

3.6 PROJECT MONITORING

Our team will use the Task Order Management Plan in conjunction with the WBS to monitor the progress of the project. All projects will adhere to our policies process definition, management, and compliance. As a result, our projects consistently perform according to industry standards and best practices. This results in consistent performance and a higher quality product that is on time and within budget.

The WBS is used to define the work to be performed and to provide a common basis of communication between our team and yours. Any changes are coordinated with and approved by the Contracting Officer before taking effect. Progress against the schedule is reported with monthly and weekly progress reports, and is kept up-to-date in electronic format accessible to our team and NEI. The project schedule can be maintained with Microsoft Project and can be presented in different formats, including Gantt chart format. We use the schedule to track planned dates versus actual dates and to forecast the effects of schedule changes. The schedule, when adjusted per the project orientation meeting to the satisfaction of both NEI and the NG team. It forms the baseline for performance measurement and establishes the period of performance for all resource estimates. Schedule changes are made according to a controlled process. Baseline changes are accommodated only for modifications to the contract or to incorporate detailed planning for activities for the next month. Changes introduced in the baseline schedule are made incrementally to ensure the impact of any baseline changes does not

3.6.1 REVIEW PROCESSES AND PROCEDURES

We recognize that clear, accurate communication is essential for the successful performance of the project. We are currently conducting the types of meetings listed below to support our existing projects. We track action items that result from reviews to closure using an action item tracking system.

3.6.2 METRICS AND MEASUREMENTS

We ensure that the project is managed by performance-based procedures. All work is planned, budgeted, and scheduled in time-phased “planned value” increments that constitute a cost and schedule measurement baseline. The Northrop Grumman team will gather metrics on cost and schedule and providing them graphically to allow “at a glance” status of a project. These metrics provide both NEI and our team with valuable information regarding the progress of the project. They also provide early warning signs if there are any developing problem areas. Using simple statistics—including Earned Value, Planned Value, and Actual Cost, This will provide you with an overall progress tasks and sub-tasks. This data also can also be used to do trend and variance analysis. This information, together with the textual monthly report and the risk report provide value-added information for managing the project.

3.7 DELIVERABLES

We will provide you with documentation throughout the project’s lifecycle. Documentation will include status reports, plans, C&A requirements, and additional documentation that will assist in keeping open communication and disaster recovery (Refer to Appendix C: Additional Deliverables for other documentation). These will be delivered to the NEI CIO and ISSO so they can be aware of requirements, risks, and status of project. Table 3-3 lists the deliverables and the dates they will be delivered.

| Deliverable | Due Date | Notes |
|-------------|----------|-------|
|-------------|----------|-------|

| | | |
|---|---|---|
| Task Order Management Plan | Upon Award + 5 days | Provide a documented framework for control of the project. |
| Work Breakdown Structure (WBS) | Upon Award + 5 days | Tracks the progress of the contract at the individual task level. |
| IT Security Policy & Procedures | Monthly | Will be developed as contract progresses. |
| Team Training Plan | 15 calendar days of the Start of Work, and then Annually. | Will detail the annual training plan for personnel assigned to the project. It will have a minimum of 2 training sessions and 1 conference. |
| Contract List/Invoice with CIO-SP2i CLIN | Upon Award | Standard invoice and listing of employees, their assigned CIO-SP2i CLIN, hourly rate of charge associated with CLIN & timesheets. |
| Outstanding Risk Report | Weekly | New and outstanding risks – delineate UNIX Wintel & Mac platforms. |
| Risk Tracking Report | Weekly | Specifies actions taken on identified risks - delineate UNIX Wintel & Mac platforms. |
| Security Tracking Summary | Weekly | Summarizes new, outstanding, and closed risks for the week. |
| Activity Report | Weekly | Summarizes the activities of the technical personnel performing each task. |
| Project Officer Quarterly report | Quarterly | Goal/Milestones/Anticipated achievements for next quarter |
| Performance Matrix | 30 days of Start of Work. | Based on the agreed upon goals and milestones mentioned in SOW. |
| Employee Leave Report | Monthly | List of schedule leave for upcoming quarter. |
| Contention and Proposal Solution Report | Varies | Areas where the Northrop Grumman team and NEI disagree on methodology/architecture/timelines/miscellaneous. |
| System Log Report | | |
| Tripwire Reports | | |
| IDS Reports | | |
| Firewall Reports | | |
| Backup Reports | | |
| Daily Security Checks | | |
| NIH Computer Security Awareness Training Log | As staff completes training. | Log of all staff under contract who have completed the NIH Computer Security Awareness Training Log. |
| Other daily/monthly/quarterly/yearly reports | | Refer to Appendix C: Additional Deliverables |

Table 3-3: Deliverables

1. TECHNICAL

4.1 TECHNICAL DESCRIPTION

Understanding your overall security requires that you examine all aspects of your network architecture, including its design, implementation, and processes. Our solution is divided in three phases (Please refer to subsequent sections for more detailed descriptions):

- Assessments of your current network infrastructure and processes
- Extensive testing of your workstations and network to check for vulnerabilities
- Implementation of the plan that we (NEI and QUICK BEAM) design

Our proposed solution will ensure that your IT Security program follows the defined HHS “Secure One” methodologies, policy, and procedures, NIST guidelines, NIH processes, the FISMA requirements, any and all existing federal government Information Systems guidance. We recommend the following solution to strengthen your current IT security program.

