EVALUATION REPORT

REDACTED VERSION

Office of the Inspector General Information
System Security Evaluation of Region I-
King of Prussia, PA

OIG-09-A-20 September 30, 2009

Office of the Inspector General
Information System Security Evaluation of
Region I – King of Prussia, PA

Contract Number: GS-00F-0001N
Delivery Order Number: 20291

September 30, 2009

EXECUTIVE SUMMARY

BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) has four regional offices that conduct inspection, enforcement, investigation, licensing, and emergency response programs for nuclear reactors, fuel facilities, and materials licensees. The Region I office operates under the direction of a Regional Administrator and is located in King of Prussia, Pennsylvania. The region covers an 11-state area and the District of Columbia, including 8 states with nuclear power plants. Region I also oversees materials licensees in Region II.

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. FISMA also requires assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines. FISMA requires the annual evaluation to be performed by the agency's Inspector General or by an independent external auditor.

The NRC Office of the Inspector General (OIG) requested that the four NRC regional offices and the Technical Training Center (TTC) be included in the independent evaluation of the agency's implementation of FISMA for fiscal year 2009. Information security policies, procedures, and practices at the regional offices and the TTC were last assessed in 2003 and 2006. This report describes evaluation findings for Region I.

PURPOSE

The objectives of the information system security evaluation of Region I were to:

- Evaluate the adequacy of NRC's information security program and practices for NRC automated information systems as implemented at Region I.
- Evaluate the effectiveness of agency information security control techniques as implemented at Region I.
- Evaluate corrective actions planned and taken as a result of previous OIG evaluations.

[1] For the purposes of FISMA, the agency uses the term "information system security program."

RESULTS IN BRIEF

Region I has made improvements in its implementation of NRC's information system security program and practices for NRC automated information systems since the previous evaluations in 2003 and 2006. All corrective actions from the previous evaluations have been implemented. However, the information system security program and practices are not always consistent with the NRC's automated information systems security program as defined in Management Directive (MD) and Handbook 12.5, *NRC Automated Information Systems Security Program*, other NRC policies, FISMA, and National Institute of Standards and Technology (NIST) guidance. While many of the Region I automated and manual security controls are generally effective, some security controls need improvement. Areas needing improvement included continuity of operations and emergency planning, and configuration management. Specifics cannot be presented in this publicly released version of the report.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's information system security program and implementation of FISMA at Region I.