**

*DEPARTMENT OF HOMELAND SECURITY*

*SCIENCE AND TECHNOLOGY DIRECTORATE*

Project Management Plan (PMP)

Cyber.gov

Version 2.2

09/21/17

**PMP Approvals:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_**

**Project Manager Date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ Division Director Date**

Record of Changes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Figure # or Section #** | **A/M/D\*** | **Description of Change / Rationale** |
| 0.5 | 07/27/16 |  |  | Initial draft |
| 1.0 | 08/05/16 |  | M | Updated draft based on Front Office review and comments |
| 2.0 | 01/13/17 |  | A/M | Updated document based on new scope of work |
| 2.2 | 09/21/17 | 1.4 | A/M | Introduced new architecture and adoption strategies |

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

Contents

[1. Project Summary 1](#_Toc474764692)

[1.1 Background and Purpose 1](#_Toc474764693)

[1.2 Customer(s) 3](#_Toc474764694)

[1.3 Deliverables/Products 5](#_Toc474764695)

[1.3.1 Product or Service Descriptions 5](#_Toc474764696)

[1.3.2 Capability or Performance 6](#_Toc474764697)

[1.4 Transition Plan 14](#_Toc474764698)

[1.5 Schedule and Budget Summary 20](#_Toc474764699)

[1.6 Project Organization 21](#_Toc474764700)

[1.6.1 Project Personnel 21](#_Toc474764701)

[1.6.2 Internal Structure 22](#_Toc474764702)

[1.7 Benefits to S&T 22](#_Toc474764703)

[1.7.1 New Capabilities / Technology 22](#_Toc474764704)

[1.7.2 New Intellectual Property 23](#_Toc474764705)

[1.7.3 Public Access of Federally Funded Scientific Research 23](#_Toc474764706)

[1.7.4 Data Management 23](#_Toc474764707)

[1.7.5 Other Benefits 23](#_Toc474764708)

[1.8.0 Assumptions 23](#_Toc474764710)

[2. Requirements 24](#_Toc474764711)

[2.1 Requirements Management Plan 24](#_Toc474764712)

[2.1.1 Test and Evaluation 25](#_Toc474764713)

[2.2 Customer Engagement 26](#_Toc474764714)

[2.3 Customer Requirements 27](#_Toc474764715)

[2.4 Key Functions and Desired Performance Requirements 30](#_Toc474764716)

[2.5 Other Metrics 31](#_Toc474764717)

[3. Technology and Innovation 31](#_Toc474764718)

[3.1 Core Technology 31](#_Toc474764719)

[3.2 Technology Scouting 32](#_Toc474764720)

[3.3 Technical Approach 32](#_Toc474764721)

[3.3.1 Trade Space Analysis 32](#_Toc474764722)

[3.3.2 Preferred Alternative 34](#_Toc474764723)

[3.3.3 Logistics Considerations 35](#_Toc474764724)

[4. Project Management 35](#_Toc474764725)

[4.1 Acquisition Management 35](#_Toc474764726)

[4.1.1 Program Acquisitions 35](#_Toc474764727)

[4.1.2 Acquisition Strategy 36](#_Toc474764728)

[4.1.3 Potential Sources 36](#_Toc474764729)

[4.2 Scope Management 37](#_Toc474764730)

[4.2.1 Work Breakdown Structure 37](#_Toc474764731)

[4.2.2 Scope Control Plan 38](#_Toc474764732)

[4.2.3 Schedule Management 38](#_Toc474764733)

[4.2.4 Milestones/Deliverables 38](#_Toc474764734)

[4.2.5 Schedule Control Plan 39](#_Toc474764735)

[4.3 Cost Management 40](#_Toc474764736)

[4.3.1 Cost Estimate 40](#_Toc474764737)

[4.3.2 Cost Baseline 40](#_Toc474764738)

[4.3.3 Cost Control Plan 40](#_Toc474764739)

[4.3.4 Status Reporting 40](#_Toc474764740)

[4.4 Cost/Schedule/Performance Trade-Offs 40](#_Toc474764741)

[5. Risk Management 40](#_Toc474764742)

[5.1 Risk Management Plan 40](#_Toc474764743)

[5.2 41](#_Toc474764744)

[5.2.1 Technical Risks 41](#_Toc474764745)

[5.2.2 Programmatic Risks 42](#_Toc474764746)

5.2.2.1 Cost Risks

5.2.2.2 Scope/Performance Risks

5.2.2.3 Schedule Risks

[5.2.3 Risk Management Approach 42](#_Toc474764747)

5.2.3.1 Risk Management Program Objectives

5.2.3.2 Critical Success Factors

5.2.4 Risk Management Process and Procedures

5.2.4.1 Overview

5.2.5 Risk Register ……………………………………………………..……………………………………………………………………………45

# Project Summary

## Background and Purpose

The National Cyber Protection System (NCPS) was developed to protect the information systems of the civilian U.S. Government from intrusion and attack, especially from foreign cyber threats. DHS is tasked with improving cyber security for more than 100 civilian government departments and agencies ranging in size from 10’s to 100’s of employees (such as the Selective Service System) to more than 250,000 employees (such as the Department of Veterans Affairs).

DHS roles described in the Comprehensive National Cybersecurity Initiative (CNCI) released in January 2011 include deploying an intrusion detection system called EINSTEIN 2 to monitor traffic to and from Departments and Agencies (D/As), deploying an intrusion prevention system called EINSTEIN 3 (now called E3A) to block attacks to D/As, and coordinating and integrating cyber information to provide situational awareness across D/As. In addition a DHS program called Continuous Diagnostics and Mitigation (CDM) provides tools and services that strengthen the security posture of D/As through continuous monitoring and corrective actions.

The Cyber.gov project seeks to address some of the current shortfalls identified with these programs, many of which were identified in two separate studies commissioned by the Department. One study was conducted by the Massachusetts Institute of Technology-Lincoln Laboratory and the other study was a Blue Ribbon Panel (BRP) report delivered to DHS S&T in December 2015. The Cyber.Gov team will also investigate the current use of classified signatures from E3A and quantify their impact.

In addition to addressing some of the issues identified in the reports above, the Cyber.gov project is working with OMB and the Office of the Federal Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to develop a security architecture and associated technical components to that architecture for deployment across the entire Government domain. At present, there is no security architecture or enforceable policy governing all federal agencies. As a result, many agencies are provisioning their own commodity IT services, even though this is not a core mission function, and many agencies lack the ability to provide sufficient resources to keep up with technology advances and security threats. The situation has resulted in IT services duplication and waste within and between agencies, as documented in GAO Reports and OMB analyses of agency investment data. The situation has also resulted in a growing number of agency cyber-incidents wherein there has been a loss of significant amounts of sensitive mission, financial, and personnel data.

As a result, Cyber.gov is creating a robust, innovative and holistic cyber security architecture design that mitigates modern threats (Asset Management, Configuration Management, Phishing, DDoS, Ransomware, Mobile, Cloud issues and more) by leveraging best practices and implementable solutions with minimal impact to workforce efficiency. It will not only addresses some of the issues of perimeter based defense, but also brings new technologies such as Software Defined Perimeter (SDP) tailored to the .Gov domain, while guiding CIOs and CISOs in selecting and implementing current best practices for 34 cyber security components.

Cyber.gov will significantly improve the security and resiliency across the D/As.

To ensure proper feedback, adoption, and transition, , significant efforts are made to engage with D/As to assess their current cyber defense architecture, current software and hardware inventory, threats and gaps;

In addition, the Cyber.Gov team will facilitate the deployment of technology to improve security and resiliency by identifying implementable innovative solutions, by prototyping capabilities and assessing technology maturity to meet the new cyber security baseline requirements.

For each component of the cyber architecture designed, baseline requirements will be created, leverage the NIST publications, the NIST Cybersecurity Framework, the NIST 800-53 controls and common best practices, to ensure proper implementation and guide CIOs/CISOs in their decision making process to select proper solutions and smart sourcing.

Thanks to these significant deliverables, the Cyber.Gov program will achieve significant impact.

Using bottom-up and top-down analysis, feedback from systems analysis of D/A needs, modeling, simulation, metrics, and technology prototyping, the program will provide D/A leadership, Federal CIO/CISO and the Office of Management and Budget (OMB) with the information needed to incrementally adopt the Cyber.gov architecture. This will allow them to steadily and substantially improve the cyber security of their infrastructure and deter the growing threats.

To achieve these goals, Pacific Northwest National Laboratory (PNNL) and MIT Lincoln Laboratory will work collaboratively, and partner with external collaborators when appropriate (for instance for independent red-teaming of proposed solutions).

This project is aligned to other national, departmental and S&T Directorate Goals outlined below:

**National Level Alignment**:

The Cybersecurity National Action Plan (CNAP), released by the White House in February 2016, outlined a series of near term actions to enhance cybersecurity capabilities within the Federal Government and across the country. One element that the Cyber.gov program will address is to Strengthen Federal Cybersecurity by properly implementing 34 cyber security components. Cyber.gov will significantly improve the cyber security posture of the D/As while adding new potential layers to solve additional threats related to Cloud, Legacy and Mobile systems.

Furthermore, the new administration is currently preparing to draft a new Executive Order to address the current cyber security issues across the D/As. The new architecture will address many of those issues and will align with National Protection and Protection Division (NPPD) and Office of Management and Budget (OMB) oversight.

**Department Alignment**:   
The 2014 Quadrennial Homeland Security Review (QHSR), calls for Safeguarding and Securing Cyberspace as one of its primary missions. There are several corresponding goals under Mission 4. In particular, Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise will be addressed by the Cyber.gov research.

**S&T Directorate Alignment:**

One element of the S&T Strategic Plan is to deliver force multiplying solutions by “making strategic investments in high-impact, priority areas”. Since NCPS is used by CS&C across all Federal Agencies in the .Gov domain, this investment has the potential to make a tremendous impact in the overall federal civilian network cybersecurity posture. The new cyber security architecture designed by the Cyber.gov team will be deployable not only by the Federal D/As but also by State, Local and even private sector companies as governed by NPPD and OMB.

This project will establish research leadership position for S&T by:

1. Demonstrating the value of up front systems and architectural analysis for cybersecurity defense of a distributed network
2. Demonstrating S&T research capabilities outside of the Department – through working with other D/As that use NCPS
3. Demonstrating the positive impact S&T can have on a major acquisition program by demonstrating the art of the possible in the near term (1-2) years versus the longer term that some view the R&D timeline as.

## Customer(s)

The primary customers for Cyber.gov are OMB, every D/As, the state and local CIOs/CISOs, the public sector and CS&C. This is described in more detail in Section 2.2.

