

## 6.3 Security Services (Schedule 3.3 – Appendix 3)

*Instructions to Vendors:* Unless specifically noted in the appropriate tables below, Vendor agrees to perform, for the environment (described in Schedule 3.3 – Appendix 3, Section 2), the services and associated roles and responsibilities (as outlined within Schedule 3.3 – Appendix 3, Section 3 Security Services Requirements), at the defined service levels (as outlined within Schedule 3.3 – Appendix 3, Section 4). Section 3 is not considered to be all-inclusive. Vendor will be responsible for the complete life-cycle management of these services, unless otherwise noted. Vendor shall clearly indicate in the tables below if it does not accept the requirements defined in Schedule 3.3 – Appendix 3 Commonwealth considers the Vendor to agree to all Schedule 3.3 – Appendix 3 unless identified herein. Vendor should add rows to the tables below as necessary. Absence of issues will constitute agreement for those items not herein addressed, and will be off the table for further negotiation.

### 6.3.1 Security Services Solution Overview

*Instructions to Vendors:* Provide an overview of the Security Services solution you propose to address the Commonwealth Requirements stated in Schedule 3.3 – Appendix 3. This overview should **not be more than two-pages** long. Additional details should be provided in Section 11 of this Vendor Proposal document.

### *The Commonwealth Partners' Vision for the Commonwealth*

Security is a critical component in any enterprise today and the Commonwealth Partners are proud to offer the Commonwealth a security solution that leverages the Commonwealth Partners' broad portfolio of security services and includes an Enterprise Security Operations Center (eSOC), giving the Commonwealth the ability to leverage the knowledge of IBM's 3,000 global security practitioners. This solution provides security services that are both reliable and cost effective. Further, IBM is excited about providing a career development path for Information Security practitioners in the Commonwealth of Virginia.

Our security vision for the Commonwealth has a number of goals. First, our security services will provide a comprehensive solution for Security policies, standards, procedures, and access controls. The eSOC will take a leadership role in working with the Commonwealth for the creation and approval of the Security Controls Policy Document (GSD331), as well as continuously measuring and reporting the level of compliance to security policy across the IT environment. Processes and procedures are some of the most effective tools for internal network security. Verifying that End-Users use complex passwords, user accounts are audited, and failed logon attempts are monitored, will allow us to proactively manage and protect access within the network. End-Users will not be allowed to access any information that they are not approved to access. By continuously updating and measuring against the Security Controls Policy Document, the eSOC will provide an improved security audit posture across the agencies.

Second, this solution will assist in reducing the number of security incidents. This will be done by leveraging three areas of IBM expertise: Prevention, Detection, and Response. Prevention will be achieved with IBM's Anti-virus management services, including virus response and virus alerting, and IBM's Security Intelligence Services (ISIS). As potential security threats transform into widespread security attacks, the Commonwealth will take advantage of IBM's state-of-the-art early warning system (ISIS) so that proactive measures can be taken to mitigate the impact. Detection and Response will be achieved with intrusion detection and prevention solutions, designed to detect attacks on the Commonwealth's network and critical servers by providing fully redundant, fully scalable 24x7x365 monitoring of intrusion detection and prevention devices. The combination of prevention, detection, and response allows the eSOC to provide the Commonwealth with a reduction in both the number and impact of security incidents.

Third, the eSOC will provide vulnerability scanning, vulnerability assessments, and risk assessments in order to improve the Commonwealth's security posture. This will provide visibility into vulnerabilities across the Commonwealth, which the eSOC can then use in order to determine the most cost effective way to reduce security risk across the IT environment.

Fourth, the eSOC will assist with verification of the overall security of the Commonwealth's IT infrastructure. The eSOC will provide security awareness and security training in order to verify that individuals understand the importance and severity of security. The eSOC will also provide analysis of security technologies and will assist with security architecture reviews and security configuration decisions. Finally, logical security and physical security are included as vital components for verifying end-to-end security.

Our security solution provides the Commonwealth with a robust security program. One of the primary benefits of this solution is the tight integration between the Commonwealth's eSOC and IBM's Security Operations Center (SOC) in Boulder, Colorado. While a large majority of the work will be conducted by the Commonwealth's eSOC, the IBM SOC will provide the 24x7x365 security monitoring. This provides the following three benefits to the Commonwealth:

1. IBM is able to leverage its global perspective of monitoring over 1,000 NIDS and HIDS in over thirty countries to notify the eSOC of attacks before they reach the Commonwealth's network.
2. This approach alleviates the eSOC of having to bear the enormous costs of two redundant Security Event Management infrastructures and associated monitoring facilities and personnel costs.
3. Instead of the eSOC being staffed with level one and level two security analysts, the eSOC will be staffed with Information Security Advisor(s), Security Intelligence Analyst(s) and Vulnerability Assessment Analyst(s), providing a much more robust set of security skills to the Commonwealth.

