

November 2015

Weaknesses Identified in the Corporation's Information Security and Privacy Program

Office of Inspector General



OIG Highlights

Objective

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 FY 2015 FISMA evaluation of the Corporation. The objectives were to evaluate a representative subset of the Corporation's information systems for compliance with FISMA, Office of Management and Budget (OMB), and National Institute of Standards and Technology (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 and privacy program will require a disciplined and sustained effort, as well as a commitment of substantial resources.

The Corporation has begun, but not yet implemented, the four key prior year recommendations. The OIG recommends that the Corporation take four key steps:

- (1) Establish an IT project to prioritize and remedy the weaknesses, led by the CISO
- (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 Project Plan
- (4) Establish performance metrics for information security oversight and obtain support from agency leadership.

What the OIG Found

The Corporation for National and Community Service (the Corporation) has taken a number of meaningful steps to address information security and privacy weaknesses from the fiscal year (FY) 2014 Federal Information Security Management Act of 2002 (FISMA) evaluation: resolving three out of sixteen findings from the FY 2014 evaluation and hiring a Chief Information Security Officer (CISO) and Security Analyst in June 2015 to support the development of the Corporation's Information Security Program. Additionally, the Corporation established a Memorandum of Agreement (MOA) in November 2014 with the Department of Homeland Security (DHS) to participate in DHS's Continuous Diagnostics and Mitigation (CDM) Program.

Despite these preliminary steps, progress towards resolving fundamental weaknesses within the Corporation's Information Security Program has been limited, and serious vulnerabilities remain. Kearney & Company, P.C. (Kearney), under the Office of Inspector General's (OIG) supervision, identified new or continuing weaknesses in all 11 areas tested. The controls were found to be ineffective in eight of these areas, and, in two of them (i.e., Continuous Monitoring Management and Risk Management), the defects were severe enough to constitute a significant deficiency, warranting immediate corrective action and attention by agency leadership. Eight of these findings were reoccurring from the FY 2014 evaluation. Kearney also uncovered four new weaknesses: (1) information technology (IT) procurement; (2) access controls; (3) strategic planning, and (4) inventory management. Responses to DHS's 100 security metric questions identified 54 instances of noncompliance with applicable laws, regulations, and authoritative guidance governing information security. Kearney also found significant weaknesses in the Corporation's privacy controls for protection of Personally Identifiable Information (PII).

FY 2015 FISMA Evaluation Results

2015 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 ¹	Significant Deficiency
2. Configuration Management	9 of 12	Control Deficiency
3. Identity and Access Management	1 of 9	Control Deficiency
4. Incident Response and Reporting	2 of 8	Control Deficiency
5. Risk Management	9 of 16	Significant Deficiency
6. Security Training	3 of 7	Control Deficiency
7. POA&Ms	6 of 9	Control Deficiency
8. Remote Access Management	3 of 12	Control Deficiency
9. Contingency Planning	10 of 12	Control Deficiency
10. Contractor Systems	3 of 7	Control Deficiency
†Privacy	N/A	Control Deficiency

† – Consistent with the addition of privacy controls to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, the OIG contracted with Kearney to evaluate the Corporation's implementation of specific privacy controls as part of the FY 2015 FISMA evaluation.

¹ – To enable comparison of this year's results with those of FY 2014, Kearney analyzed this year's Continuous Monitoring Management using the same eight Continuous Monitoring Management questions applicable in FY 2014. However, a new standard for assessing Continuous Monitoring Management, using a maturity model, went into effect on June 19, 2015, and Kearney assessed the Corporation's Continuous Monitoring Management under that standard. The maturity model yields the Corporation a score of "1 – Ad Hoc" in each of the three areas (People, Process, and Technology) evaluated.

In response to the OIG's FISMA report, the Corporation agreed to devote the resources and management attention to resolve the noted weakness and strengthen its Information Security Program. OIG looks forward to working with management to address these weaknesses.