Within OMB, the senior level primary points of contact are:

* Margaret Graves, Acting Chief Information Officer,
* Grant Schneider, Federal Deputy Chief Information Security Officer, EOP/OMB
* Scott Bernard, Federal Chief Enterprise Architect, EOP/OMB

Within CS&C, the senior level primary points of contact are:

* Danny Toler, Deputy Assistant Secretary, CS&C
* Laura Delaney, Deputy Director of CS&C, Network Security Deployment (NSD) Division

Some of the current senior level stakeholders participating include:

* Jeffrey Eisensmith, DHS Chief Information Security Officer
* Small Business Administration CIO/CISO (SBA)
* United States Citizenship and Immigration Services CISO / Deputy CISO (USCIS)
* Central Intelligence Agency (CIA)
* Department of Veterans Affairs (VA)
* Occupational Safety and Health Review Commission CIO (OSHRC)
* Washington, DC, Chief Information Security Officer
* National Institute of Standards and Technology (NIST)

The CS&C staff has demonstrated commitment on the project. CS&C suggested further coordination on these efforts to minimize duplication of efforts. Jointly, CS&C has also funded an effort to examine the utility of the classified signatures.

## Deliverables/Products

### Product or Service Descriptions

The initial set of Year 1 Cyber.gov tasks, products and services to be delivered are described below:

| **Task/Subtask Number and Name** | **Milestones/Deliverables** | **Due Date or Completion Date** |
| --- | --- | --- |
| Task A: Classified Indicator Study of E3A. | Assess and measure E3A impact of classified indicators. | Task A:  October 2017 |
| Task B: Measurement Infrastructure of E3A | 1) Basic applicability of indicator information  2) Quality of signature that results  3) Whether O/S impedes or contributes  4) Disambiguation of notifications | Task B:  October 2017 |
| Task C1: D/A Engagement and System Analysis | Inventory of cyber solutions (H/W and S/W) used by 10 to 15 D/As in order to prioritize integration of future pilots.  An out-brief to each D/A containing analysis addressed to improve cyber security posture of system.  A combined presentation that provides system analysis results. | Task C1:  First analysis report by May 2017 up to October 2017. |
| Task C2: Cyber.gov Architecture  C2a: Software Defined Perimeter Assessment and Baselining  C2b: Development / Prototyping  C2c: Architecture Baseline and Recommendations | Design an innovative and holistic cyber security architecture and requirements, prototype and pilot.  C2a: Testing, demonstration of SDP technology with select vendors in test environments.  Evaluate SDP suitability, define requirements for implementation and assess benefits  C2b: Prototyping of technologies such as a Trust Central System to consolidate device state/patching information  C2c: Initial draft Cyber.gov D/A Architecture  C2c: Initial High Level Architecture  C2c: First final version of the Architecture baseline | C2a: April 17  C2b: Ongoing as needed  C2c: First draft of the architecture by April 17. Next version 1 by October 17 |
| Task C3: Cyber.gov Testbeds and Implementations | C3: Initial instantiation of D/A architecture in testbed  C3: Initial instantiation of SDP  C3: Initial instantiation of D/A relevant threat  C3: Execution of technology assessments in testbed environment | C3: June 17 |
| Task C4: D/A Engagement, Planning, and Pilot Preparation | C4: D/A engagement plan  C4: Initial D/A profiles and environment requirements complete  C4: First D/A Meeting  C4: Summary report of D/A feedback, insights, and/or requirements complete | C4: April 17  C4: May 17  C4: May 17  C4: Sep 17 |

### Capability or Performance

#### Task A: Classified Indicator Study

Objective is to assess whether E3A implementation of classified indicators provides a proper impact compared to its cost. A report providing recommendations of quantitative measures as currently deployed in NCPS. A finding in both the Blue Ribbon Panel and MIT Lincoln Lab evaluation report revealed lack of instrumentation within the underlying system.

In the near term, this task will generate the instrumentation and perform the data collection to support the systems analysis and classified indicator studies.

Four aspects are relevant for analysis including volume, timeliness, uniqueness, and impact. DHS has identified these aspects as critical to the analysis of USG indicators in use by the Einstein 3 Accelerated (E3A) in the National Cyber Protection System (NCPS). While several studies have been performed on volume, timeliness, and uniqueness, impact has yet to be well defined, understood, and documented.

The primary objectives of this test are to:

1. Define impact, the data requirements to measure impact, and measure impact.

2. Reproduce volume, timeliness, and uniqueness for the specific data sample under study.

3. Produce a report of these four aspects of the value of USG indicators as they are used by E3A.

#### Task B: Measurement Infrastructure

A finding in both the Blue Ribbon Panel report and the Lincoln Laboratory evaluation report on NCPS was the lack of instrumentation within the underlying system. In the near term, this task will generate the instrumentation and perform the data collection to support the systems analysis and classified indicator studies. The instrumentation needs to support at least four contributing factors to the overall security of the D/As. These factors are: 1) basic applicability of the indicator information upon which NCPS signatures are based, 2) the quality of the signature that results from the indicator information, 3) whether the manner of operating the system impedes or contributes to resolution of any underlying threat, and 4) disambiguation of notifications.

To support measurements required in the indicator study, we will construct data collection infrastructure to be used as needed. We propose that initial data collection using this infrastructure will take place in two stages. The first stage is a quick-look data collection of one month that will be used to validate the instrumentation and the proposed analytical techniques to be used in the indicator study. The second phase will be a longer-term data collection activity of 6 months to one year in duration in order to support assessment of longer term trends in indicator effectiveness.

#### Task C1: D/A Engagement and System Analysis:

Direct engagement with a collection of D/As will inform the design of a modular, flexible architecture leveraging existing government and commercial off the shelf solutions.

The objective is to create an overview of various sized (from micro to large) Departments and Agencies (D/As)’ asset inventory and gap analysis. We are conducting an extensive inventory of the different software solutions used for each of the Exhibit A components, a current hardware inventory, gap assessments and potential threats. These assessments and data gathering effort will provide an initial Asset inventory that will serve to better understand our current posture and protect our systems accordingly. In fact, it represents the first step of the NIST Cybersecurity framework, well recognized and established for many years (“Identify”).

Based on information gathered during the engagement, a System Analysis will provide a data driven, evidence-based approach to support the development of the architectural requirements and the reasoning behind the architecture. Such an analysis informs the architecture team to avoid the development of an architecture founded on assumptions which are driven solely by best practices. The user-focused process will ensure that the actual needs of the D/As are being addressed by any proposed solutions.

Output of this analysis will be an interim and final report, detailing the operational postures of the D/As examined; threats in the cyber domain to the specific D/As examined and the broader community; the capability gaps and needs to address those threats; and existing tools at the D/As and a path forward for the Cyber.gov effort in partnership with OMB, CIO, CISOs, and others.

#### Cyber.gov Software Defined Perimeter Assessment and Baselining

Software Defined Perimeter (SDP) was created by the Cloud Security Alliance (CSA) in December 2013. Multiple private commercial companies provide it as a service, on premise or hosted. Several corporations and government entities are utilizing SDP, including Coca Cola, Verizon, Google (for the entire company with their BeyondCorp project), the Department of Defense, the Canadian Government and more.

As an additional layer to the existing Border and Perimeter Network controls, SDP provides several additional unique advantages while solving multiple current issues. First, it not only protects systems on the perimeter network, including legacy but also on the Cloud and Mobile.

SDP provides several additional unique advantages while solving multiple major issues:

* + Grants access to specific systems based on granular role based rules, enforcing “Need to Know” / “Least Privilege”.
  + Verifies the device’s state including Antivirus/Malware, OS Fingerprinting, and Vulnerability scan before granting access.
  + Protects various systems including Legacy and Cloud and Mobile systems.
  + Enforces strong authentication including two factor authentication.
  + Enforces patching by checking patch levels before granting access.
  + Protects against DDoS and vulnerability scans by leveraging the “Dark Cloud” concept.

“Dark Cloud” means that only specific systems that need to be accessed by that user, with that specific device are visible, enforcing “Need to know”. The other systems cannot be seen scanned or mapped.

Cyber.gov is currently creating a baseline requirement for proper implementation of SDP in the .Gov domain. We are implementing SDP pilots while collaborating with several corporations such as Verizon and Google.  We are also engaged in discussions with, leading vendors such as Cryptzone, Vidder and Waverley Labs.

#### Task C2: Cyber.gov Architecture:

The goals of the architecture task are to design a robust, innovative and holistic cyber security architecture that mitigates modern threats (Asset Management, Configuration Management, Phishing, DDoS, Ransomware, Mobile, Cloud issues and more) by leveraging best practices and implementable solutions with minimal impact to workforce efficiency. The new Cyber.Gov architecture will also address weaknesses in existing architectures including attack surface coverage, timeliness, measurements and metrics to understand its effectiveness. To achieve impact quickly, this task will incorporate both top-down analysis and bottom-up technology development and deployment simultaneously.

* The top-down approach of the architecture task will be to create an initial high-level architecture that encompasses the full 3+ year vision for the creation of a securable and defensible architecture for federal D/As (Task C2c). In parallel, the architecture task will have a team conducting assessment and testing of Software Defined Perimeter (SDP) and create its requirement baseline to be used in the .Gov domain (Task C2a).
* Leveraging Agile methodologies, Cyber.gov Testbeds and Implementations will be executed in order to prove efficiency of the proposed architecture, Cyber.gov, the team will conduct testing and setup a testbeds to assess current and potential new technologies.
* In addition, Cyber.gov is leveraging the National Institute of Standards and Technology (NIST) Cybersecurity framework and NIST component controls to design the architecture, insuring proper mapping and implementation.

**1.3.2.6. Architecture** Concepts

To better protect D/As from new and emerging threats, the Cyber.gov

program has identified four key cybersecurity pillars, which are the driving

philosophies of this architecture:

1. Leverage fine-grained monitoring and control, allowing cyber threats to be

mitigated with precision, minimizing impact on legitimate activities.

2. Use whitelist-based security policies to describe allowed activity, instead of

trying to enumerate the ever-increasing types of malicious activity.

3. Automate the cybersecurity decision loop, reducing the burden on cyber

operators and speeding up the rate at which cyber threats can be

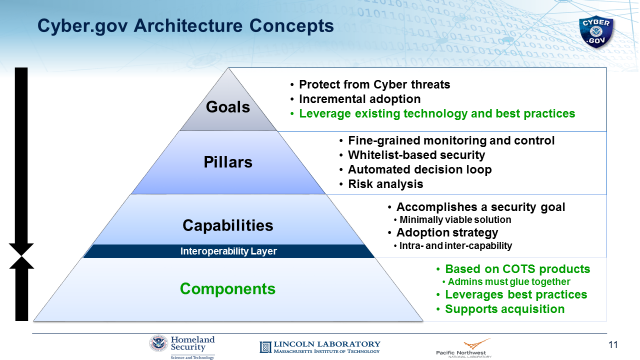
detected and mitigated.

4. Continuously conduct risk analysis in order to assess and strengthen the

D/As cybersecurity posture.

In order to fully realize the four pillars of the architecture. The Cyber.gov

architecture synergizes the concepts of Components and Capabilities.



**Figure 1: Architecture Concepts**

**Capabilities**

Capabilities are at the core of the Cyber.gov architecture. They are the items

that most directly accomplish the architecture’s goals and implement the

architecture’s cybersecurity pillars. In essence, any given capability is

responsible for accomplishing a concrete security goal that reduces risk for a

D/A. Capabilities are each *minimally-viable solutions* to the security

problem they target, and they can be deployed independently of each other

to provide immediate value. As more capabilities are deployed, they

interoperate and their utility increases.

