex Program Schedule**



\* Executable dollars

**Table 1 - NGCI Apex Budget Summary**

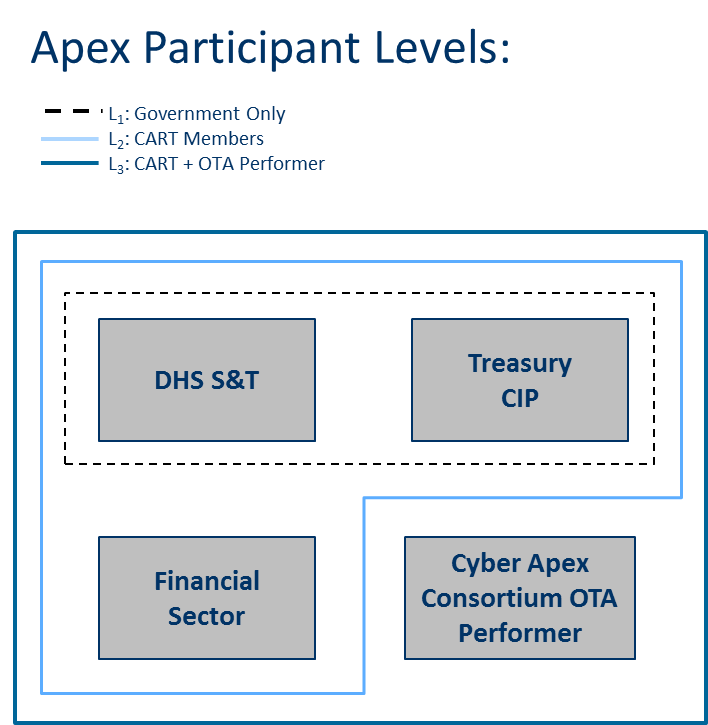
## Program Organization

The NGCI Apex program is composed of a variety of groups responsible for its overall success. There are different levels through which all of the tasks, management, and oversight are performed. Each level is described in more detail below (illustrated in Figure 4). The levels are as follows:

**Level 1:** Federal Government (DHS S&T PMO and U.S. Treasury Department)

**Level 2:** Federal Government (Level 1) and Financial Services Sector (also known as the CART)

**Level 3:** CART and Cyber Apex Consortium Contractor (performer)



**Figure 4 - NGCI Apex Program Entities / Team Relationships**

### Federal Government Participation (Level 1)

The NGCI Apex Federal Government Participation is shown in Figure 6 and includes members of the DHS S&T PMO and representatives from the Department of Treasury. For DHS S&T PMO contact information, refer to Table 2. The Federal Government level (Level 1), in particular DHS S&T, as the sponsor of this program, holds the ultimate decision-making authority in matters of funding and scope.

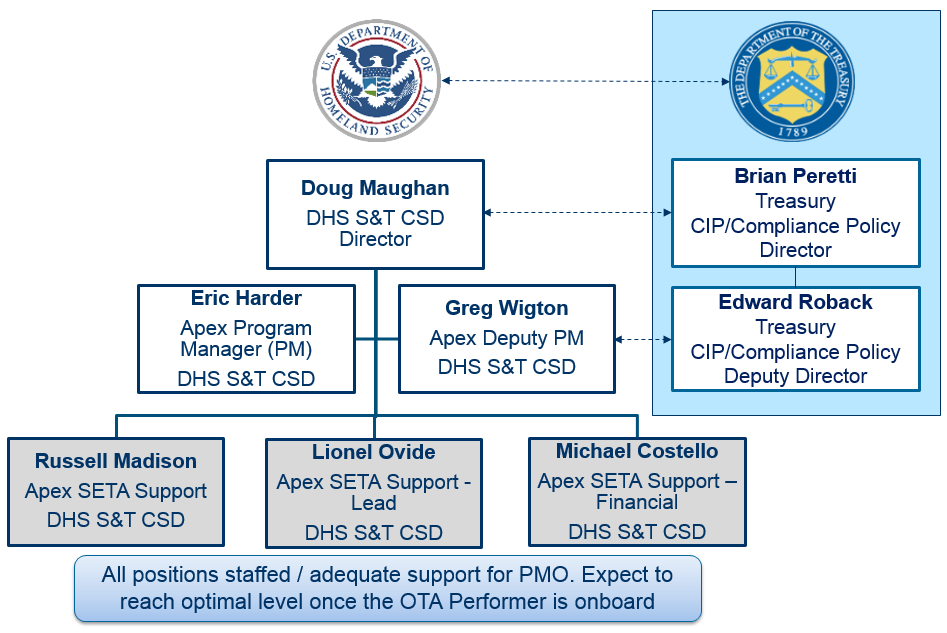
### Cyber Apex Review Team (Level 2)

The Cyber Apex Review Team (CART) consists of the Federal Government (as represented by DHS S&T PMO and the Department of Treasury), along with financial industry partners. The role of the CART is to set direction for the work performed by the Cyber Apex Consortium contractor through actively participating in regular CART meetings, by providing critical feedback, and by supplying needed information for internal surveys, polls or decisions. The CART’s responsibility is to provide input into the decision-making with regards to technical direction, solicitation requirements, proposal recommendations, and advancement of prototype technologies through developmental, operational, and transitional phases.

**NOTE:** Under the SVIP approach, the review of vendor proposals will be limited to Federal employees only. CART members may provide input to the criteria to consider for a successful application/award.

### CART + Cyber Apex Consortium Contractor (Level 3)

The Cyber Apex Consortium contractor, Cyber Apex Solutions, LLC (CAS), will conduct requirements gathering, technology foraging, metrics development, and end-user identification, for the critical infrastructure technology gaps identified by the CART. CAS will maintain a consortium of vendors that will be leveraged to supply technologies and solutions to the Financial Sector’s needs. CAS will evaluate consortium proposals and develop a recommendation package consisting of multiple vendors that is reviewed by the CART. The Federal Government (as defined in 1.7.1) will then make the final decision on the recommendation package. The CART and DHS S&T PMO will also oversee the development, testing, evaluation, and integration of technologies.



**Figure 5 - NGCI Apex Federal Government / Support Representatives**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Email | Phone |
| Eric Harder | **Program Manager** | **Eric.Harder@hq.dhs.gov** | **202-254-8723** |
| Greg Wigton | **Deputy Program Manager** | **Gregory.Wigton@hq.dhs.gov** | **202-254-6140** |
| Lionel Ovide | **Support Contractor (Lead)** | **Lionel Ovide@associates.hq.dhs.gov** | **202-254-6359** |
| Michael Costello | **Support Contractor (Finance)** | **Michael.Costello@associates.hq.dhs.gov** | **202-254-5722** |
| Laurel Buleza | **Support Contractor** | **Laurel.Buleza@associates.hq.dhs.gov** | **202-254-4837** |

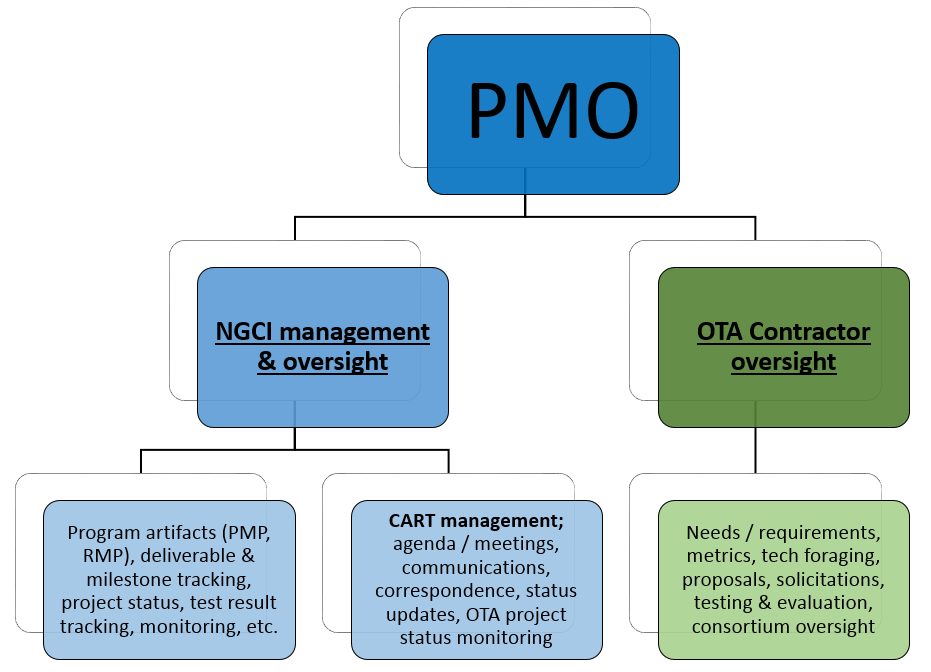
**Table 2 - DHS S&T PMO Contact Information**

