



Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-18-A-14

June 6, 2018

Results in Brief

Why We Did This Review

The Federal Information Security Modernization Act of 2014 (FISMA) outlines the information security management requirements for Federal agencies, which includes an annual independent evaluation of the agency's information security program and practices to determine their effectiveness.

FISMA requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent auditor. The Nuclear Regulatory Commission (NRC) OIG retained Richard S. Carson & Associates, Inc., to perform the fiscal year 2017 FISMA evaluation, including conducting an external vulnerability assessment and penetration test.

The objective of the testing was to verify the presence of network devices, identify vulnerabilities, determine risk, and aid management in countering or mitigating associated risks.

U.S. Nuclear Regulatory Commission Office of the Inspector General External Vulnerability Assessment and Penetration Test (OIG-18-A-14)

What We Found and Recommend

OIG conducted a vulnerability assessment and penetration testing of external Internet systems on the NRC computer network. The testing was conducted from Carson, Inc. Penetration Testing Lab in Bethesda, Maryland and the Washington, DC, metro area. As a result of the assessment and testing, OIG made one recommendation to the Executive Director for Operations that will improve NRC's information security program.