Each Cyber.gov capability has the following properties:

• **A security goal** describing specific threats against which the capability

protects.

• **Operational recommendations** that aid successful deployment and

operation of a capability (for example, rule classes, risk calculations,

segmentation strategies).

• **An implementation point** defining where the capability is logically (and

sometimes physically) placed to accomplish its security goal.

• **Interoperability with other capabilities** through producing data that

can be used by other capabilities and consuming data produced by other

capabilities.

• **An incremental adoption plan** defining a phased adoption allowing

D/As to incrementally roll out the capability and minimize impact to the

D/A’s workflow.

**Components**

Components are the products and services that are used to implement

capabilities. Broadly speaking, these map to one or more existing solutions

(e.g., commercial products, open source, or government technology). They

also detail what interoperability functionality the components must support

to enable the capability.

Each component includes a set of requirements, which are classified as

*required, recommended, or nice-to-have*. These requirements dictate the

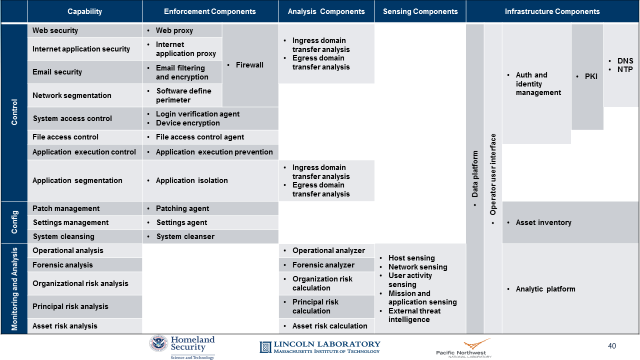
functionality an off-the-shelf product must support in order to be fulfill the

role of this component in the Cyber.gov architecture.

Many components support only a single capability, but some are leveraged

by multiple capabilities.

***1.3.2.7*** *Capabilities mapped to Components*



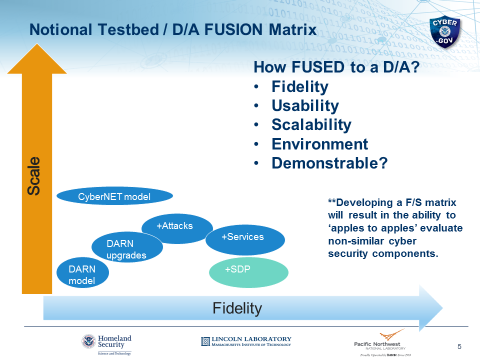
**Figure 2: System ArchitectureOverview**

#### 1.3.2.8Task C3: Cyber.Gov Testbeds and Implementations

PNNL has developed and maintains several testbeds that support a variety of applications, including enterprise cyber testing and evaluation, power systems and ICS/SCADA systems, as well as classified capabilities. These are cloud-based systems that provide easy extensibility and reconfiguration for the cyber systems being modeled. Additionally, these environments are fully instrumented, and scientifically controlled to provide assurance for any experiments or system validation and verification efforts. Many of these systems are remotely accessible and can be federated with other testbed capabilities as needed.  PNNL has also put extensive effort into developing an instantiation of a realistic enterprise (full IT infrastructure) with systems, networking, user roles, data, and specific missions in the testbed environment that serves as a well-studied model of a medium sized enterprise. PNNL also has developed an “Impediments” team, which develops and executes rigorous, repeatable experiments in the testbed environment by introducing impediments to the modeled cyber systems. These impediments go beyond the traditional red team exercises in which the goal is for the red team to prove that they can breach perimeter defenses. To test the efficacy and utility of the proposed architecture, it will be essential to leverage the Impediments team’s ability to 1) model adversary activities far upstream of breach, such as probing; and 2) model adversary activities far after breach such as lateral movement and action on target. In both cases as well as for breach instances, the goal will be to assess the ability of the proposed architecture and implementation to provide reliable indicators of adversarial behavior, and to block or interfere with this behavior. Furthermore, malicious actors will not be the only class of impediments considered. Natural faults, third party access, and environmental conditions all play a crucial role in real world cyber system security. Testing and evaluation regimens needs to ensure a full spectrum evaluation whenever possible.

For this Task, a specific instantiation of a representative, model D/A will be constructed. This will be influenced by the results of the System Analysis task so that key aspects of the model site capture the essential features of real D/A’s. This exemplar will exhibit the complexity and relevant features of the Department or Agency environment without becoming a cost prohibitive one to one recreation. This may include details about the network partition between user and service enclaves, and a mapping of how the cyber systems relate to the overall missions of the D/A, services, number and topologies of systems, and other information as necessary. In this environment we will deploy instances of key technologies and architecture design elements as needed by the Cyber.Gov team. For instance, we anticipate building SDP in the testbed for the purposes of assessing their performance and run-time requirements. Likewise, we will build out the infrastructure required by the designed architecture that is to be used for self-assessment and performance monitoring. As self-monitoring is a key element of the architecture design, this will need to be present in the testbed.

Testbed as fusion environment where a D/A network architecture is fused with SW/HW, services, threat vectors, etc., to mimic (reflect) a “real” D/A to the extent possible.



**Figure 3: D/A Notional Testbed Matrix**

#### 1.3.2.9 Task C4: D/A Engagement, Planning, and Pilot Preparation

Regular engagement across a collection of prioritized D/As that represent a varied sample across multiple categories will create the basis for feedback and validation of the work products coming out of the C2 tasks. These periodic engagements throughout the life of the program will be intended to build relational and technical trust, while allowing target customers to provide feedback to the innovation coming from the program. This task and associated personnel will function as the main points of contact for the D/As into the Cyber.Gov program.

We anticipate this relationship will unfold through a series of engagements with staff at different positions (e.g. CIO/CISO, IT managers, and cyber defenders). First, results of the system analysis will be shared with D/A’s upon request. This will ensure that two-way communication is open with D/A’s that are open to such communication. As technologies are developed and deployed in the testbed environment, additional meetings will occur with D/A’s to demonstrate the functionality of implemented components and allow for additional feedback both on the testbed environment and implementation details that may be important factors for technology adoption by the D/A. Select D/A’s who are willing to pilot technology components and/or the full Cyber.Gov architecture will have further engagements through task C4 to guide the technology transfer process with the D/A and that they are supported through the implementation process. This will maximize the potential for D/A’s to adopt the Cyber.Gov architecture.

Information obtained through task C1 on D/A tools, technology, NIST implementation, component configuration, and overall environment will be generalized to requirements for a testbed implementation. It is anticipated that multiple representative D/A instantiations will be required within the testbed to most accurately cover the breadth of diversity of D/As. Task C4 will work across C2c and C3 to ensure these environments and architecture implementations are representative, and that testing results are readily shared with the engaged D/As. D/A feedback and requirement refinements will be shared back to the broader program through this task.

## Transition Plan

**1.4.1** Project Transition

The targeted acquisition program for the Cyber.gov program is, OMB the Federal D/As, state and local CIOs/CISOs, Government Services Agency (GSA), the public sector and CS&C.

For CS&C, there are several risks that will need to be coordinated in order for this to happen:

1. Acquisition schedule synchronization. The July 2016 meeting between CSD and CS&C illustrated the need for both parties to understand both the NCPS acquisition timeline and the planned capability builds and the S&T project timeline and how demonstrations of technology would best influence the acquisition timeline.
2. Technical capability roadmap. One element of the Cyber.gov program is to make available additional technology layers. Currently, E3A only analyzes DNS and email traffic. CS&C noted that it only examines two traffic types by design and that they have funded work to examine what other traffic types should be included. This is another area where additional coordination is required between CS&C and S&T/CSD.

Several D/A’s have expressed an interest in participating in planned assessments, feedback reporting, demonstrations and pilots.

As part of the interviews and data collection for Task C1, the performer team have begun engagements with several D/As, including Mr. Grant Schnieder, U.S. Federal Chief Information Security Officer (CISO), EOP/OMB, Mr. Scott Bernard, Chief Enterprise Architect, EOP/OMB and Mr. David Walter, Chief Information Officer (CIO) of OSHRC, USCIS, FEC, CNCS, VA and others in the field to observe and capture their operations and cyber security posture categorically. In addition, Cyber.gov in cooperation with Federal Emergency Management Agency (FEMA) have begun to assess State Local Tribal Territory (SLTT) to include, State of Washington, City of Tacoma, WA and City of Santa Clara, CA. These SLTT are also aimed to influence the architecture development throughout the research and development phases.

We will ensure proper tracking of each component of the architecture into the D/As and new implemented NIST controls thanks to the new baseline requirements combined with their NIST mapping strategy.

In addition, CSD and the Cyber.gov program are coordinating with the NPPD CS&C CTO Office and the CS&C Federal Network Resilience (FNR) office, including the Continuous Diagnostics and Mitigation (CDM) and National Cybersecurity Protection System (NCPS). The CSD Cyber.gov applied R&D program will gain insight to current federal department and agency as-is capabilities as well as operational threat frameworks for Cyber.gov gap prioritization. CS&C is conducting an effort called .govCAR that is examining current federal capabilities and threats, similar to a review that DOD conducted on their NIPR and SIPR networks. CSD and Cyber.gov have already provided initial technical and architectural products to NPPD for peer review, comment, and feedback. As the ongoing phases of Cyber.gov develop a full architecture and to-be state, technical details, modeling & simulation, testbed analysis, and prototyping, there will be continuous coordination with NPPD for input and feedback. CSD executive and NPPD executives are in continuing strategic discussions as to a roadmap for potential transition points and operational implementation, budget, and acquisition mechanisms with lessons learned from the CDM program. CSD and NPPD also continue coordination with NIST as to the potential of future updates to NIST frameworks, standards, and FISMA due to Cyber.gov applied R&D results.

**1.4.2** Project Architecture Roadmap

The following technical roadmap illustrates a 3-year architecture transition pathway that begins in the late quarter of FY16 with Cyber.gov applied R&D project task to conduct a Classified Indicator Study of Einstein E3A as well as conduct initial D/A outreach. The Classified Indicator Study’s four main analysis goals include: a contextual map, impact categorization, uniqueness, and timeliness and volume. In addition, an independent analysis of modern advance persistent threats that will analyze attack vectors of a selection of modern malware and APTs detailing how the Einstein E3A system would defend against these threats. The D/A outreach has led to onsite system analysis meetings with the departments CIO/CISO teams. The outcome of these system analysis have led to an initial instantiation of the Cyber.gov Network Segmentation architecture v1.0 that includes the following baseline requirement documentation:

* Architecture Specification
* Application Isolation
* Network Segmentation
* Authentication and Identification
* Software Defined Perimeter

Cyber.gov will establish testbeds and model and simulation infrastructure to test

out the spiral phases of each instantiation of the architecture with broader testing

in a D/A Representative Network (DARN) of the full architecture. These DARN

events will be baselined into D/A proof of concept and piloted opportunities of

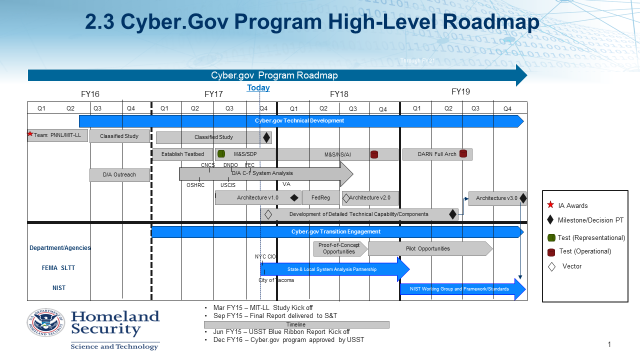
select D/A and select SLTT agencies. The feedback from these opportunities will

Influence the next version release of detailed technical capabilities and components

of the architecture. The eventual adoption of the architecture will be through

iterative peer reviews inside the Federal Register and through coordination with

NIST working group and cybersecurity framework standards.