### Functions of DHS S&T PMO

The responsibilities of the DHS S&T PMO differ in function and purpose from those of the Cyber Apex Consortium contractor. Although many activities and tasks will be transferred to the Cyber Apex Consortium contractor for execution, the DHS S&T PMO will administer, oversee, and manage the NGCI Apex program, including the Cyber Apex Consortium contractor. The DHS S&T PMO will make go/no-go decisions at specific points in the program lifecycle. See Figures 6 and 10 for specific DHS S&T PMO responsibilities. The DHS S&T PMO will:

* Monitor/track program milestones and deliverables
* Approve/disapprove solicitations for each technology area/project effort
* Determine type of testing to be conducted (representational, operational)
* Assist with the identification of end-users
* Approve technology areas and project efforts
* Review all testing & evaluation results
* Authorize advancement to next stage/phase (Go/No go)

In addition, the DHS S&T PMO will maintain the Program Management Plan (PMP), administer the Risk Management Plan (RMP) and maintain a separate risk register for specific DHS S&T PMO and Cyber Apex Consortium contractor risks. The DHS S&T PMO will also organize and chair regularly scheduled CART meetings. The SVIP Cyber Apex awards will be monitored by the DHS S&T PMO.

****

**Figure 6 - PMO Functions**

### Functions of Cyber Apex Consortium Contractor

The Cyber Apex Consortium contractor will oversee the development, integration, testing and evaluation, of selected prototype technologies. Deliverables will include items such as: needs analysis findings, Applied Research Report, monthly program plans, financial status reports, communications plans, solicitations/proposals, final reports, recommendation packages, etc.

The Cyber Apex Consortium contractor will focus on individual technology areas as directed by the CART (illustrated below):

**Individual Technology Area/Project Effort**

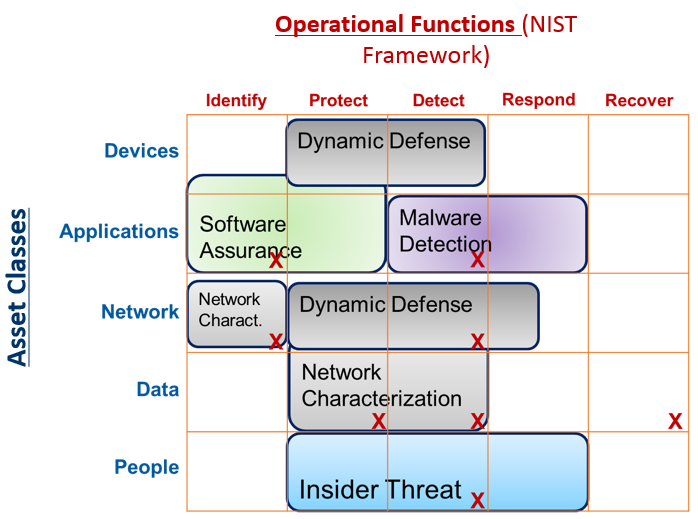
* **Requirements gathering (in collaboration with the CART)**
* **Technology foraging**
* **Metrics development**
* **Development and Testing Identification doc.**
* **Request for Proposals (solicitations)**
* **Findings Reports**

**Applied Research Report / Recommendation Package**

## Program Benefits

### New Capabilities/Technologies

The premise of the NGCI Apex program is to discover, develop, and transition new prototype technologies, designed to protect the overall critical infrastructure of the financial sector. New technologies will be deployed to identify, protect, detect, respond, and recover, from a wide range of evolving cyber threats across five identified asset classes: devices, applications, networks, data, and people. These technologies will be monitored to ensure they remain effective and relevant in the face of evolving threats. The CART has developed a matrixed approach to help identify the areas of focus for the NGCI Apex program (see Figure 8 below).

****

**Figure 8 - U-Matrix**

### New Intellectual Property (IP)

It is unknown how much IP will result from the collaboration and development of NGCI cyber technologies, therefor IP issues will be addressed in each individual Statement of Work (SOW).

### Public Access of Federally Funded Scientific Research

Upon publication of the DHS Plan to Support Increased Public Access to the Results of Research Funded by the Federal Government5, the NGCI Apex program will comply with the intent of the plan and develop the appropriate mechanisms to provide public access to peer reviewed journal articles that are funded by federal R&D after a prescribed embargo period. The NGCI Apex program will also maintain and update its publically accessible website with new or additional information as it becomes available.

### Data Management

Upon publication of the DHS Plan to Support Increased Public Access to the Results of Research Funded by the Federal Government5, the NGCI Apex program will comply with the intent of the plan and develop the appropriate data management plan if the electronic data sets created in the project fall under the purview of the DHS guidance.

# Requirements

## Requirements Management Plan

Requirements for each project effort are identified, ranked and approved by the CART. The Cyber Apex Consortium contractor is responsible for task management and sustainability while the DHS S&T PMO will monitor and track all vendor and Cyber Apex Consortium contractor deliverables outlined in section 6.4 (Deliverables Table) of the NGCI Program SOW. The DHS S&T PMO will provide the full spectrum of PMO oversight for the SVIP Cyber Apex effort.

## Customer Engagement

Refer to section 1.2. The FSS is both a customer and an end-user of the technologies scheduled for use within the NGCI Apex program. They are party to the FSSCC Memorandum of Understanding (MOU)[[5]](#footnote-5). The MOU authority is derived from section 302 of the Homeland Security Act of 2002. DHS, the Department of Treasury, and financial industry partners, convene on a monthly basis (may be adjusted once OTA is awarded). The CART serves to provide technical direction for the development of requirements, plans and approves T&E activities, metrics formulation, and other high-level decision-making for the NGCI Apex program. The CART will define and prioritize requirements, and provide input about the most appropriate methods of technology transition and adoption. However, under the SVIP Cyber Apex approach, the review of vendor proposals will be limited to Federal employees only and the Cyber Apex PMO will engage directly with the customer and vendor for synergy between stakeholders.

## Customer Requirements

Financial services partners continue to refine their cybersecurity gaps and needs assessments. Each CART meeting allows the DHS S&T PMO and the financial partners to further define the direction of proposed prototype technologies sought by the sector. Customer requirements will continue to evolve based on emerging cyber threats.

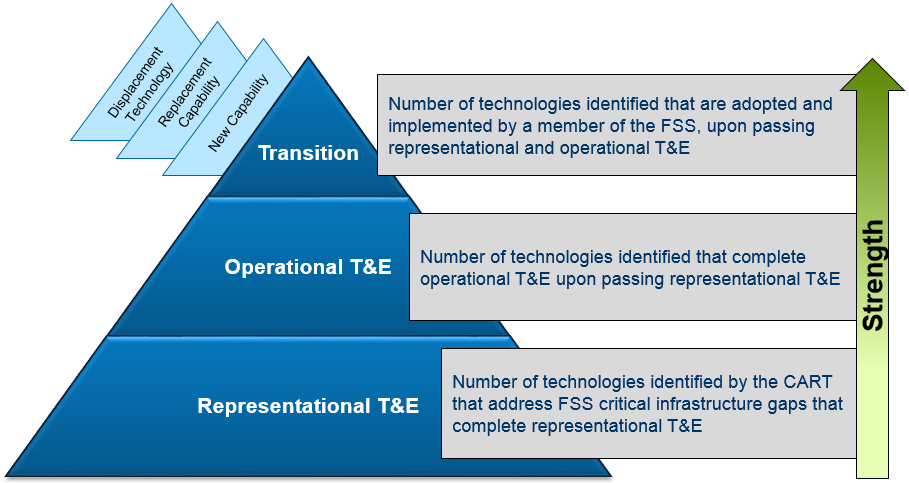
## Key Functions and Desired Performance Requirements

The NGCI Apex program will utilize a set of Key Performance Parameters to ensure maximum effectiveness is reached across the major areas of the program.