4.2 NETWORK SECURITY ASSESSMENTS

The Network Security Assessments will provide a comprehensive review of your network infrastructure, your processes, and security tools. Each component of your infrastructure will be isolated to identify the strengths and weaknesses of each separate one. Our assessments will also see if they follow current security policies and procedures. These assessments will include a review of the DHHS and NIH policies that NEI are subject to. They will also help form recommendations for additional NEI specific policies, as needed, to meet regulatory requirements, as well as insure the protection of NEI's network and information assets. The components we will review are listed below. Detailed descriptions are in subsequent sections.

- Network Architecture
- Vulnerability Assessment and Tracking
- NEI Firewalls
- NEI Intrusion Detection Systems
- Computer Security Incident Response Capability (CSIRC)
- Policies and Procedures
- Security Awareness Testing
- Disaster Recovery

4.2.1 NETWORK ARCHITECTURE

The network architecture assessment will consist of reviewing hardware, software, security tools, and firewall of your current network infrastructure. Additionally, internet connections and third-party software will also be included in this component to be analyzed.

4.2.2 VULNERABILITY ASSESSMENT AND TRACKING

Our team will evaluate your current vulnerability assessment and tracking program. We will focus on its ability to run internal and external scans, the time it takes for vulnerability identification and reconciliation, and the management and reporting tools within the program.

4.2.3 NEI FIREWALLS

Firewalls are essential for any security program. They prevent the passage of undesirable network traffic from one side to another. We will review if your current firewall has the proper configuration, the documentation in place, and how well it is protecting your network infrastructure.

4.2.4 NEI INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems are used to detect all types of malicious network traffic and computer usage not detected by a conventional firewall, including network attacks against vulnerable services, data driven attacks on applications, and host-based attacks, such as privilege escalation, unauthorized logins, malware (e.g. viruses, Trojan horses, and worms). We will evaluate your current detection systems, how they work with your firewall, its current configuration, and its reporting tools.

4.2.5 COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)

We will assess your current incident response procedures to assist us in developing a CSIRC team, documentation, and policies to strengthen your network architecture. Additionally, we will meet with the NIH Incident Response Team (IRT) to ensure that our solution will quickly transition with theirs.

4.2.6 POLICIES AND PROCEDURES

Our team will review your current policies and procedures. This will include your Business Continuity/Continuity of Operations Plan (BC/COOP), C&A requirements, and any other network documentation that you have developed in the previous years.

4.2.7 SECURITY AWARENESS TESTING

We will evaluate the current security awareness testing, which includes the Remote Access users module, for clarity and comprehension. Additionally, our assessment will see what training modules are missing to incorporate new technologies.

4.2.8 DISASTER RECOVERY

Our assessment will check your current backup processes, guidelines of any potential loss of data, and the time it would take to recover from a potential disaster.

4.2.9 UPDATED NETWORK SECURITY ASSESSMENTS

We recommend performing an Updated Network Security Assessments every 12 months. The constant changing of technologies, network infrastructure, and operational practices and affect your network security. We plan evaluate the status of all issues identified in the previous Network Security Assessment, any new security implication on your network infrastructure, and any other specific issues you would like us to assess.

4.3 TESTING

After analyzing the assessments of components described in Section 4.2, we will begin extensive testing to check for your network's strengths and weaknesses against external and internal attacks. This will be performed with four tests: Technical Vulnerability Attack, Social Engineering Assessment, Periodic External Penetration Testing, and Internal Penetration Testing. They will be describing in detail in the following subsections.

4.3.1. TECHNICAL VULNERABILITY ATTACK

We will emulate the tools and techniques used by unauthorized users attempting to attack your systems from the Internet. We check the vulnerabilities of your Internet-connected systems by utilizing a variety of techniques and attacks. "Hacker" programs and tools will be utilized to try to infiltrate your system.

4.3.2 SOCIAL ENGINEERING ASSESSMENT

Our team will try to solicit sensitive information from your users by telephone and email. This will show us what needs to be updated in the security awareness testing, so that your users are better educated on what information should not be given to outside parties.

4.3.3 PERIODIC EXTERNAL PENETRATION TESTING

We will closely monitor new vulnerabilities and threats related to Internet-connected systems. Our assessment will test the available tools and techniques that you are currently using to see if they need to be updated.

4.3.4 INTERNAL PENETRATION TESTING

This test will emulate the activities of an unauthorized user with physical access to the network environment. The purpose is to check your current security system's ability to protect against internal attacks.

4.3.5 UPDATED TESTING

We recommend that periodic and unexpected testing occur. New vulnerabilities and constant attacks happen with no warning. Therefore, we have to ensure that your system is secure enough to be able to handle these kinds of unexpected interruptions.