**Figure 4: High-Level Roadmap**

**1.4.2.1** Process Review Criteria

Cyber. Gov will develop an architecture based upon a transparent and validated

process review for each instantiation release of the architecture. Illustrated here,

the architecture team will release phased batch release of components/capabilities

into Batch releases that will then be placed into peer review at NPPD/CS&C and the

Federal Register through a Federal Notice for public comment. This process will be

approx. 60 days and then will go through an adjudication process before for the final

component/capability is updated and reflected in updated architectural products and

technical artifacts.

The Cyber.gov program recognizes that private sector enterprises are contending with similar threats and challenges, and also recognizes that there is rapid innovation of security products and architectural approaches by vendors and service providers, from start-ups to established companies. The Cyber.gov program aims to tap into those lessons learned and innovation to gather feedback on proposed architectural approaches, technical requirements, implementation guidelines, and any gaps that are not being addressed.

The first in a series of documents the Cyber.gov program will release to the federal register for public comments and feedback contains: a context document; a document describing a capability of the Cyber.gov architecture (network segmentation); and baseline requirement documents for the major components needed to implement that capability. As the program continues, a more robust and complete architectural picture is being developed that will provide a more coherent design and integration of all capabilities, which will also be made available for public comment and feedback. Likely followed by a detailed technical capability packet for application isolation/segmentation.

**B1**

V1.0

V1.0

Network Segmentation Fed Register Initial Adoption Pilot Opportunities

Control Capability Peer Review

V1.0

**B1**

Full Scale Adoption D/A Transition RFI Process Refresh/Maintenance

…

V2.0

V2.0

**B2**

App Isolation Fed Register Initial Adoption Pilot Opportunities

Control Capability Peer Review

**1.4.2.2** Transition to DHS Component Use

The successful adoption of the Cyber.gov architecture across the federal departments and agencies (D/As) hinges upon five factors to motivate acceptance by key stakeholders: cyber security benefit, coverage, value, ease, and impacts. The objective of the Cyber.gov architecture is to provide D/As access to the highest level of security currently possible. For adoption, it will be necessary to show this objective is met – through quantifiable improvements to D/As current security posture, an ability to upgrade and modify to match evolving threats, and the resilience to maintain key missions under duress. Related to this, CIOs and CISOs will require proof that the architecture provides coverage for all mandates and regulatory requirements their organization must meet (e.g. FISMA). Further, value will be an important consideration for adoption, and can be shown via a decrease in overall capital/operational expenditure and the architecture’s ability to leverage existing legacy defense tools rather the forklift upgrades. Finally, the ease of adoption and impact to users must be understood and influential in the overall adoption process. Using these factors as considerations for the successful adoption of the Cyber.gov architecture, the following four phases are presented at a high level: Initiation, Initial Adoption, Full Scale Adoption, and Sustainment/Refresh.

Phase 1- Initiation

The key to the initiation phase is to create an ecosystem which establishes a common venue for information sharing, technology distribution, and continuous improvement. Such a focal point would establish the program as a center for integration between all stakeholders including D/A management, subject matter experts, vendors of cyber security tools and services, research- and standards-focused institutions, and government-oversight entities. The ecosystem must include the canonical location for the architecture information, a marketplace for vendors to post vetted tools and services, a training and certification component, and a maintenance organization to provide the vetting of tools and support of stakeholders interacting with site services.

Phase 2 -Initial Adoption

Before full scale adoption can be established, the Cyber.gov program needs to establish credibility through proof of concept and pilot opportunities. Not only do these provide quantifiable evidence of five factors mentioned above (cyber security benefit, coverage, value, ease, impact), but they also help to establish “champions” of the architecture to convince others of the benefits of adoption. The key is to pilot technologies or services which have a measurable impact to the security posture and provide excellent feedback mechanisms for both information technology employees and end users.

Phase 3 - Full Scale Adoption

Once the initial adoption phase has resulted in greater forward progress, it will be important to understand the efforts required to sustain progress. There is a broad spectrum of D/A maturity and needs. Some organizations will need “turn-key” installations with onsite support, while other organizations will be able to complete adoption efforts with minimal helpdesk style support. Mismatch in providing the right level of support will induce frustration and cause the adoption of even the best capability to proceed poorly or even fail. Also, it is important to realize that 100% adoption will not be achievable due to the evolving nature of the architecture, and therefore it may be better to map current capabilities and understand priorities according to measured risks.

***Phase 4*** *- Sustainment and Refresh Maintenance*

The bookend of a successful adoption process results in a sustained ecosystem

which continues to fuel the full-scale adoption of the architecture. Sustainment

must include the continued measurement of benefit and risk of the current

architecture, resulting in targeted refreshes of the architecture that is not purely

based upon a date-trigger, and then relevant updates at the D/As.

To support the maintenance and update of the architecture at a given D/A, one

concept the Cyber.gov effort is exploring is utilizing a *modeled system* to assess the

need to update a particular capability and/or component of the architecture. In this

*modeled system*, there would be the ability to run comparisons using data on the

threats and vulnerabilities from specific implemented versions (since the Cyber.gov

architecture will not be a one-size fits all). Tests can be run against these models to

compare their effective mitigation, which can be condensed into a risk score of some

kind. Risk trend reports could then be produced by running tests over time to

attempt to predict when an unacceptable amount of risk would reach a threshold.

Unacceptable risk scores and/or trends towards an unacceptable amount of risk

would trigger an appropriate upgrade or refresh look at the architecture and its

components/capabilities.

To support maintenance and upgrades to the overall architecture there may be a

similar approach. The Cyber.gov effort is researching the development of a similar

*comparative analysis* of variants to drive a risk-based timeline. Monitoring and

observance of risk profiles that can trigger the need for analysis and updates to the

overall architecture. Secondly, there should be analysis of the adoption and

supporting trends for the architecture. The gaps revealed by this analysis would be

an important indicator for prompting a new evaluation of the overall architecture.

These methods of analysis will require an understanding of which components and

capabilities are in use at various D/As including which ones are not being adopted.

While exact operational and policy mechanisms would need to be established,

there could be a data store of a variety of usage data sent to a central authority

voluntarily or as a requirement from the D/As. That data could be used to

maintain the models and to help assess risk. The Cyber.gov architecture is

researching and does contemplate inclusion of a data sharing platform as a key

component.

An additional longer term consideration is based upon current facts that there are

several critical services which many D/As are not able to sustain on their own due

to resource constraints, including *cyber forensics* and *red teaming*. As part of

sustainment and architectural refresh processes, DHS or some other operational or

policy entity should consider establishing a highly skilled team as a shared asset or

service for the resource-constrained D/As. Such support capability or a National

Coordination Office concept could provide the necessary data and inputs upon

which architectural analysis and refresh trigger points would utilize, in addition to

ongoing awareness of what private and commercial sectors are adopting as

innovative or next-generation cyber-security architectures and products/services

emerge.

## Schedule and Budget Summary

### Project Schedule and Budget Summary

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Funding Source** | **FY16** | **FY17** | **FY18** | **FY19** | **FY20** | **FY21** | **Total** |
| Internal (S&T) | 10,000,000 | 9,999,690 | 10,000,000 | 10,000,000 | 10,000,000 | 10,000,000 | 59,999,690 |
| External | N/A | N/A | TBD | TBD | TBD | TBD |  |
| **Total** |  |  |  |  |  |  | **$59,999,690** |

**Figure 5: Budget Source Summary (\*Note FY17 and out year numbers subject to final budget decisions and appropriations)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Project Activities** | **FY16** | **FY17** | **FY18** | **FY19** | **FY20** | **FY21** | **Total** |
| Program Support (e.g. IPA/SETA/CAPO/SBIR/PPP) | $1,038,618 | $1,930,739 | $1,100,000 | $1,100,000 | $1,100,000 | $1,100,000 | $7,369,357 |
| Cyber.gov Subject Matter Expertise | $176,251 | $363,692 | $363,692 | $363,692 | $363,692 | $363,692 | 1,994,711 |
| Utility of Classified Signatures (A) | $1.500,000 |  |  |  |  |  | 1,500,000 |
| Measurement Infrastructure (B) | $500,000 |  |  |  |  |  | 500,000 |
| D/A Engagement and System Analysis (C1) | $350,000 | $1,200,000 | $1,000,000 | $1,000,000 | $1,000,000 | $1,000,000 | $5,550,000 |
| Architecture, Test beds, Continuous Update/Assessment, Implementation (C2, C3, C4) | $6,435,131 | $6,505,259 | $7,536,308 | $7,536,308 | $7,536,308 | $7,536,308 | $43,085,622 |
| **Total Executable** | **$10,000,000** | **$9,999,690** | **$10,000,000** | **$10,000,000** | **$10,000,000** | **$10,000,000** | **$59,999,690** |

**Figure 6: High-Level Milestone and Budget Summary**

## Project Organization

### Project Personnel

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Organization** | **Title/Role** | **Email** | **Phone** |
| Douglas Maughan | DHS S&T/Cyber Security Division (CSD) | CSD Division Director | [Douglas.maughan@hq.dhs.gov](mailto:Douglas.maughan@hq.dhs.gov) | 202-254-6145 |
| Chase Garwood | DHS S&T/Cyber Security Division | Program Manager (PM)  Contracting Officer Rep (COR) | [Chase.Garwood@hq.dhs.gov](mailto:Chase.Garwood@hq.dhs.gov) | 202-254-6076 |
| Michael Jones | Office of Procurement Operations (OPO) | Contracting Officer | [Michael.Jones@hq.dhs.gov](mailto:Michael.Jones@hq.dhs.gov) | 202-254-5676 |
| David Collins | DHS S&T/Cyber Security Division (CSD) | SETA Support | [david.collins@associates.hq.dhs.gov](mailto:david.collins@associates.hq.dhs.gov) | 202-254-6737 |
| Teresa Burt | DHS S&T/Cyber Security Division (CSD) | SETA Support | [teresa.burt@associates.hq.dhs.gov](mailto:teresa.burt@associates.hq.dhs.gov) | 202-254-5337 |
| Laura Delaney | Office of Cyber Security and Communications (CS&C) | Deputy Director | [Laura.Delaney@hq.dhs.gov](mailto:Laura.Delaney@hq.dhs.gov) | 703-235-3015 |
| Paula Donovan | MIT-LL | MIT-LL Assistant Group Leader | pjdonovan@ll.mit.edu | 781-981-7589 |
| Jeff Mauth | PNNL | PNNL Project Manager | Jeff.Mauth@pnnl.gov | 509-578-4864 |

Figure 7: Project Personnel

### Internal Structure

Figure 8: Project Personnel

## Benefits to S&T

### New Capabilities / Technology

Cyber.gov will provide significant deliverables including an innovative and holistic cyber architecture including its detailed schema and baseline requirements.