**Key Performance Parameters (KPP)**:

* CART Confidence
  + Characterizes the sentiment of the CART’s assessment of the program - measured by survey of participating members and participation rate. Original CART membership consist of 26 FSS institutions.
* Technology Foraging
  + Determined by the quality and relevance of foraged technology, from which recommendation packages are derived (critical to project effectiveness) - measured by a tech foraging survey and CART review.
* Applied Research Reports/Recommendation Packages
  + Will be used to assess the potential and transition likelihood of candidate technologies for each technology area (within each project effort). This includes negative findings (no relevant technologies to test for given technology area).
* Testing & Evaluation (T&E) satisfaction
  + This parameter characterizes the extent to which FSS organizations find the testing and evaluation efforts acceptable - measured through CART surveys.
* Market Coverage (Transition)
  + Determined by the extent to which FSS institutions engage and transition the evaluated candidate technologies through 1) direct pilot programs, 2) managed security service providers (MSSP), 3) venture capital entities, or 4) open source.

## Project Effort Metrics

Metrics will be developed for each project effort undertaken. Each project effort will consist of a prototype technology designed to carry out a specific cyber-defense function. The metrics are driven by the priorities of the CART (see Figure 9). To obtain these, the Cyber Apex Consortium Contractor will conduct needs analysis, requirements gathering, and tech foraging, to create an Applied Research Report for each project effort undertaken. If the CART approves the findings, the Government may award a project order for representational and operational testing, respectively. The results obtained during the representational architecture testing and evaluation phase, will fine-tune the operational architecture testing metrics. Additionally, program metrics will also be guided by coverage, compliance and confidence. The coverage metric will be dictated by the percentage of CART members participating in technology transition, as well as the extent to which a candidate technology transitions. The compliance metric will seek to determine how well technologies meet federal cyber regulatory requirements. The confidence metric will be used to gauge the satisfaction level of the CART (as feedback to the DHS S&T PMO) on how well the program is meeting intended objectives

**Figure 9 – High-level Performance Measurement**

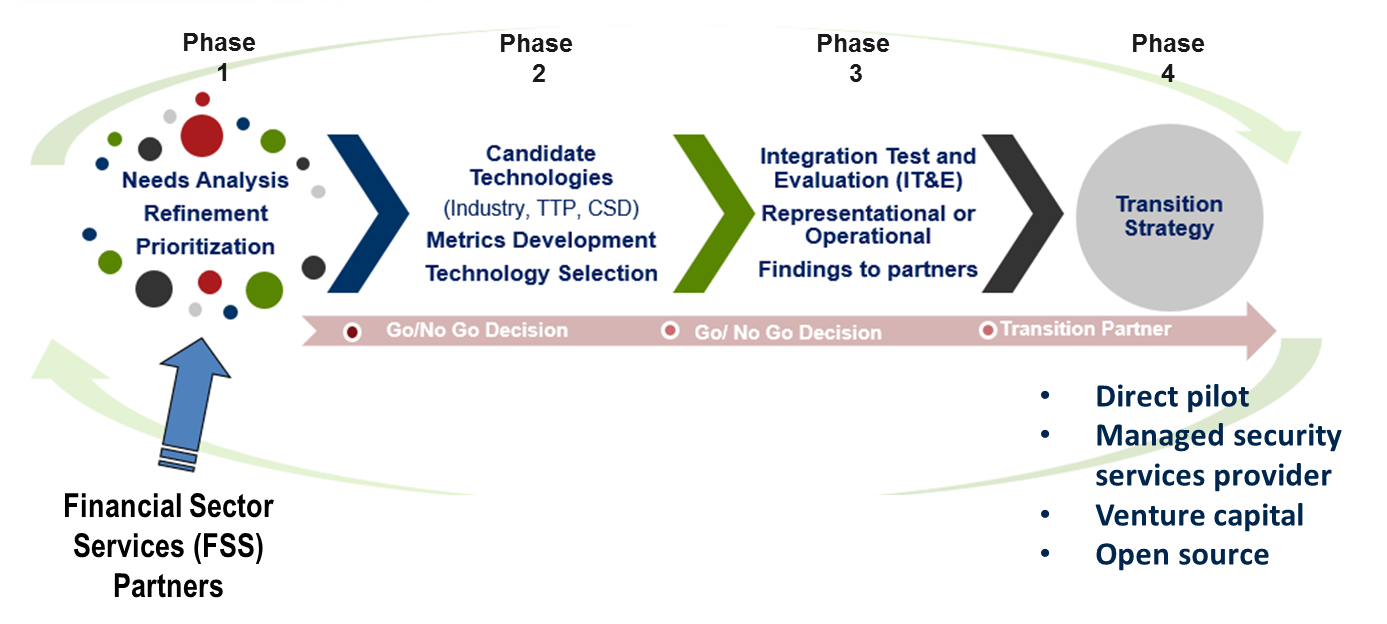
# Technology and Innovation

## Core Technology

The Cyber Apex Consortium contractor will utilize the vendor consortium to develop, test, integrate, evaluate, and transition, prototype cyber technology tools. The vendor consortium will be comprised of private sector businesses and firms. Consortium vendors will bid on individual project order solicitations to build the prototype technologies sought by the financial sector.

### Cyber Apex Consortium Approach

The NGCI Apex program will leverage existing, federally funded and private sector research efforts that provide the required technology capabilities. The process is designed with a flexible, repeatable, and continuous process to identify, test, evaluate, and transition, cyber technologies to the financial sector. The process will be implemented in four phases. Refer to Figure 9 below:



**Figure 10 - NCGI Apex Program Approach**

Phase 1: Needs analysis/requirements, and priorities: During this phase, financial industry partners identify their specific technology gaps to the CART, of which they are members. These requirements are then ranked and prioritized before proceeding to the next phase.

