The SPARK Institute, Inc.
SHAPING AMERICA'S RETIREMENT

GUIDELINES FOR COMMUNICATING PENETRATION TESTING RESULTS

Developed by SPARK's Data Security Oversight Board

Release 1.0

April 2020

The Spark Institute, through the work of its Data Security Oversight Board, developed the following guidelines to assist record keepers in properly communicating with clients and consultants about their Penetration Testing. These guidelines are not intended to provide recommendations on how penetration tests are conducted or guarantee against a data breach or loss.

Penetration tests are used to highlight vulnerabilities in a system and expose areas of a potential weakness. For this reason, record keepers must maintain a level of secrecy and privacy about these test results to continue to secure client data and assets. Conversely, the industry recognizes a client's need to know that the vendors they rely upon to protect their employees' benefits are secure and well protected.

The intent of these guidelines is to establish a base of communication between record keepers and their clients for how best to use penetration tests for those shared goals. By using these guidelines, clients and consultants can properly validate a vendor's cyber security program while still maintaining the necessary level of confidentiality.

Industry Guidelines for Public Use of Penetration Testing & Reporting

1. SPARK members consider the release of penetration test results to any external parties valid only in rare and exceptional situations. It is a reasonable expectation that detailed results will be shared internally and with the record keepers own auditing partners. Careless distribution of penetration test results carries with it significant risk. The release of penetration test results to outsiders is a dangerous practice that can expose the vendor, clients and participants hosted on that platform to breaches (see SPARK Data Breach definition).

2. Industry members can communicate certain information about their penetration testing to clients and consultants that can be valuable when evaluating a vendor's cyber security. The recommend method to share that information is through the record keeper's representation of adherence to the SPARK data security best practices.

3. Penetration testing is defined by NIST[1] as "security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network".

4. Types of penetration testing includes; systems, application, infrastructure, network, cloud, other.

5. Penetration testing should be inclusive of anywhere customer- or plan-provided Non-Public Information (NPI) or Personally Identifiable Information (PII) is processed or stored.

6. When reporting information about penetration testing, SPARK's guidelines recommend members to communicate the following details:

SPARK Penetration Test Guidelines

Information	Purpose
Penetration Test Performed	What types of penetration tests were performed (application, network, cloud, other)?
Frequency of Tests	This lets the client know that penetration tests are a regular part of a vendor's cyber security practices

[1] NIST SP800-115 [nvlpubs.nist.gov] (Tech Guide to Security Testing) -Penetration testing is security testing in which evaluators mimic real-world attacks with the intent to identify ways to circumvent the security features of an application, system, or network

Information	Purpose
Entity that performed the penetration test	Clients and consultants need to know who is responsible for the penetration testing to validate their expertise
Criticality level of findings	Do you follow CVSS, OCOAS, or other industry standard scoring? If no, please explain. Did your testing identify any material vulnerabilities (critical or high)?
Remediation	Were any findings remediated within your P&P timeframes? What are your remediation timeframes?

7. At a minimum SPARK recommends sharing the type of testing conducted, date(s), who performed testing and an acknowledgement that any critical or high findings were remediated or will be remediated by a certain date:
   - A _____ (application; network, cloud, other) penetration test was conducted on ____, by ___ and any material (commonly understood as critical and high) findings were remediated or will be remediated by ______.