The team will also provide a complete assessment of Software Defined Perimeter and its benefits which could potentially help mitigate dozens of current threat vectors which many are the source of the latest breaches of the .Gov domain.

The initial phase of Cyber.gov includes a systems analysis, architecture analysis of alternatives and piloting of a measurement infrastructure. The results of these, as well as the results of a classified signature study, will help determine the right technologies (or non-material solutions) to pursue development in the case of new technologies, or accelerated deployment of, in the case of existing capabilities.

### New Intellectual Property

At this point in the project, it is unknown what, if any, intellectual property will be produced by this effort. The Cyber.gov program management team will contact Lavanya “Elle” Ratnam at [Lavanya.ratnam@hq.dhs.gov](mailto:Lavanya.ratnam@hq.dhs.gov) at S&T’s Office of General Council for assistance with all IP questions and issues.

### Public Access of Federally Funded Scientific Research

The Cyber.gov program will comply with the intent of the DHS Plan to Support Increased Public Access to the Results of Research Funded by the Federal Government 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.

### Data Management

The Cyber.gov program will comply with the intent of the DHS Plan to Support Increased Public Access to the Results of Research Funded by the Federal Government and develop the appropriate data management plan if the electronic data sets created in the project fall under the purview of the DHS guidance.

### Other Benefits

No additional benefits for S&T are expected to be produced by this effort other than those described in Section 1.7.1. Given the nature of research and development, however, this is subject to change.



### Assumptions

Assumptions for this project include, but are not limited to:

* The S&T project was established by the USST and while collaboration with the Program Management Office for NCPS is important, this is a research effort that is proceed semi-autonomously. This is in line with the philosophy that a research pull is sometimes needed for capability advancement rather than requirements “push”.
* New research areas or requirements may emerge once the current research begins.

Constraints include:

* NCPS Program Office may not provide the proper data to assess classified indicator impact within the scope of Cyber.gov program related to the Task A and B. (Confirmed this during Q4, FY 16 meeting)
* Resources at D/As are limited and this will require coordination ahead of any deployment or demonstration.

# Requirements

## Requirements Management Plan

The initial requirements for Cyber.gov were derived from three primary documents, the aforementioned reports from MIT-LL and the BRP and GAO Report 16-294[[1]](#footnote-2). As discussions with NPPD (CS&C) and other D/As continue following the project kick off in Q4, FY 16, there may be additional requirements collected.

Requirements will be tracked primarily in common Microsoft Office tools so they can be shared widely with the Cyber.gov project team, other stakeholders and the research teams as needed. A requirements traceability matrix template has been developed for this project and includes key elements such as:

* Technical Assumption(s) or Customer Need(s): Description of the technical assumption or customer need linked to the functional requirement.
* Functional Requirement: Description of the functional requirement.
* Status: Current status of the functional requirement.
* Architectural/Design Document: This column should be populated with a description of the architectural/design document linked to the functional requirement.
* Technical Specification: This column should be populated with a description of the technical specification linked to the functional requirement.
* System Component(s): This column should be populated with a description of the system component(s) linked to the functional requirement.
* Software Module(s): This column should be populated with a description of the software module(s) linked to the functional requirement.
* Test Case Number: Test case number linked to the functional requirement.
* Tested In: The module or activity that the functional requirement has been tested in.
* Implemented In: The module or activity that the functional requirement has been implemented in.
* Verification: A description of the verification document linked to the functional requirement.

### Test and Evaluation

Four approaches will be used to assess the extent to which the project requirements are met: *modeling and simulation*, an *emulation testbed*, *deployment/cyber posture* *data analysis* and an *adversarial assessment*.

Modeling and Simulation: This activity will develop and demonstrate a cyber modeling and simulation framework that supports quantitative assessment of cyber capabilities intended for deployment on D/A enterprise networks. This framework will contain the following components to provide meaningful quantitative results: environment model, threat model, defensive capability model, mission model and cyber metrics. MIT-LL and PNNL will work together on this activity to help develop a modeling and simulation framework.

Testbed: PNNL will lead the testbed effort, leveraging their existing cloud based T&E systems. These environments are fully instrumented, and scientifically controlled to provide assurance for any experiments or system validation and verification efforts. Many of these systems are remotely accessible and can be federated with other testbed capabilities as needed. PNNL has also put extensive effort into developing an instantiation of a realistic enterprise (full IT infrastructure) with systems, networking, user roles, data, and specific missions in the testbed environment that serves as a well-studied model of a medium sized enterprise. PNNL also has developed an “Impediments” team, which develops and executes rigorous, repeatable experiments in the testbed environment by introducing impediments to the modeled cyber systems. These impediments go beyond the traditional red team exercises in which the goal is for the red team to prove that they can breach perimeter defenses. To test the efficacy and utility of the proposed architecture, it will be essential to leverage the Impediments team’s ability to 1) model adversary activities far upstream of breach, such as probing; and 2) model adversary activities far after breach such as lateral movement and action on target. In both cases as well as for breach instances, the goal will be to assess the ability of the proposed architecture and implementation to provide reliable indicators of adversarial behavior, and to block or interfere with this behavior. Furthermore, malicious actors will not be the only class of impediments considered. Natural faults, third party access, and environmental conditions all play a crucial role in real world cyber system security.

For this C3 Task, a specific instantiation of a representative D/A will be constructed. This will be influenced by the results of the System Analysis task (see 1.3.2.3) so that key aspects of the model site capture the essential features of real D/A’s. This exemplar will exhibit the complexity and relevant features of the Department or Agency environment without becoming a cost prohibitive one to one re-creation. This may include details about the network partition between user and service enclaves, and a mapping of how the cyber systems relate to the overall missions of the D/A, services, number and topologies of systems, and other information as necessary.

In the first two years of the program, the Cyber.gov project will, via PNNL:

* Construct a model of a selected D/A
* Map mission activities to this model
* Instrument this model using an architecture similar to that proposed by the Architecture team (preliminary instrumentation via initial funding; refined instrumentation contingent on additional funds)
* Develop experimental Impediments to challenge and assess the value of the proposed architecture

Deployment/Cyber posture data analysis: in order to properly assess the success of the cyber security architecture, a data analysis of the D/As will be performed to measure new controls implemented and components implemented.

Adversarial Assessment: The Cyber.gov project intends to subject each system, their component technologies, and the processes and procedures that result from the research to an independent, adversarial red-team assessment to identify the extent to which they truly make D/A missions and systems more resilient to cyber-attack and exploitation. AIS will be the lead organization for this element of the test and evaluation process.

## Customer Engagement

The customers for Cyber.gov include the Federal D/As, State, Local, NPPD (CS&C) and, private sector customers. The team will do its best to work with a minimum of 10 D/As to understand their challenges and the solutions they currently utilize (software, hardware, and process), in order to create a comprehensive view of their cyber security architecture. This provides value in both as is (baseline) and to be (future) in order to quantify benefit measures this analysis provides. The selected D/As will include a diverse set of types and sizes to include at least two small, three medium, and two large D/As.

CS&C leadership was involved in early discussions on the Cyber.gov project following the release of the MIT-LL and BRP reports. The Cyber.gov team and CS&C leadership initiated further discussions on the program in early Q4, FY16 and are expected to continue. The primary CS&C representative for Cyber.gov interactions will be Ms. Laura Delany, Deputy Director of the Network Security Deployment (NSD) Division of CS&C.

D/As’ participation in Cyber.gov is critical as they are critical end user of the NCPS system, in addition to their own network security systems. CSD has secured interest from several agencies to participate in pilots of Cyber.gov technologies and research, including, but not limited to: the DHS OCIO (Jeffrey Eisensmith), the United States Citizenship and Immigration Services (USCIS), the Occupational Safety and Health Review Commission (OSHRC), and the Office of Management and Budget (OMB).

Influential decision makers who have endorsed this work include:

* Dr. Reginald Brothers, USST. During Dr. Brothers’ tenure, he directed S&T/CSD to develop a program strategy to address the findings and recommendations from the MIT-LL and BRP reports.
  + Result of this phone call were to establish within OMB guidance to develop Cyber.gov program within S&T

## Customer Requirements

The high level requirements for the Cyber.gov project are derived from common threats, the findings and recommendations from the MIT-LL, and BRP reports and common best cyber security practices. These findings are summarized below.

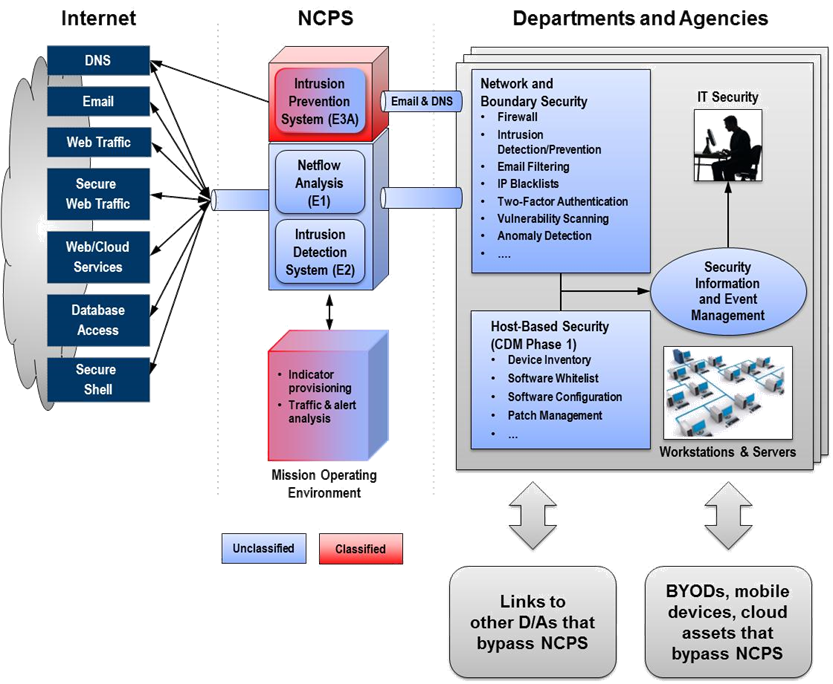
* + A proper cyber security posture does not rely solely anymore on Border Perimeter(s), we have to also address proper baseline requirements documentation for the other components of the cyber security architecture. We have currently defined 34 components that will be assessed and properly documented with clear requirements and implementation guidelines during FY17.
  + The .Gov domain needs to implement additional layers such as Software Defined Perimeter solutions at a faster pace, similar to the commercial sector in order to remain secure and up to date.
  + Government Officials did not possess proper asset information regarding the current software solutions and hardware systems on the .Gov domain. A software and hardware inventory must be performed to understand the current positioning and properly adapt our cyber security controls accordingly.
  + We must be able to rapidly prototype and tests technologies according to clearly defined baselines and ensure requirements are properly met.
  + We must guide vendors to develop and integrate desired features to their solutions at little or no cost to the D/As by defining baseline requirements for each components and updating them at least yearly.
  + Perimeter defense alone is no longer effective against advanced persistent threats (APTs).
  + E3A blacklists are beneficial but do not prevent the most advanced threats.
  + Best practices have revealed effective cyber defense system should be made up of overlapping, redundant, layered, pervasive, and rapidly updated defenses.
  + There is a critical need to provide new security controls against threats on Legacy systems, the cloud and mobile.
  + The capabilities of NCPS along with allocated resources and authorities are not aligned with the responsibilities that have been given to DHS nor do they align with DHS’s own aspirations and the self-characterization of its systems. Additional layers will be required.