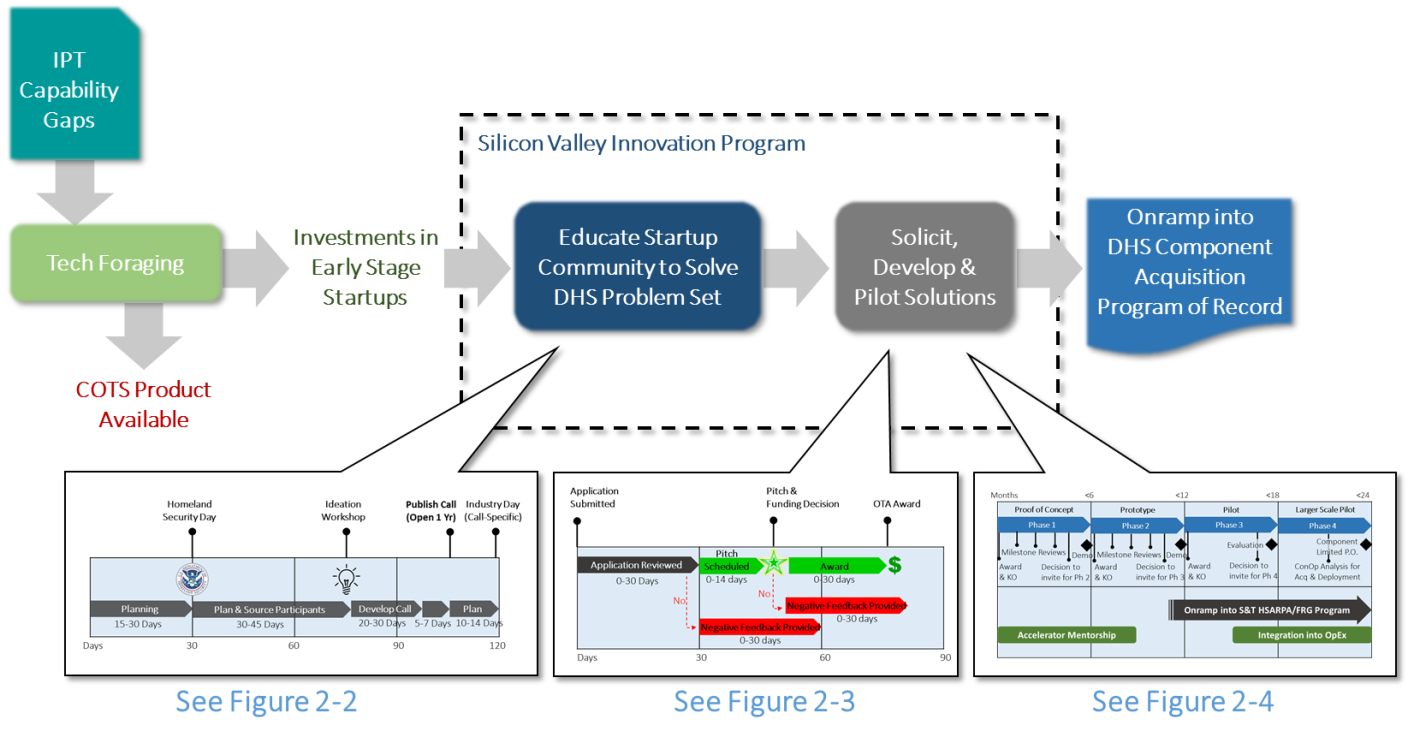
Phase 2: Technology requirements gathering, metrics development, and foraging for technologies: Based on initial requirements approved by the CART in phase 1, this phase consists of foraging for promising prototype technology candidates, and the development of metrics for the program. This phase will lead to the creation of an Applied Research Report / Recommendation Package for the CART, and constitute an individual project effort. Based on the findings, DHS S&T contracting may then award a project order for representational prototype testing. If the results of the representational prototype testing meet the requirements, DHS S&T contracting may then award a project order for operational prototype testing. This cycle will repeat itself for each project effort, and resulting project order awarded under the NGCI Apex program.

Phase 3: Testing type, integration testing, and evaluation: In this phase, the CART determines the type of testing to be conducted. NGCI Apex includes two types of prototype testing – representational and operational. Testing types depend on end-user needs and preferences. The technology will be integrated, tested and evaluated for the quality of its performance.

Phase 4: Transition prototype technologies - from testing to use in real-time operational networks: At the conclusion of the testing and evaluation phases, financial institutions (end-users) will adopt selected technologies best-suited to their operations through one of four options; managed security services providers (MSSP), entrepreneurial or venture capital firm purchases, direct acquisition of technology, or open source.

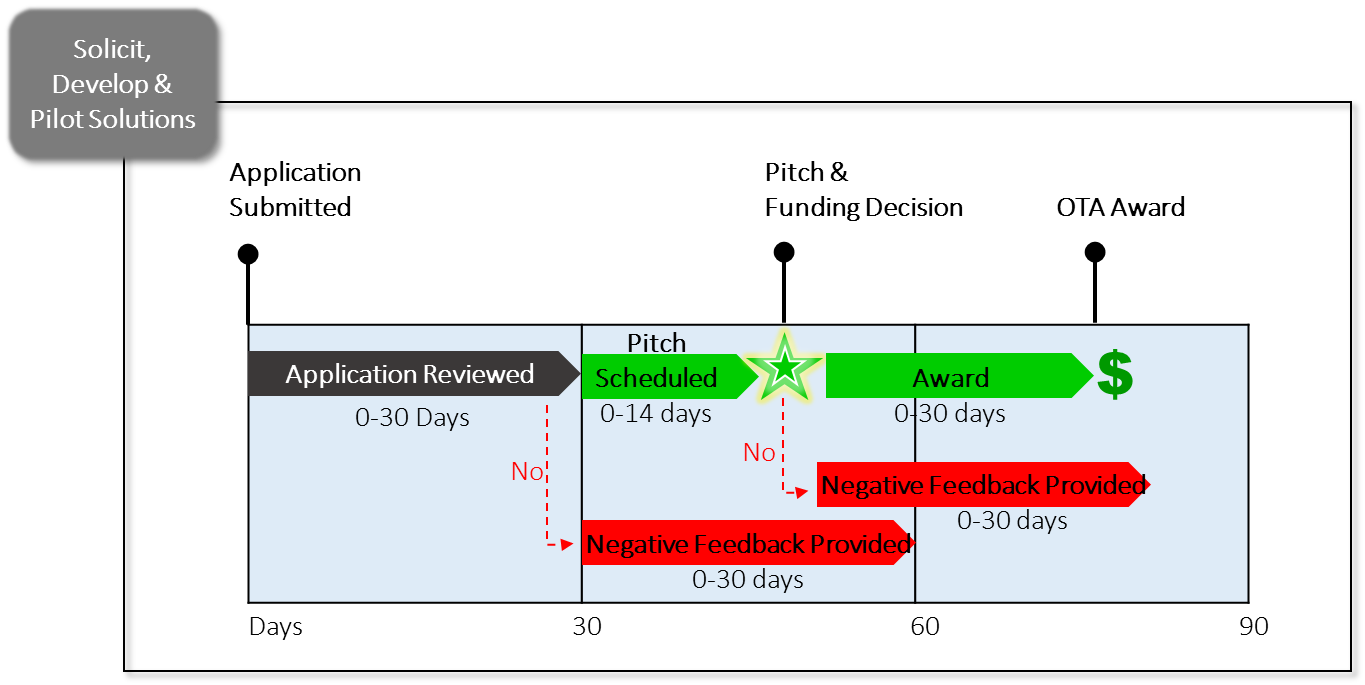
### SVIP Cyber Apex Approach

The NGCI Apex program will leverage the SVIP to capitalize on the innovation in the growing entrepreneurial and startup technology communities around the country and world. This program aligns with DHS and S&T strategic priorities, addresses cross-cutting Integrated Product Teams (IPTs), and creates transition onramp to programs. These cross-cutting needs posed by DHS and the broader HSE offer unique challenges for the startup community to address. DHS considers this community as non-traditional partners, as they do not typically seek government contracts. However, this community is adept at solving hard problems quickly and cheaply. *Figures 11, 11a through 11c* collectively depict the SVIP operating model that the DHS S&T PMO will leverage to address FSS cyber issues[[6]](#footnote-6).

