LIMITED DISTRIBUTION

Effectiveness of the Social Security Administration’s Server Patch Management Process A-14-14-14043

SOCIAL SECURITY ADMINISTRATION
OIG

September 2014 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration’s (SSA) server patch management program effectively addressed known system vulnerabilities.

Background

The National Institute of Standards and Technology recommends that security issues be patched timely to maintain the operational availability, confidentiality, and integrity of information technology systems. Additionally, the Government Accountability Office’s *Federal Information System Control Audit Manual* requires that an effective patch management process be documented and implemented. SSA’s policies and procedures also require timely patching of systems.

To test the security of SSA’s systems, the independent public accounting firm we contracted with to audit SSA’s Fiscal Year 2013 financial statements performed systems penetration tests. The firm identified weaknesses with the Agency’s patch management process, which contributed to the firm’s determination that SSA had a significant deficiency in its systems environment.

Our Findings

SSA did not have a comprehensive server patch management program. Consequently, the Agency did not always address known vulnerabilities timely. Specifically, we found that the Agency did not always:

- patch Windows servers according to its patch management policies;
- have effective policies and procedures to ensure UNIX servers were patched timely; or
- address software vulnerabilities on the Windows servers.

Without an effective patch management process in place, systems are at risk of unauthorized access.

Our Recommendation

We recommend that SSA develop and implement a comprehensive server patch management program to ensure all vulnerabilities are identified and patched timely.

The Agency agreed with our recommendation.