# Mobile Device Security
# A-14-14-14051

SOCIAL SECURITY ADMINISTRATION
OIG

**September 2014** **Office of Audit Report Summary**

## Objective

To determine whether the Social Security Administration's (SSA) mobile device security conformed with Federal standards and business best practices to mitigate unauthorized access to the Agency's sensitive information.

## Background

While mobile devices allow employees to work from various locations, their mobility makes them susceptible to loss and theft. Recent data indicate that mobile devices are under increasing attack by cyber-criminals exposing them to such risks as theft and introduction of malicious software, potentially disclosing sensitive information.

Given these vulnerabilities, the National Institute of Standards and Technology recommends agencies fully secure each mobile device before allowing a user to access it. Further, organizations should have a mobile device security policy to define what information employees can access with these devices.

## Our Findings

We determined that SSA's security of mobile devices did not always conform with Federal standards and business best practices to mitigate unauthorized access to Agency sensitive information. Specifically, we found the Agency lacked a comprehensive, consolidated mobile device policy, did not secure all mobile devices, and provided minimal mobile device security training.

## Our Recommendations

We recommend the Agency:

1. Develop a comprehensive, consolidated mobile device policy.
2. Develop and apply standard security configurations for all Agency-issued mobile devices.
3. Enhance annual information technology security awareness training to remind individuals who use mobile devices of their responsibilities, acceptable behavior, and specific risks when using Agency-issued mobile devices.

The Agency agreed with our recommendations.