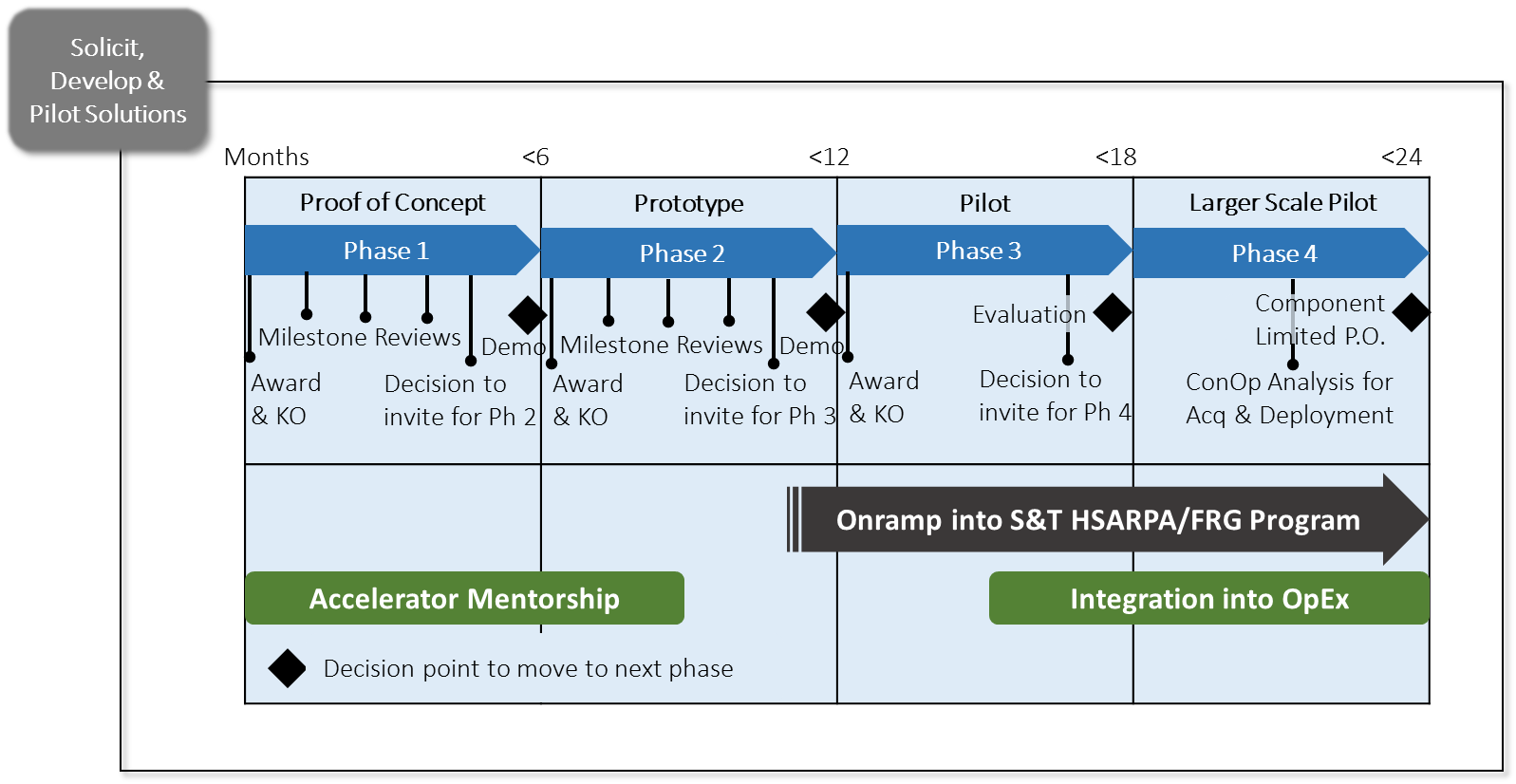
 **Figure 11 – SVIP Operating Model**



**Figure 11a – SVIP Operating Model – Educating the Startup Community**



**Figure 11b – SVIP Operating Model – Solicitation, Application, Pitch & Award**



**Figure 11c – SVIP Operating Model – Develop & Pilot Startup Solutions**

### Logistical Considerations

The DHS S&T PMO has established regular CART meetings to coordinate project details. CART meetings are held monthly, alternating between New York City and Washington, DC. This schedule will likely continue for the foreseeable future, although meeting frequency may be adjusted as needed.

# Program Management

## OTA Project Effort Execution Process

As noted in section 1.3, the NGCI Apex program will leverage an OTA. The Cyber Apex Consortium contractor will be responsible for planning and executing multiple project efforts following a repeatable process shown in Figure 11. The Cyber Apex Consortium contractor will engage in the three activities on the upper left, denoted by interlocking rings: requirements gathering, metrics analysis, and technology foraging for each technology area. See Figure 11a.

Once the activities inside the rings are completed, the Cyber Apex Consortium contractor will submit a Development & Testing Identification document to the CART for review/approval. This document lays out the feasibility of the proposed “preferred” technology, an end-user (if any), or whether no testable technology exists at all. From here, the process flow may result in one of three different paths. Refer to figure 11b.

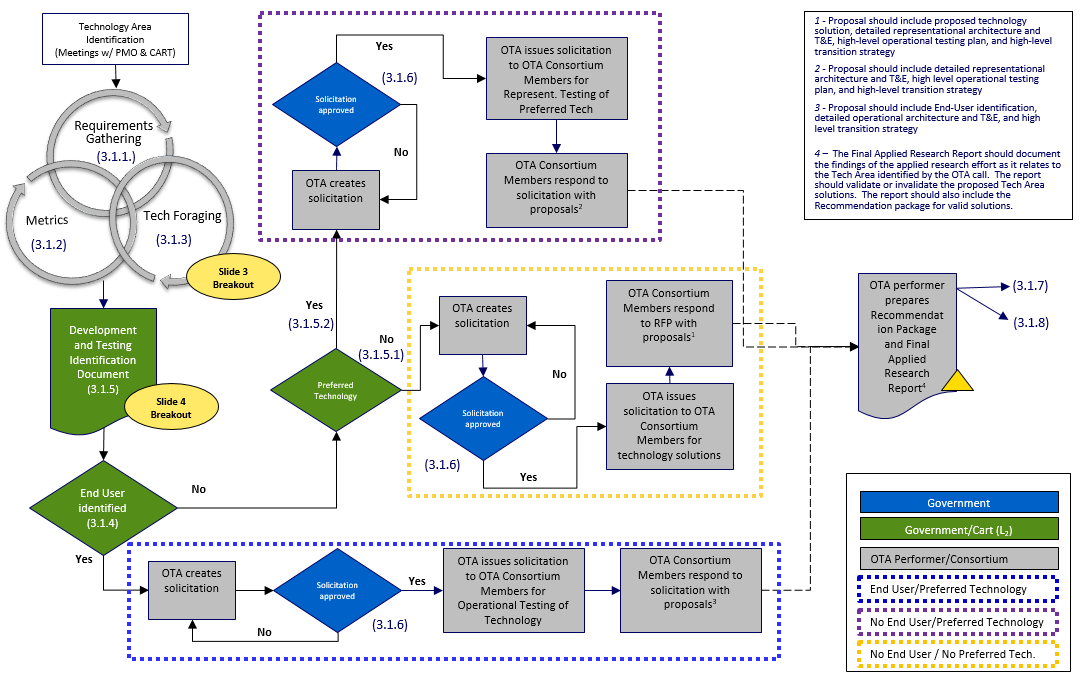
Option 1 – An end-user (FSS partner) has been identified, and has decided to proceed directly to operational testing.

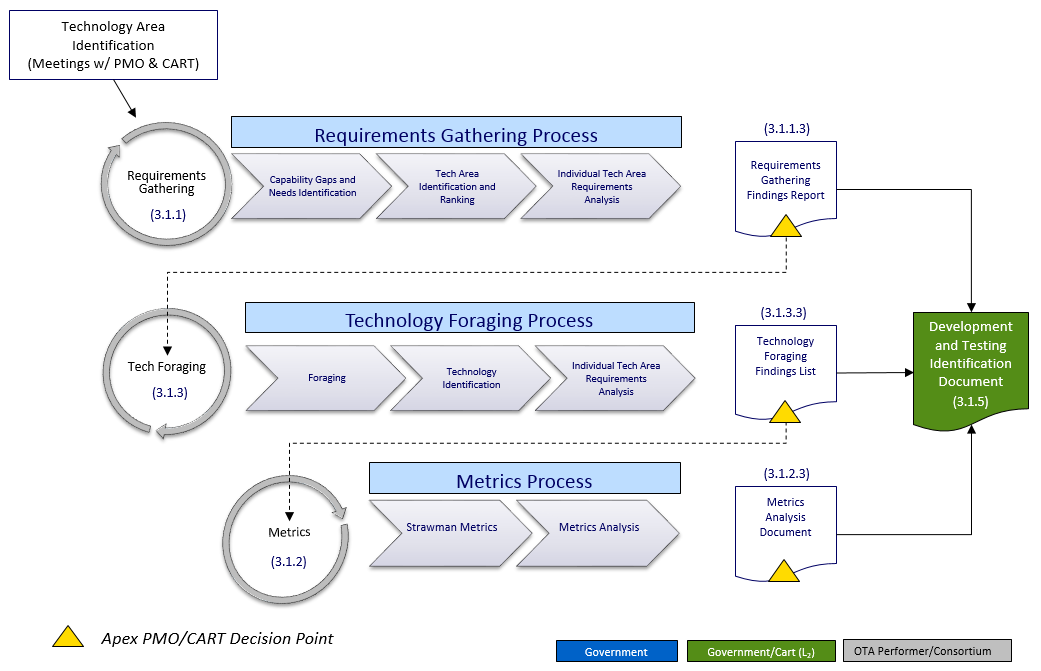
Option 2 – No end-user is identified, but there is consensus among the CART to test a specific prototype technology using representational testing.

