



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 CliftonLarsonAllen, LLP (CLA), to perform the fiscal year 2023 FISMA audit, including conducting an vulnerability assessment and external penetration test.

The audit objective was to assess the NRC's technical configuration and security controls by performing coordinated network and host-based security tests supporting the NRC's FY 2023 FISMA audit.

U.S. Nuclear Regulatory Commission's Vulnerability Assessment and External Penetration Test (OIG-23-A-11)

OIG-23-A-11

September 29, 2023

What We Found

The OIG contracted with CliftonLarsonAllen, LLP (CLA) to conduct a vulnerability assessment and an external penetration test of the U.S. Nuclear Regulatory Commission's (NRC) information system environment in support of the NRC's fiscal year (FY) 2023 Federal Information Security Modernization Act of 2014 (FISMA) audit. During the vulnerability assessment and external penetration test, CLA identified weaknesses that, if remediated, would help strengthen the NRC's security posture.

What We Recommend

As a result of the assessment and testing, two recommendations were made to assist the NRC in continuing to strengthen the vulnerability management program.