In addition, the 2015 DHS IPT process brought to light some of the same capability gaps identified by the studies. For example:

* + IPT Gap #G-Cyber-NWSec-026 was described as: “Lack the capability to perform detailed analysis of the utility of classified E3A indicators compared to commercial approaches and to the protection currently provided by D/A security tools.

The DHS NPPD, which has responsibility for acquisition and operation of the NCPS, has accepted the recommendation for the need to study and document the contribution of classified indicators to NCPS effectiveness and has agreed to work jointly with the DHS Science and Technology (S&T) Directorate’s Cyber Security Division (CSD) to that end. While NPPD determines its path forward with respect to the other recommendations, S&T CSD will embark on a program of research, design, implementation and demonstration that will leverage the successful aspects of the existing NPPD platform while bridging the gap between what the D/As have today and what they truly need.

A basic Operational View (OV) of NCPS is presented below for reference.

**Figure 9: NCPS Overview**

## Key Functions and Desired Performance Requirements

The key Performance Parameters outlined in the table below were submitted as part of the Portfolio Assessment Review (PAR) review panel in May 2016 and updated in January 2017. As customer engagement progresses, these KPPs may be adjusted.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Key Performance Parameters** | **Current Capability**  (Existing operational capability) | **Threshold Objective**  (Min acceptable performance improvement) | **Project Objective**  (Stretch goal for project) | **Time Frame** |
| **# of common capability gaps addressed by architecture, solution in testbed and implemented at D/A or DARN** | **N/A** | **4** | **8** | **Length of Program** |
| **# of D/As. Assessed for common capability gaps in order to inform the architecture** | **N/A** | **8** | **10** | **FY17, FY18Q3** |
| **% of D/A feedback surveys indicating that the D/A is interested in adopting a portion of the Cyber.gov architecture** | **N/A** | **60%** | **90%** | **Length of Program** |
| **# of Individual components implemented/deployed within a generic DARN environment** | **N/A** | **5** | **33** | **12 Months** |
| **# of integrated capability packages (collection of components) successfully deployed/cleared in a generic DARN environment/recommended for D/A Pilots** | **N/A** | **1** | **16** | **18 Months** |

Figure 10: Key Performance Parameters (Draft)

## Other Metrics

None at this time.

# Technology and Innovation

## Core Technology

The first year of the Cyber.gov Program will primarily focus on the 34 components of the cyber architecture including a focus on Software Defined Perimeter solutions and data collection and instrumentation, systems analysis and architectural analysis. The results of this early analysis will inform the proper implementation strategy to support Cyber.gov objectives. Additionally, there is a specific task for the research team to recommend technology development and deployment in order to meet technical gaps and/or deficiencies detected during the D/As’ assessments.

The research centers for this activity are MIT-LL and PNNL. The project will always try to leverage commercially available solutions first, including existing best practices from the commercial and private sector.

## Technology Scouting

Technology scouting is a continuous process that needs to be revisited and refined as a program evolves. The Cyber Security Division performs technology scouting on a regular basis through several proven methods:

* Industry engagement events. CSD sponsors several events and participates in a broad range of other industry and federal sponsored events, such as the annual RSA Conference, several events by the Security Innovation Network (SINET), Black Hat Conference and the annual Small Business Innovation Research (SBIR) Workshop DHS co-sponsors with DoD Office of the Assistant Secretary of Defense, Research and Engineering and the National Science Foundation.
* The Transition to Practice (TTP) Project regularly identifies technologies developed by other Federal research activities (primarily Department of Energy Laboratories, but also including DOD labs.
* Scouting of commercially available solutions in the private sector with several partners such as Google, Microsoft, RSA, Tenable, and more.
* Leveraging expertise from top experts in the private sector and world renowned labs
* Interagency coordination. CSD co-chairs the Networking and Information Technology research and Development (NITRD) Program’s Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG). Through monthly meetings and collaborations on specific technical planning projects, CSD stays up to date on what the 15 other Federal Agency participants in the IWG are funding across a broad range of cyber security topics, some of which are directly applicable to the requirements of the Cyber.gov research.

Members of the Cyber.gov team attend several of these events to determine the applicability of new or existing technologies in this space.

## Technical Approach

### Trade Space Analysis

The first year of the Cyber.gov program is a significant trade space analysis exercise. Specific tasks that will be used to determine a final technical approach include:

**Architectural Analysis.** Task C2. The objective of this task through the life of the Cyber.gov program is to very significantly improve upon the existing NCPS architecture, adding several additional layers in order to better protect the current cyber posture of the .Gov domain. This effort will review best practices, NIST publications and the 3 previous studies’ key findings and recommendations and provide a data call to the other sub-teams within the Cyber.gov effort. This data call will include (but will not be limited to) an understanding of cyber-related operations, industry standards, and the threat landscape by the System Analysis sub-team, an assessment of the effectiveness of the current classified indicators compared to commercially available indicators and the additional value of NCPS over the security mechanisms already in place at the D/As – by the Metrics and Data Analysis sub-team. Information, analysis and assessment results collected, along with substantial knowledge of current state-of-the-art and best practices, will enable the Architecture sub-team to design and eventually deploy an improved architecture.

The Architecture team will carefully consider how to effectively integrate existing D/A defenses with a national protection system. To accomplish this, the team will evaluate decentralized, hierarchical, and centralized architectures. The currently deployed centralized architectures may not provide the performance, scalability, and resilience needed as more types of data are gathered, analyzed, and acted upon. This task will also investigate architectures that incorporate cyber protection and defense services deployed inside D/As into a national protection system. The current NCPS system operates at the perimeter of D/A networks and therefore has limited information to use for detection and prevention and does not help to protect cloud and mobile systems.

D/As have also reported the difficulty in acting on notifications from the perimeter of their networks since that information does not have any internal D/A context. In addition, the perimeter of a D/A network is less well defined as organizations adopt cloud computing and integrate mobile devices into their environments.

The team will also consider the variety of D/A sizes, security postures, and threats to create architecture with a modular adoption approach. This would allow larger D/As to maintain more of their own infrastructure while relying on a national system where appropriate, while smaller or less capable D/As can subscribe to a more comprehensive set of cyber defense services.

An important characteristic of such architecture is the availability of interoperable components so that D/As and the national protection system can select components from vendors that best meet their needs. However, those components should seamlessly participate in the overall architecture. This task will therefore perform a gap analysis on interoperability standards that could be used in the architecture.

This task will study potential architectures for and the benefits of national coordination to aspects of the cyber defense mission, such as collaborative analytics, protection, and response. The current centralized NCPS has limited coordination and collaboration between itself and D/As. An architecture that supports higher levels of automated collaboration could result in earlier detection as well as faster and more thorough responses.

Finally, the architecture team will consider how a future cyber-resilient NCPS architecture can be designed. Such architecture would incorporate appropriate monitoring and actuation to observe the status of the NCPS system, respond to attacks, and evaluate the effectiveness of the system in normal operation and when the system itself is attacked.

**D/A Systems Analysis**. Task C1 focuses on understanding current cyber-related operations in the relevant D/As and the threat space encountered in the Cyber domain. D/A operations will be compared and contextualized with industry standards and the threats identified in order to scope the initial focus of the Cyber.gov effort. In order to understand the operational environment, PNNL and MIT LL will work with several D/As to understand their cyber defense systems as deployed and what threats are considered highest priority. Cyber defenses will be considered at both the “enterprise” level and for specific tactical networks to determine cyber vulnerabilities in the near and far term, including for tactical networks with an attack on enterprise systems, which could have major operational consequences. This task will also examine the challenges faced by the D/As in implementing cyber defense systems.

### Preferred Alternative

The technical approach emphasizes foundational analysis activities in Year 1 and 2 of the Cyber.gov project, working primarily with D/As but also with NPPD (CS&C) to:

* understand how their cyber defense operations work today,
* understand their current asset inventory (hardware, software),
* understand their most significant challenges
* Use threat characterization to drive system requirements to ensure relevancy
* Develop prototype systems that can be integrated with other D/A tools into an extensible architecture including Software Defined Perimeter pilots,
* Instrumented prototype system
* Conduct independent, adversarial red team assessments, helping characterize the effectiveness of the prototype system and help quantify the extent to which the prototype system actually increases adversary workload.

The key questions the Cyber.gov research team aims to answer in Year 1 and 2 in order to define a path forward for technical solution development is below:

1. Under what conditions can alerts from classified indicators provide positive return-on-investment to DHS and D/As? From a practical perspective and in light of security, privacy, financial and other constraints, should NCPS continue to employ classified indicators?

2. How do we create proper security controls to solve the current gaps in mobile, legacy, cloud and patching/asset management systems?

3. Which architecture component(s) should be included to create an implementable and holistic cyber security architecture baseline that would solve many of the current vulnerabilities the D/As are facing today?

4. How do D/As operate their cyber defense systems today, and how do these operations compare to industry standards?

5. What are the highest priority cyber threats facing the D/As? To what extent are their existing systems mitigating those threats?

6. What tools or services should the government provide at the national level that would be most effective at mitigating the threats that the D/As cannot address by themselves individually, and what is the appropriate architecture for integrating the capabilities of these tools and services? What is the current maturity-level of the tools and services required?

7. How should threat and other cyber data be shared to better protect each D/A? Are D/As better off operating mainly independently, albeit with newer, more effective tools, or would they all benefit from shared experiences, data, knowledge and technology?

### Logistics Considerations

Logistics considerations for this project include:

* Ensuring access for the research team to DHS information and data, particularly for the classified signature study. Research team members who will need SCI access have been identified as well as those requiring SECRET. S&T/CSD PM Team will coordinate with the NPPD (CS&C) POC to facilitate access to required information.
* Given the dispersed geographic nature of the team (Washington DC, Lexington, MA, Richland, WA and Rome, NY), the majority of coordination will be done via email. Program reviews will be held primarily in Washington DC, but as needed, may be held in performer locations, especially if it coincides with a technical demonstration.