Option 3 – No end-user is identified, and no prototype technology has been selected. A sector-relevant prototype technology will undergo representational testing.

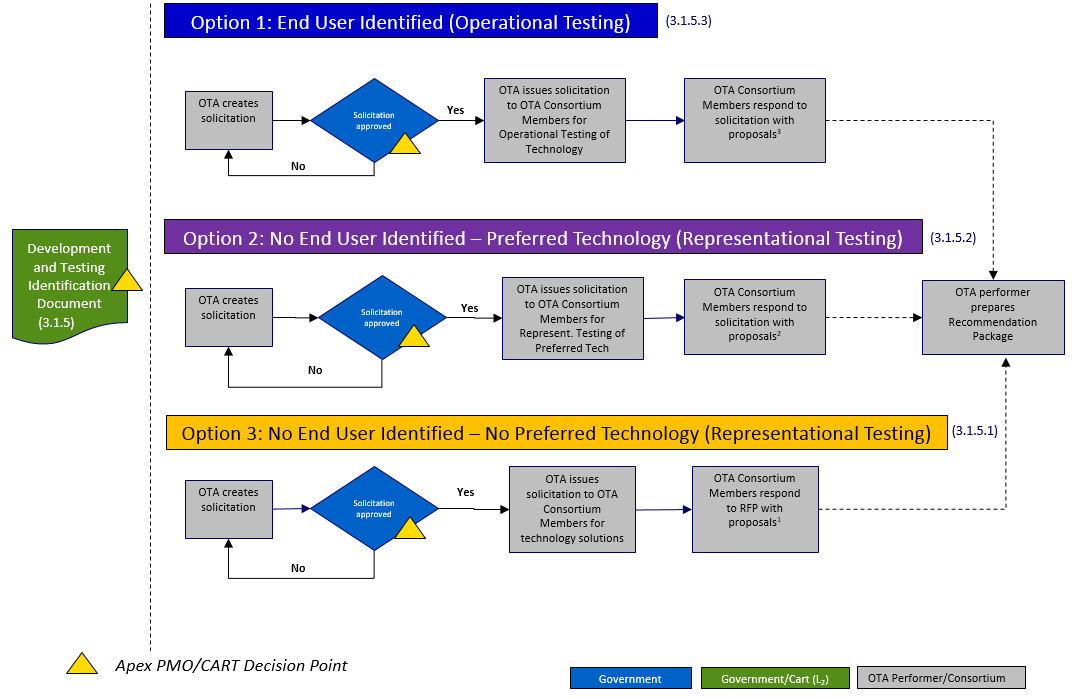
Once a path has been decided, the process will result in either a solicitation to begin a project, disapproval, or a reason why the technology prototype will not satisfy the objectives of the project effort. All of this will be outlined in an Applied Research Report / Recommendation Package. If a prototype technology proceeds to representational testing, it may be approved to continue to operational testing. There may also be an end-user interested in proceeding directly to operational testing, bypassing the representational testing altogether.

In all options exercised above, the outcome is identical: the Cyber Apex Consortium contractor will prepare an Applied Research Report containing a recommendation package with favorable proposals from the consortium, to present to the CART (Figure 11c). If the DHS S&T PMO approves, the DHS contracting officer will award a project order. If the findings contained in the Applied Research Report invalidate the results of the prototype technology, the program will move forward with the next technology area and subsequent project effort.

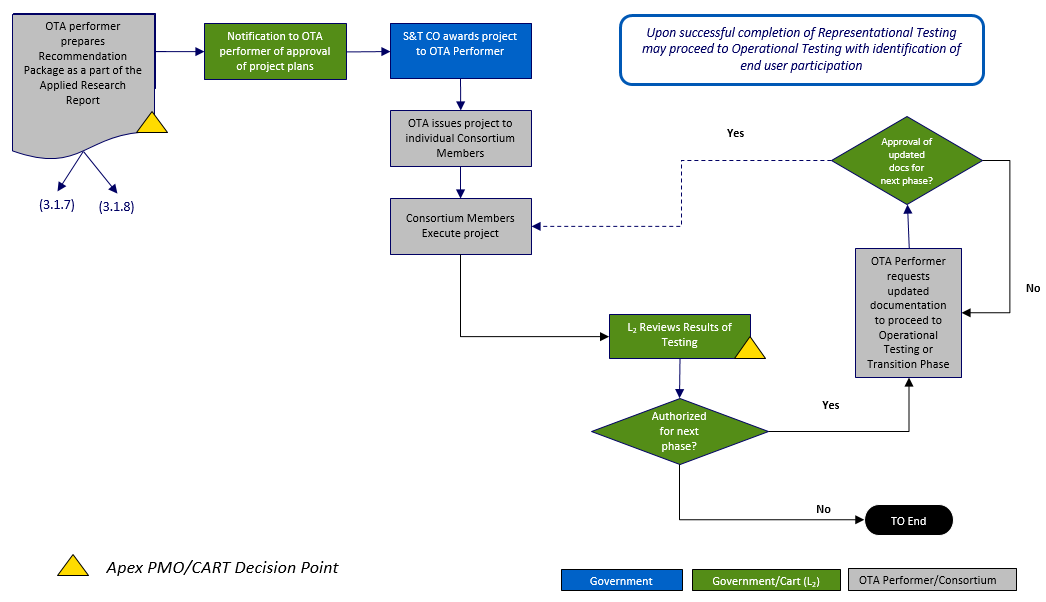
**Figure 12 - Cyber Apex Consortium Task Order Execution Flowchart (overall)**



**Figure 12a - Technology Area Identification (enlarged)**

****

**Figure 12b - Testing Type & End-User Identification**



**Figure 12c - Recommendation package / Project approval**

## SVIP Cyber Apex Project Effort Execution Process

As noted in section 1.4, the NGCI Apex program will establish one or more solicitation Call(s) under the SVIP. The SVIP is structured into four phases, with each phase being a separate fixed price, payable milestone-based OTA. Each phase is approximately three (3) to six (6) months, with down-selects after each phase. Assuming a successful award, a company is funded with up to $200,000 per phase. However, each Call will describe phase duration, associated funding levels, and expected number(s) of awards per phase. *Figure 12* below shows the four phases of the Innovation Other Transaction Solicitation (OTS)[[7]](#footnote-7) [[8]](#footnote-8).





**Figure 13 – Startup Company SVIP Funding Phases**

## Scope Management

### Scope Control Plan

For each project awarded (per technology area), DHS S&T PMO will continuously monitor all status reports and task execution (see section 4.5.1) of the applicable project effort to ensure performance remains in scope, and to make corrections as required.

## Schedule Management

All activities and progress of each project effort will be tracked and monitored per the terms and conditions laid out in the SOW for each project order (refer to section 4.5.1). This will be accomplished by using various project schedule repositories, such as Microsoft Project, and will be administered and maintained by the DHS S&T PMO to ensure timely fulfillment of contractual obligations.

