Francis L. Mayer, CISSP Comment on Proposed rule s7-04-22 'Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies'

Recommended Changes: Page 26, paragraph 1.c. Information Protection, line 19 from top of page,

CHANGE “The program could also include independent testing of systems, including penetration tests.

" TO READ “The program will also include independent testing of systems, including penetration tests, and all issues uncovered will be managed to reduce the risk to a low level. Testers will not be in the reporting chain of managers that have a conflict of interest because they also manage the organization that maintains or develops the system or application under test. Test reports will be provided to the most senior executive managers of the company that are above any manager of the company or outside contractors that maintains or develops the system or application under test."

JUSTIFICATION: Penetration and other tests must be made independent, practical, and mandatory because if testing is not mandatory and independent it then it is worthless. Without rigorous testing the entire program is worthless as it becomes a paper drill that wastes time and money while producing little value in terms of real security. I served in government and industry for many years in the field that evolved into cybersecurity. I have seen security breaches firsthand and in every case a lack of true independent penetration testing with mandatory fixes of issues uncovered resulted in extremely high risk of exploitation and compromise. GAO reports going back decades, such as https://www.govinfo.gov/content/pkg/GAOREPORTS-T-AIMD-98-170/pdf/GAOREPORTS-T-AIMD-98-170.pdf, point to the need for penetration testing and action on the results.