# Project Management

## 4.1 Acquisition Management

### Program Acquisitions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Acquisition**  **Description** | **Acquisition Strategy**  **(Contract, BAA, Grant, IA etc.)** | **Location of Work To Be Performed** | **Period of Performance** | **Award FY/Q** | **Total Estimated Value** |
| **PNNL Research Activity** | **Interagency Agreement** | **Richland, WA and Washington DC** | **30 June 2016 – 31 Aug 2017** | **Q3, FY 16** | **4,000,000** |
| **MIT-LL Research Activity** | **Interagency Agreement** | **Lexington. MA and Washington DC** | **30 June 2016 – 31 May 2017** | **Q3, FY 16** | **3,500,000** |
| **AIS** | **Contract** | **Rome, NY** | **6 June 2017 – 8 Aug 2020** | **Q3, FY 16** | **500,000** |

**Figure 11: Table of Acquisitions**

**\*Planned in FY 17 spend plan; subject to budget availability and other external factors (e.g. Continuing resolution)**

### Acquisition Strategy

For this research effort, Interagency Agreements were determined to be the best acquisition approach for several reasons:

* S&T/CSD was able to award funding through Interagency Agreements much more rapidly than through the normal competitive process
* MIT-LL was the author of one of the reports and thus had familiarity with the problem space.
* MIT-LL had developed relationships with several D/As as part of their investigations for their report “Evaluation of the Department of Homeland Security National Cyber Protection System”
* Use of National Lab and FFRDC resources is more appropriate than private firms, at least in the initial stages, due to the sensitive nature of the research
* PNNL has demonstrated past performance and expertise in managing the department of Energy’s CPP program, which shares similar objectives as NCPS.
* AIS has demonstrated past performance in red teaming activities

### Potential Sources

We are assessing 34 components’ vendors including SDP vendors such as Cryptzone, Vidder and Waverley Labs but at this point, it is still too early to determine what other developers could be because the analysis will be based on the baseline requirement which are to be determined based on initial Year 1 research and analysis.

## Scope Management

### Work Breakdown Structure

* Task A and B: **impact assessment of the E3A (Einstein) classified indicators** and **measurement infrastructure**.
* Task C: a **modern and holistic new cyber architecture** for the .Gov domain which solves many of the current issues with cloud, mobile, patching, legacy systems etc.:
  + Task C1: an overview of various sized (from micro to large) **Departments and Agencies (D/As)’ asset inventory and gap analysis**. We are conducting an extensive inventory of the different software solutions used for each of the System Architecture components (see 2.3)), the current hardware inventory, gap assessments and potential threats. These assessments will provide an initial Asset inventory that will serve to better protect our systems.
  + Task C2A: Software Defined Perimeter Assessment and Baselining.
  + Task C2B: Development of quick prototyping solutions to solve architecture issues
  + Task C2C: creation of a **complete architecture, implementation schemas and more importantly a baseline table of requirements for each component of the cyber architecture** (34 components, see Fig 2)) to guide CIO/CISOs on how to select vendors and properly implement those components into their architecture. Each component will have their own baseline, in order to properly guide the CIOs/CISOs through implementation.  It will motivate vendors to become more innovative and develop new “recommended” features, making those features move from “Recommended” to “Required” every year. It will also serve as a driving factor to encourage vendors to develop those features for the D/As at no cost. These requirements tables are based on the NIST publications and 800-53 controls.
  + Task C3: Cyber.gov testbeds, implementations: testing the proposed architectures against common threats and vulnerabilities issues. Implementation guidance for the D/As to ensure proper implementation.
  + Task C4: D/A Engagement, Planning, and Pilot Preparation: Information obtained through task C1 on D/A tools, technology, NIST implementation, component configuration, and overall environment will be generalized to requirements for a testbed implementation. It is anticipated that multiple representative D/A instantiations will be required within the testbed to most accurately cover the breadth of diversity of D/As. Task C4 will work across C2c and C3 to ensure these environments and architecture implementations are representative, and that testing results are readily shared with the engaged D/As.
  + Ideally, as technical solutions are developed, tested, measured, and reviewed with D/As the basis for pilot implementation will be formed. Task C4 will provide the definition, planning, and management of those pilot implementations and ensure high customer satisfaction throughout.

### Scope Control Plan

Products for this project are identified in the WBS in section 4.2.1. This is the product set for Year 1 of the project, which is analysis and a first draft of the cyber architecture design and schema. The WBS will be updated as the results of the Year 1 analyses are completed or nearing completion and decisions are made regarding implementation of alternative architectures and development or deployment of new technical capabilities.

This baseline will be maintained and changes to it must be approved by the Program Manager.

### Schedule Management

Schedule management is the process used to manage the project schedule to ensure that all products are delivered in the required timeframe. The major schedule milestones are listed in Section 4.2.4, Milestones/Deliverables, and the processes used to control the schedule are defined in Section 4.2.5, Schedule Control Plan.

### Milestones/Deliverables

| **Major Project Milestones/Deliverables** | **Scheduled Date** | **Status** |
| --- | --- | --- |
| **Task A and B** | |  |
| Program Strategy Approval | 12/2015 | Complete |
| Assess and measure E3A impact of classified indicators | 10/2017 |  |
| 1) Basic applicability of indicator information | 10/2017 |  |
| 2) Quality of signature that results | 10/2017 |  |
| **Task C** | |  |
| C1 – First D/A interview | 01/2017 | Complete |
| C1 – Initial System Analysis Brief (3-4 D/As) | 05/2017 | Complete |
| C1 – Interim System Analysis Brief | 08/2017 |  |
| C2a – Create simple development environment at MIT-LL | 02/2017 | Complete |
| C2a – Working demonstration of SDP with selected vendor(s) (within a testbed or test environment) for internal use only | 04/2017 | Complete |
| C2a – Report and Baseline requirements table for SDP | 04/2017 | Complete |
| C2b – Implementation and integration of first SDP (to be selected) features in a testbed | 05/2017 |  |
| C2b – Development of in-house components or middleware if needed for SDP and Cyber.gov architecture pilots | 10/2017 |  |
| C2b – Initial pilot of developed capabilities from the Cyber.gov architecture for select D/A partners | 01/2018 |  |
| C2c – Schedule and assignments for Baseline table components for P3-P6 | 03/2017 | Complete |
| C2c – Initial modeling and analysis capability | 04/2017 |  |
| C2c – Initial Architecture Technical Presentation | 04/2017 |  |
| C2c – Initial Architecture Report including baseline tables for priorities P0-02 | 04/2017 |  |
| C2c – Initial Architecture Programmatic Presentation | 04/2017 |  |
| C2c – Final Architecture Programmatic Presentation | 07/2017 |  |
| C2c – Final Architecture Technical Presentation | 08/2017 |  |
| C2c – Final Architecture Report including baseline tables for priorities P0-P6 | 10/2017 |  |
| C2c – Prototyping/deployment plan for FY18 | 12/2017 |  |
| C2c – Refined architecture | 01/2018 |  |
| C2c – M&S analysis capability for 3 (or more) architecture components | 01/2018 |  |
| C2 – Additional assessments | Ongoing, as needed |  |
| C3 – Initial Instantiation of D/A Architecture in testbed | 03/2017 | Complete |
| C3 – Initial Instantiation of SDP | 03/2017 | Complete |
| C3 – SDP technology stood up in a development and QA environment | 04/2017 | Complete |
| C3 – Initial Instantiation of D/A relevant threat | 05/2017 | Complete |
| C3 – Execution of technology assessments in a testbed environment (Pending completion of other Cyber.gov tasks) | 07/2017 | Complete |
| C3 - Implementation and integration of first SDP (to be selected) features in a testbed | 07/2017 | Complete |
| C3 – Additional Assessments | Ongoing as needed |  |
| C4 – D/A Engagement Plan | 04/2017 | Complete |
| C4 – Initial D/A profiles and environment requirements complete | 05/2017 |  |
| C4 – First D/A Meetings | 05/2017 | Complete |
| C4 – Summary report of D/A feedback, insights, and/or requirements complete | 09/2017 |  |
| C4 – Additional Assessments | Ongoing as needed |  |

Figure 12: Major Project Milestones and Deliverables by Phase

### Schedule Control Plan

The project schedule for each performer and the overall project will be reviewed at least bi-weekly with the Cyber.gov project team and performer to ensure all understand the current status of each task and to assess impacts of delayed tasks. If milestones are at risk based on task slippage, corrective action will be taken by the responsible party to a) get the tasks back on track and b) assess the root cause of the slippage in order to prevent future slippage for the same reason.

## Cost Management

### Cost Estimate

The total estimated cost for this project is $59.39M from FY 16 to FY 21.

Total cost was estimated based on conducting research efforts of similar size, and scope when aggregated into a larger set of research activities such as Cyber.gov. For example, CSD and other S&T organizations have conducted architectural assessments, utility assessments and data collection pilots and demonstrations.

Cost estimates are also based on previously funded work S&T has awarded to the National Laboratories, MIT-LL and other FFRDCs.

### Cost Baseline

The initial cost baseline of the project is outlined in Figure 5.

### Cost Control Plan

Cost reporting will be done on a monthly basis for each performer supporting the project. Currently, this includes MIT-LL, PNNL, and AIS.

Monthly costs will be compared against the expected costs established as part of the baseline. The Cyber.gov program management team will also examine schedule progress as part of the cost review to maintain a comprehensive picture of the project.

Monthly variances greater than 5 percent or cumulative variance greater than 10 percent will be examined to determine a) root cause of the variance, b) any impacts to project deliverable dates/quality, and c) corrective actions to bring the project closer to plan.

### Status Reporting

Monthly status reports are submitted by the current performers. The monthly status reports include: Technical Progress made in the previous month, planned technical activities for the next period, financial information from the previous month (expenditures, chart of planned vs actual expenditures, both for the period and cumulative) any schedule, technical or cost issues.

## Cost/Schedule/Performance Trade-Offs

Once the Year 1 analysis activities are completed, detailed trade off analysis can be conducted.

# Risk Management

## Risk Management Plan

The purpose of the Risk Management Plan (RMP) is to define the approach and practices a program will use to help minimize exposure to risks that negatively affect how the program fulfills its defined objectives. The RMP defines processes and tools that facilitate program efforts to execute projects successfully.

To help meet aggressive deadlines and get the most out of program resources, the RMP facilitates management focus on areas where the consequences of risks are most severe and where handling risks will be the most effective. The RMP focuses on early analysis and response to potential risks, and also supports the measurement of results and the use of lessons learned to reduce risks on future work. In addition to defining specific risk management (RM) processes, the RMP also defines the general practices (e.g., training and reviewing) that support the processes.

### Scope

The RMP covers all aspects of managing risks from preparation for risk management to execution of plans for handling identified risks. The RMP applies to all components of the program to include contractor (internal and external) and stakeholder support. The plan describes activities needed to manage risks at the Cyber.gov program management office (PMO) level. However, this risk management plan will utilize risk registers for tracking Cyber.gov program-level risks.

The RMP also provides insight on procedures for managing or escalating risks outside of a program to mitigate the program's high-impact risks. The Program Manager and Director will determine whether such escalation takes place.