### Milestones/Deliverables

On a quarterly basis, the S&T Performance Team will issue a data call for milestones through the Executive Secretariat (Exec Sec) process. The milestones, which are aligned to the program and maintained by DHS S&T, are measured against the master milestones. Each project awarded will proceed in succession (one doesn’t have to be completed for the next one to begin). The Apex PMO, and the CART both have milestones. Because the Cyber Apex Consortium OTA has not yet been awarded, the milestones and deliverables listed in Table 3 only contain estimated duration dates rather than completion dates. Projects awarded through the Cyber Apex SVIP approach are shown in Table 4. Table 5 shows milestones and deliverables from the Homeland Security Systems Engineering and Development Institute (HSSEDI).

|  |  |  |
| --- | --- | --- |
| **Product/Action Owner**  **Cyber Apex Consortium** | **Major Program Milestones/Deliverables** | **Estimated Duration** |
|  | **Pre-Project Effort actions & deliverables** | **60 – 100 Days** |
| PMO | Approve solicitation from OTA Contractor | 5 - 10 days |
| PMO + CART | Identify end-users of newly developed technologies | 5 – 10 days |
| PMO + CART | Approve OTA Project Effort plans | 5 - 10 days |
| PMO + CART | Review Recommendation package | 10 - 15 days |
| PMO | Complete PMP, RMP, PMA, and other program artifacts | 30 days |
| OTA Contractor | Task solicitation (incl. needs analysis and requirements gathering) | 10 - 15 days |
| PMO + CART | Testing determination (representational / operational) | 5 - 10 days |
| OTA Contractor | Project Effort proposal evaluation | 10 - 15 days |
| OTA Contractor | Project Order awarded | 10 - 15 days |
|  | **Representational Testing Phase** |  |
| OTA Contractor | Representational architecture testing execution | 90-180 days |
| PMO + CART | Assessment, evaluation and review | 30-60 days |
|  | **Operational Testing Phase** |  |
| OTA Contractor | Operational architecture testing execution | 90-180 days |
| PMO + CART | Assessment, evaluation and review | 30-60 days |
|  | **Transition Phase** |  |
| OTA Contractor | Transition or commercialize technology | TBD |

**Table 3 - Program Deliverables by PMO + CART**

|  |  |  |
| --- | --- | --- |
| **Product/action owner**  **Cyber Apex SVIP** | **Major Program Milestones/Deliverables** | **Estimated Duration** |
|  | **Deliverables** | |
| PMO (SVIP) | Phase 1 (Proof of concept demo) | 90-180 days |
| PMO (SVIP) | Phase 2 (Prototype demo) | 90-180 days |
| PMO (SVIP) | Phase 3 (Pilot prototype in operational environment) | 90-180 days |
| PMO (SVIP) | Phase 4 (Pilot using multiple scenarios, conditions, and scale – optional phase) | 90-180 days |
| PMO (SVIP) | Transition of prototype | TBD |

**Table 4 – Program Milestones and Deliverables (SVIP)**

|  |  |  |
| --- | --- | --- |
| **Product/action owner** | **Major Program Milestones/Deliverables** | **Completion Dates** |
|  | **Deliverables** |  |
| HSSEDI | Open-systems Architecture (OSA) Project Management Plan (PMP) | Award + 30 days |
| HSSEDI | Alpha specification (OSA) | Award + 60 days |
| HSSEDI | Beta specification (OSA) | Award + 120 days |
| HSSEDI | Summary report of findings – Alpha spec. | Award + 120 days |
| HSSEDI | Summary report of findings – Beta spec. | Award + 180 days |
| HSSEDI | Stakeholder Assessment Analysis – Draft | Award + 90 days |
| HSSEDI | Stakeholder Assessment Analysis - Beta | Award + 180 days |
| HSSEDI | Cyber Risk Metrics Survey | Award + 90 days |
| HSSEDI | Cyber Risk Metrics Assessment | Award + 120 days |
| HSSEDI | Cyber Risk Metrics Implementation Plan | Award + 150 days |
| HSSEDI | Threat Model Survey | Award + 90 days |
| HSSEDI | Threat Model Survey Assessment | Award + 120 days |
| HSSEDI | Threat Model Survey Implementation Plan | Award + 150 days |

**Table 5 - Program Deliverables by HSSEDI**

### Schedule Control Plan

Progress made by the performers of either OTA (Cyber Apex Consortium & SVIP Cyber Apex) will be assessed utilizing the monthly reports due to DHS S&T, as well as through weekly DHS S&T PMO / performers meetings established to coordinate task status and overall progress. This will allow the DHS S&T PMO to easily address task status concerns and discuss corrective actions.

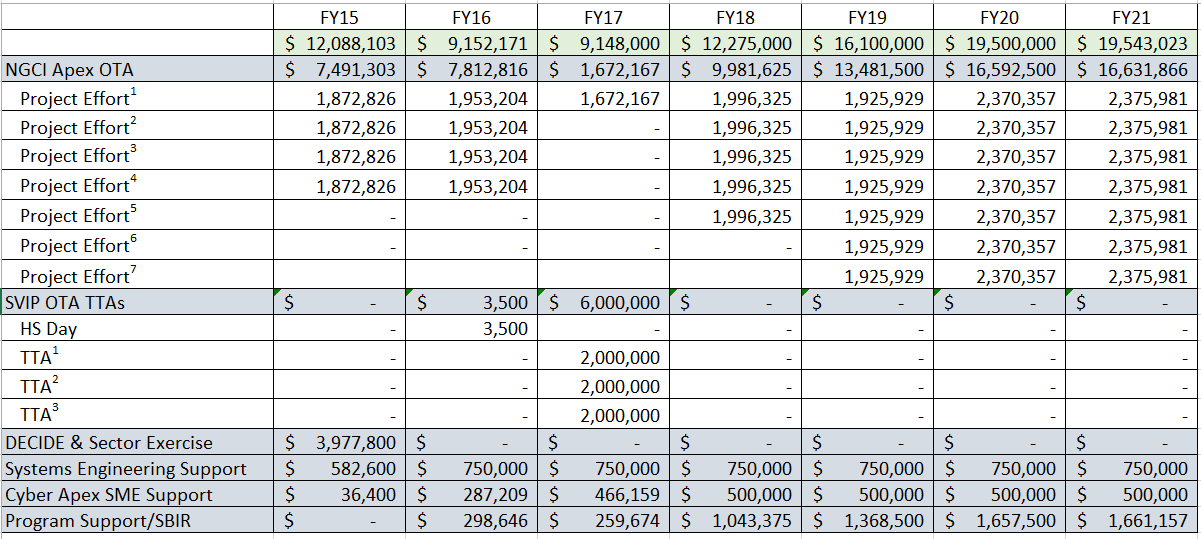
## Cost Management

### Cost Estimate

The NGCI Apex program has estimated funding for a period of 5 years, totaling ~$55M.

### Cost Baseline

Table 5 shows the budget breakdown by task order over the five-year program lifecycle.



TTA1 = Intrusion Deception TTA2 = Moving Target Defense TTA3 = Isolation & Containment

**Table 6 - Task Order Breakdown by Fiscal Year**

### Cost Control Plan

DHS S&T will receive monthly expenditure reports detailing program spending trends and cost breakdowns. These documents will be reviewed by the DHS S&T PMO to ensure compliance and oversight.

## Status Reporting

### Deliverable tracking

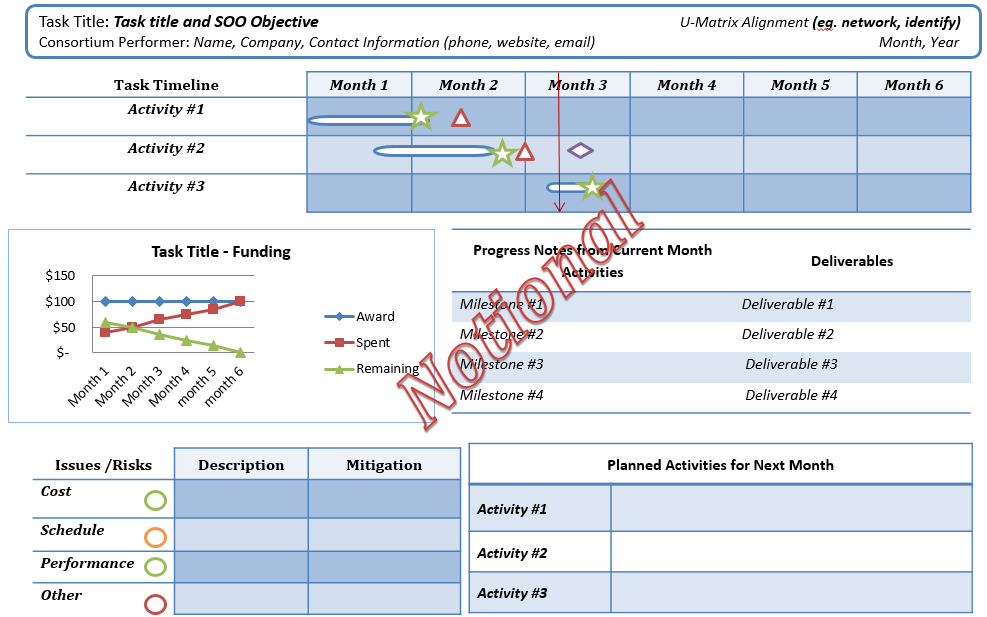
On a recurring basis (monthly), the Cyber Apex Consortium contractor and any SVIP acquired startup vendors, will furnish the following to the DHS S&T PMO to monitor the Cyber Apex Consortium contractor’s performance:

