
OIG Highlights

Objective

The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to undergo an annual independent evaluation of its information security program and practices. The OIG contracted with Kearney to conduct the fiscal year (FY) 2014 FISMA evaluation of the Corporation. The objectives were to evaluate a representative subset of the Corporation's information systems for compliance with FISMA, OMB and NIST guidance and to evaluate the operating effectiveness of the information security and privacy controls over those systems.

Recommendations

Resolving serious security and privacy weaknesses throughout the Corporation's information security program will require a disciplined and sustained effort, as well as commitment of substantial resources. The OIG recommends that the Corporation take four key steps: (1) Establish an information technology project to prioritize and remedy the weaknesses, led by a Project Manager; (2) Develop a Project Plan, with specific milestones and assignments of responsibility; (3) Identify and marshal the resources, skills and expertise necessary to implement the plan; and (4) Establish performance metrics for information security. Oversight and support from agency leadership is crucial to that effort.

November 2014

Information Security and Privacy Program at the Corporation for National and Community Service Requires Great Improvement



What the OIG Found

The information security and privacy program at the Corporation for National and Community Service (Corporation) does not meet minimum standards and needs substantial improvement across the board. Kearney & Company, P.C. (Kearney), under the Office of the Inspector General's (OIG) supervision, uncovered weaknesses in 11 of the 12 areas tested. The controls were found to be ineffective in seven of these areas, and in four of them—Continuous Monitoring, Risk Management, Plans of Action & Milestones and Privacy—the defects were severe enough to constitute a significant deficiency, requiring immediate correction and attention by agency leadership. Five of these findings were recurring from last year. A review of the Department of Homeland Security's 115 security metric questions, divided into 11 subjects, identified 49 instances of non-compliance with applicable laws, regulations and authoritative guidance governing information security. Kearney also found significant weaknesses in Corporation's privacy controls for protection of Personally Identifiable Information (PII). Notably, Kearney concluded that the Corporation did not exercise meaningful oversight of the security measures by the contractors to whom it outsources its critical IT functions.

FY 2014 FISMA Evaluation Results

2014 DHS IG FISMA Reporting Area and Privacy	# of DHS Exceptions / Total DHS IG Questions	Severity of Noted Exceptions
1. Continuous Monitoring Management	8 of 8	Significant Deficiency
2. Configuration Management	7 of 13	Control Deficiency
3. Identity and Access Management	1 of 12	Control Deficiency
4. Incident Response and Reporting	2 of 9	Control Deficiency
5. Risk Management	10 of 17	Significant Deficiency
6. Security Training	2 of 7	Control Deficiency
7. POA&Ms	6 of 9	Significant Deficiency
8. Remote Access Management	1 of 13	Control Deficiency
9. Contingency Planning	8 of 13	Control Deficiency
10. Contractor Systems	4 of 8	Control Deficiency
11. Security Capital Planning	0 of 6	N/A
12. Privacy	N/A	Significant Deficiency

The Corporation took steps to correct certain of the deficiencies and has promised a plan for addressing others. However, throughout the evaluation field work, the Corporation maintained that its security program met all applicable standards, disagreed with Kearney's assessment of the severity of noted weaknesses, and questioned the value of adopting and documenting comprehensive policies and procedures for information security.