



Federal Deposit Insurance Corporation

550 17th Street NW, Washington, D.C. 20429-9990

Division of Risk Management Supervision

October 18, 2016

R. Kinney Williams
President
Yennik, Inc.
4409 101st Street
Lubbock, Texas 79424

Dear Mr. Williams:

Thank you for your letter dated September 16, 2016, requesting clarification of guidelines governing any requirement that a financial institution periodically utilize different firms to conduct penetration testing. In your letter, you state that Federal Deposit Insurance Corporation (FDIC) examiners requested that some of your client banks change to a new firm for penetration testing as these banks have been using your firm's services for a number of years. Chairman Gruenberg asked that I respond on his behalf.

The FDIC does not require financial institutions we supervise to change penetration testing firms on a periodic basis. Any such decision would be up to bank management. Relevant examiner guidance is contained in the Federal Financial Institutions Examination Council Information Technology Examination Handbook on Information Security (Handbook) that discusses penetration testing in the context of information security risk management. This Handbook was updated last month. As outlined in the Handbook, financial institution management is expected to review the qualifications of testing personnel to verify their capabilities are adequate to support the penetration testing objectives. During Information Technology examinations, FDIC examiners will determine whether a financial institution's penetration testing firm is using the most up-to-date tools, scanners, and techniques. The changing of penetration testing vendors is not discussed in the Handbook.

Thank you again for contacting the FDIC. If you have additional questions regarding this matter, please contact Mr. Donald Saxinger, Chief, Information Technology Supervision. Mr. Saxinger can be reached at (703) 254-0214.

Sincerely,

Doreen R. Eberley
Director