While alternate solutions were discussed, such as a dedicated SOC for 24x7x365 monitoring, it was determined to be cost prohibitive and did not provide the comprehensive level of security achieved with the current solution.

### ***Solution Description***

In this section, not all of the solution components are discussed in detail. Instead, the major solution components are described. Please see **6.3.6 Vendor Additional Comments relative to service provisioning for Schedule 3.3 – Appendix 3** at the end of this document for a more detailed description of the solution components.

Intrusion detection services (IDS) and intrusion prevention services (IPS) provide monitoring of the Commonwealth's network using a combination of hardware and software called an intrusion detection/prevention sensor. If an attack pattern is detected, the sensor sends an event notification to the IBM SOC, which is staffed 24 hours a day, 365 days a year. SOC personnel evaluate the event and, if necessary, contact the eSOC. The eSOC then uses its process and procedures for analyzing and responding to the event.

IBM will provide the Commonwealth with a Security Portal for accessing reports. This Security Portal is accessible via a Web browser and requires a user ID and password. Attacks are tracked, reported, and trended on IBM's Security Portal in a number of different manners. An 'Executive Summary' report is produced, along with tracking attacks in a number of various charts and tables.

Vulnerability scanning services consist of testing a target system, based on the Commonwealth's Security Policy for known vulnerabilities and configuration weaknesses, and then reporting on problems found. Vulnerability scanning is optimized to create minimal impact on well-configured systems. The scanning report will be configured (filtered) according to the security controls for the Commonwealth and will only flag problems that are in violation of the security controls. The basic report will also include a risk assessment with aging, and a reference describing the problem. The output from the vulnerability scans is

reviewed by the eSOC to verify that the test ran successfully. A summary report will be created and provided to the appropriate individuals for the appropriate and corrective action to be taken.

Vulnerability Assessment services consist of scanning a target system or network device for security vulnerabilities, and attacking these vulnerabilities in an effort to gain unauthorized access. The purpose of the service is to identify specific security weaknesses on the target systems, and to recommend techniques or improvements to strengthen the security of the target system. This service is provided for all platforms (UNIX, Linux, Windows, etc.).

### ***Benefits/ Future State***

This security solution provides three benefits to the Commonwealth that can only be provided by IBM:

1. The Commonwealth will be able to leverage IBM's two Security Research Labs and 3000 global security practitioners because the eSOC will have access to all whitepapers, newsgroups, security events, and other sources of information and can participate in the security community within the IBM Company.
2. IBM leverages its Business Intelligence in Information Security to give data analytics and data mining that are unparalleled in the industry. The data mining and data visualization that are provided by the eSOC will give the Commonwealth insight into low-and-slow attacks, and other subtle trends that cannot be detected in 24x7x365 monitoring and are not provided by other service providers.
3. IBM has a large portfolio of security services that the Commonwealth can take advantage of within the enterprise. Services additional to those provided in our solution can be brought to bear on the Commonwealth's network through discussions over the life of the contract..

### **6.3.2 Security Service Environment Acceptance and Exceptions**

Vendor shall reference and provide detailed accepted and/or proposed service environment components as attachments to the proposal where required and as indicated in Schedule 3.3 – Appendix 3, Section 2.

- Check - Vendor agrees with Schedule 3.3 – Appendix 3, Section 2, except for the elements listed in the table below.

**Table 24. Security Service Environment Issues**

**Redacted**

### **6.3.3 Security Services Requirements Acceptance and Exceptions**

- Check - Vendor agrees with Schedule 3.3 – Appendix 3, Section 3, except for the elements listed in the table below.

**Table 25. Security Services Requirements Issues**

**RedactedRedacted**

### **6.3.4 Security Management Acceptance and Exceptions**

- Check - Vendor agrees with Schedule 3.3 – Appendix 3, Section 4, except for the elements listed in the table below.

**Table 26. Security Management Issues**

**Redacted**

### **6.3.5 Security Management Tools**

Describe the automated tools used in the delivery of this service in the table below.

**Table 27. Security Management Tools**

**Redacted**

### **6.3.6 Vendor Additional Comments relative to service provisioning for Schedule 3.3 – Appendix 3**

Please refer to Section 11.3.4 Details on the Security Services Solution that includes:

1. Enterprise Security Operations Center
2. Intrusion Detection and Prevention Solution
3. Vulnerability Management Solution