In addition, the RMP describes the procedures for contingency planning and the methods to be used in tracking the various risk factors, evaluating changes in the levels of risk factors, and the responses to those changes. Additional factors that are considered in the Risk Management plan: contractual risk; technological risks; risks caused by the size and complexity of the product; risks in the development and target environments; risks in personnel acquisition, skill levels, and retention; risks to schedule and budget; and risks in achieving acquirer acceptance of the product.

## Risk Identification and Assessment

The risks associated with this project are as follows:

### Technical Risks

Primary technical risk for the Cyber.gov project in the analysis phase is the ability to conduct effective instrumentation and data collection demonstrations with D/A’s without disrupting or hindering their normal operational posture.

Mitigation: Detailed planning meetings with the D/A leads (identified early in the project), the performer team and the Cyber.gov program management team. Coordination meetings and joint development and review of the demonstration plans and events will also help mitigate this risk.

As other technical risks are identified, they will be placed on the risk register.

### Programmatic Risks

#### 5.2.2.1 Cost Risks

Cost risk will be closely managed by the Cyber.gov program management team. Monthly financial reporting is required from each performer and will be reviewed monthly to identify any unfavorable or unexpected trends.

#### 5.2.2.2 Scope/Performance Risks

Scope and performance risk are identified in the risk register below. The biggest scope risk is related to the position the NCPS Program Office (CS&C) has with the research areas and tasks that S&T has funded MIT-LL and PNNL to execute. CS&C feels that some of the tasks in Task A and B should be under their purview as the acquisition agent for NCPS.

This could potentially lead to ill-defined scope for the research team and could require modification to the existing IAs. This will in turn, result in some schedule slip, depending on the scale/complexity of the requested modifications.

Ensuring adoption of the cyber security architecture by the new team from the Office of Management and Budget and current administration will also be critical.

#### 5.2.2.3 Schedule Risks

For Task A and B, schedule risk is highly dependent on the outcomes of additional conversations needed between NPPD, S&T and potentially The DHS Under Secretary for Management (USM). Agreement (or not) at that level on the scope of Cyber.gov will determine:

* which elements of the Cyber.gov project plan will continue as outlined in the program strategy delivered to and approved by USST Brothers
* which elements will need modification, and
* which elements may be cancelled

Modification of the scope will incur schedule delays, especially if significant enough to require modifications to the Interagency Agreements (IA) awarded to MIT-LL through the US Air Force and PNNL.

Mitigation: Continued dialogue with CS&C and request USST engagement with U/S NPPD.

Other schedule risks are captured in the baseline risk register below.

### Operational Risks

The primary operational risks are identified in the baseline risk register below.

### 5.2.3.1 Risk Management Approach

This section describes the Cyber.gov approach to risk management. This section includes a definition of risk management as it applies to the Cyber.gov program and provides an overview of the risk management processes and procedures. It also describes the relationship of risk management to other program management functions.

### 5.2.3.2 Risk Management Program Objectives

Risk management shares many of the same activities as program management, including planning, staffing, directing and controlling. Risk management shares the same goal – ensuring that the program are delivered on time, within cost, and in compliance with the program’s performance goals. Therefore, risk management is most successfully implemented when it is integrated into the existing program management processes, rather than as a separate process. As such, the risk management program will strive for the following objectives:

* + - **Rigorous identification of risk**. The Cyber.gov PM will institute a thorough and repeatable process for regularly assessing the program’s conditions in order to capture newly introduced risks. This process will be an open process that encourages all stakeholders to participate, rather than relying solely on specific individuals within the Cyber.gov program.
    - **Timely decisions**. The focus of the risk management process will be on managing risks, not just identifying them. Risks and their associated data will be forwarded to management in a timely manner to facilitate the decision-making process. Prompt and timely decision making will focus on ensuring that risks are controlled before negative consequences occur.
    - **Effective planning and assignment of priorities.** The development of an appropriate mitigation plan will involve consideration of different mitigation strategies, the cost of managing a risk, and the best use of program resources
    - **Systematic tracking of progress.** The Cyber.gov program staff will ensure that the mitigation progress is tracked and regularly reported to upper management. Management will ensure that the planned mitigation achieves the desired result and, if not, be prepared to execute an alternative mitigation or invoke a contingency plan.
    - **Prudent escalation of countermeasures.** Contingency plans, like mitigation plans, must be developed within the guideline that the cost of managing a risk should be less than the projected impact of the risk. To ensure this, contingency plans will be developed before they are needed rather than as ad hoc actions.

### 5.2.3.3 Critical Success Factors

A number of factors are critical to the success of implementing a risk management program.

* + - **Commitment of an executive as the risk management sponsor.** The Director, Cyber Security Division (CSD) will act as the risk management executive leader providing the necessary level of leadership and ensuring that clear communication exists across the Cyber.gov Program. The CSD executive leadership will help to reinforce the importance of risk management to ensure that the implementation is effective and the results become visible.
    - **Development, articulation, and communication of a risk management strategy.** The Risk Management Plan communicates the overall risk management strategy. Work products, such as the processes and procedures (including the risk matrices), also support the communication of this strategy. As the risk management strategy evolves, it is necessary to inform the organization of any changes.
    - **Commitment to the risk management program by all levels of management.** All levels of management must be committed to the program because it requires a fundamental shift in organizational culture, especially in the areas of openness and communications. Managers and their staff must feel free to identify risks without fear of reprisals
    - **Implementation of a system that rewards desired behavior.** This success factor, which is central to any process improvement effort, underscores the importance of positively rewarding new behaviors, such as identifying risk
    - **Availability of appropriate resources.** Risk management should not be delegated to a special group; it should be integrated with program management. Therefore, it is crucial that the program directors integrate risk management with their other program management duties. Time must also be allocated for training and for implementing and executing risk management activities. Since this may necessitate an incremental increase in the staffing level (Government or contractor personnel), this factor will be considered appropriately in the program planning stages.
    - **Application of a consistent set of processes and tools.** A consistent set of processes and tools influence the quality and sharing of risk data across the program and the ability of different program segments to make decisions based on that shared data.

### Risk Management Processes and Procedures

### 5.2.4.1 Overview

The context diagram in Figure 13 documents the high-level risk management process that will be used for the Cyber.gov Program.

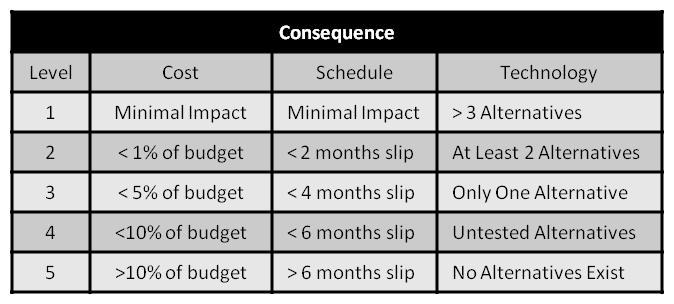


**Figure 13: Risk Management Process**

Each of the activities in Figure 13 provides input into the next activity. The enabling activity of communication facilitates these activities. The essential characteristics of this framework are promoting open communication, rewarding information sharing, performing proactive and continuous risk management, focusing on what’s most important to the program, and integrating these activities with other program management activities. These activities are performed continuously throughout the program life cycle.

### 5.2.5 Risk Register

The Cyber.gov program has established and will maintain a risk register as part of its overall risk management plan. The baseline risk register is included in this document.



**Figure 14: Risk Assessment Values Tables**

**5**

**4**

**3**

**2**

**1**

**1**

**2**

**3**

**4**

**5**

Likelihood

Consequence

Figure 15: Risk Score

| **Risk Number** | **Risk Name** | **Risk Description** | **Risk Category** | **Risk Score** | **Response Strategy** | **Action**  **Code** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | NPPD(CS&C) agreement on requirements and execution | CS&C, the program office for NCPS, does not concur with all of the research tasks being funded by CSD. | Operational, Schedule | 15 (L3; C5) | This would likely require discussions at the USST Griffin, U/S NPPD and U/S USM level. The following actions will be taken: 1) Provide additional information as requested for senior leadership discussions 2) Consider alternate research approaches such as addressing other findings and recommendations from the MIT-LL and BRP reports | Doug Maughan, Division Director |
| 2 | Research team gaining access to required data | Delays in processing research team for DHS suitability, especially for those team members performing the Classified Signature Utility study | Schedule | 9 (L3, C3) | Work closely with S&T security and PNNL/MIT-LL teams to ensure timely processing of suitability applications. Ensure MIT-LL and PNNL maximize use of researchers who already possess DHS suitability. | Cyber.gov SETA team |
| 3 | Tech demo interference with D/A operations | Demonstrations (measure infrastructure, technology, integration and Information Dissemination) interfere with daily operations | Technical, Schedule | 10 (L2, C5) | Cyber.gov team will need to ensure the D/As selected for technology demonstrations are able to support them in terms of staff and infrastructure resources. MIT-LL/PNNL will develop detailed demonstration requirements for each demo and scale them to the size of the participating agency. | Chase Garwood, Program Manager |
| 4 | Capability transition risk | Demonstrated technologies may not transition to the NCPS program of record if they do not meet the NCPS acquisition timeline and strategy and direction of Office Management and Budget | Operational | 9 (L3, C3) | Use a combination of top-to-bottom and bottom-to-top approaches in order to ensure proper adoption by OMB, NPPD (CS&C), CIOs and CISOs. | Chase Garwood, Program Manager |
| 5 | Adoption/Integration | Resistance to adoption may occur due to integration, environmental and other technical complexities | Operational, Schedule | 9 (L3; C3) | Utilize prototypes and testbeds to increase confidence and reduce installation and adoption risks. | Doug Maughan, Division Director |
| 6 | Changing Political Landscape | New or modified direction due to changing political landscape | Schedule | 8 (L4, C2) | Regular communication to ensure current efforts are beneficial to the potential paths forward | Doug Maughan, Division Director |
| 7 | Limited D/A Engagement | Limited D/A engagement impacts ability to perform system analysis and architecture design | Technical, Schedule | 15 (L3, C2) | Lean forward on initiating D/A engagements and carefully foster relationships | Chase Garwood, Program Manager |
| 8 | Classified Study | Inconsistencies in the data provided for Task A (Classified Study) may limit the reliability of the final report. | Technical | 8 (L4, C2) | Continue working with NPPD and the whole Task A team to clearly understand the data sets. | Chase Garwood, Program Manager |
| 9 | Community Feedback | Community feedback yields a very high number of responses to resolution | Technical, Schedule | 6 (L3; C2) | Provide resolution to responses in next version. Consider adding contractor personnel support for comment resolution. | Chase Garwood, Program Manager |
| 10 | D/A Responses | Lack of responses from D/As necessary to meet systems analysis and program needs | Technical,  Schedule | 6 (L3, C2) | Add more team members to aid in reach out phase to new D/As | Chase Garwood, Program Manager |
| 11 | State and Local Engagements | Unknown scope of state and local engagements could affect Cyber.gov | Operational, Schedule | 4 (L2; C2) | Define scope per effort in conjunction with FEMA and increase staffing | Doug Maughan, Division Director |

**Figure 16: Risk Register**

1. “DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System”, dated January 2016. <http://www.gao.gov/assets/680/674829.pdf> [↑](#footnote-ref-2)