* Financial status report
* Program plan outlining activities completed during the current reporting period and those planned for the upcoming reporting period
* Project Status Reports
* Schedule of activities
* High-level program overview (quad chart format)
* Monthly summary report

### Configuration Management

The DHS S&T PMO will control all NGCI Apex program-level deliverables, such as the items listed in 4.6.1. All CART meeting summaries, program management plan (PMP), risk registers, SOWs, and other acquisition documents will be maintained on the DHS S&T SharePoint site. The DHS S&T PMO will regularly access and maintain the site with updated program artifacts.

Items, such as, fund expenditures, program schedule compliance, performance metrics and risk factors are examples of products that will provide an overview on deliverables. The DHS S&T PMO will interact with the Cyber Apex Consortium contractor on a weekly basis for coordination, clarification, or follow-up on any specific items. A project dashboard will be used to provide an overall summary of program status with regards to cost, schedule and performance. Figure 13 shows an example of a dashboard.

**

**Figure 14 - Sample Dashboard**

## Human Systems Integration (HSI)

Many of the acquisition systems in use are too complex and require multiple disciplines in order to properly define, design, integrate, test, evaluate, or deploy successful systems. HSI requires involvement and interaction from program managers, systems engineers, operators, analysts, trainers, developers, and so forth. The combined knowledge efforts of these distinct professions / competencies must be coordinated and syncretized to achieve maximum effectiveness for best results. In the case of Cyber Apex, there will be varying levels of HSI involved in each phase of the project efforts (project effort dependent). For example, HSI can be expected to play a role in the design of the testing architectures for the program, inputs made to optimize testing parameters, design of threat models for testing phases, threat simulations (exercise inputs/scenarios), integration into operational environment of financial institutions, etc. HSI will be considered for all of the phases within the program.

## Security and Classification

Although there may be specific information relating to financial sector critical infrastructure which is classified, the NGCI Apex program is, in and of itself, unclassified.

# Risk Management

## Risk Management Plan

The Risk Management Plan (RMP) describes how generic and program-specific risks are identified, analyzed and prioritized. The RMP is a separate document which outlines procedures for tracking risks, evaluating changes in the level of individual risks (e.g. when a risk goes from High to Medium), and responses to those changes.

The risk management plan will describe how to address the following questions for each risk:

1. What might happen?
2. How likely is it that it will happen (and when, if this can be addressed)?
3. If it does happen, what are the consequences (and when, if this can be addressed)?
4. What could be done about the given risk (and when, if this can be addressed)?
5. What should be done about the given risk (and when, if this can be addressed)?
6. What is going to be done about the given risk (and when, if this can be addressed)?
7. How well is the chosen course of action (of mitigating the risk) working?
8. Has anything changed that requires altering existing risk management measures (and when, if this can be addressed)?
9. Are there current trends and/or potential future development that could require altering existing risk management measures (and when, if this can be addressed)?
10. What information about the given risk needs to be communicated (and when, if this can be addressed)?
11. Who needs to know about the given risk (and when, if this can be addressed)?
12. How can necessary risk information be most effectively communicated (and when, if this can be addressed)?

## Risk Identification and Assessment

Risks to the NGCI Apex program can be divided into the high-level categories outlined below.

### Technical Risks

The NGCI Apex program employs the use of advanced cyber technologies to deter detrimental and disruptive cyberattacks. This leads to risks involved with software development, engineering, integration, and testing; these risks can involve both the Cyber Apex Consortium contractor and consortium vendors. Examples of technical risks include; programming errors, glitches, lack of technical knowledge, incorrect threat modeling, scalability issues, unclear / undefined data collection requirements, and other concerns.

### Programmatic Risks

#### Cost Risks

Funding for NGCI Apex program will be managed by DHS S&T. However, the Cyber Apex Consortium contractor will be approved to manage the money assigned to each project. DHS S&T will receive a monthly expenditure report detailing spending trends and cost breakdowns. These risks will be monitored as a part of the DHS S&T PMO’s risk management plan.

#### Scope and Performance Risks

Examples of risks associated with scope or technical performance include:

* Software defects
* Scope gap (scope is not well defined and subject to disputes that could impact cost and schedule)
* Scope creep
* Dependency changes, such as unexpected legal, regulatory, compliance action
* Integration issues due to changes in expected behavior

#### Schedule Risks

Examples of risks associated with schedule include:

* Project dependencies (a risk associated with one task may generate a risk for another)
* Errors in estimating length of a given task
* Delays in decisions to award projects (these could happen due to multiple factors)
* Issues associated with product integration
* Issues associated with product testing at any level
* Issues involved in technology transition

### Operational Risks

When the Cyber Apex Consortium contractor begins representational (open-source) architecture testing and operational architecture testing, using institution-specific parameters, (see Figure 10), different risk factors will apply. Poorly managed software integration for testing purposes has the potential to generate setbacks. Improper testing and evaluation methods could result in a cyber technology product not fully ready for deployment. The same is true of inaccurate threat modeling. Not having deployable-ready technologies available to the customer can lead to schedule delays. Sub-standard software performance may have the same effect. Since the NGCI Apex program will be broken up into distinct project efforts, some risks may be project dependent.

## Risk Register

The NGCI Apex Risk Register contains the following information and is an excel document located on the S&T CSD Shared drive: \\dhsnet.ds1.dhs\S&T\_shares\Cyber Security\NGCI Apex

* Issue Date – Date when the risk was first recorded
* Date Last Reviewed – Date when the risk was last reviewed by the program risk management board
* Risk Title – A short name for the risk
* Risk ID
* Risk Category – Cost, Schedule, Performance, Supportability, Representational, Operational[[9]](#footnote-9)
* Risk Status – Open or Closed
* Risk Description – Complete details on what the risk entails and the consequences if not mitigated
* Risk Mitigation Category – Avoid, Transfer, Mitigate, Accept
* Risk Mitigation Details – Complete details on how the risk will be mitigated, including how the mitigation effort will be monitored
* Risk Owner – DHS S&T PMO, Cyber Apex Consortium Contractor, Vendor
* Probability (of occurrence) – Very Low, Low, Medium, High, Very High (scale of 1-5)
* Impact (of occurrence) - Very Low, Low, Medium, High, Very High (scale of 1-5)
* Risk Score – Product of Probability and Impact. Risk color assignments are: Green (1-4), Yellow (5-10), Red (11 and higher)

1. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* [↑](#footnote-ref-1)
2. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* [↑](#footnote-ref-2)
3. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014 [↑](#footnote-ref-3)
4. “Silicon Valley Innovation Program: FY2016-FY2020 Strategic Plan”. June 2016. [↑](#footnote-ref-4)
5. Memorandum of Understanding between DHS, and FSSCC, June 2016. [↑](#footnote-ref-5)
6. “Silicon Valley Innovation Program: FY2016-FY2020 Strategic Plan”. June 2016. [↑](#footnote-ref-6)
7. Silicon Valley Innovation Program (SVIP) 5-Year Innovation Other Transaction Solicitation (OTS), HSHQDC-16-R-B0005, <https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC16RB0005/listing.html> [↑](#footnote-ref-7)
8. “Silicon Valley Innovation Program: FY2016-FY2020 Strategic Plan”. June 2016. [↑](#footnote-ref-8)
9. A given risk may span one or more risk categories. [↑](#footnote-ref-9)