The Department of Justice Office of the Inspector General (OIG) today released a report on the Executive Office for United States Attorneys' (EOUSA) encryption program and practices for laptop computers and electronic tablets. The OIG audit identified several weaknesses in EOUSA's efforts to safeguard sensitive and classified Department data on these devices.

Specifically, our findings included the following:

- Six of the 120 EOUSA-owned laptops used for unclassified processing that we tested were not encrypted and we could not determine the encryption status for three others. The six unencrypted laptops were used for special purposes, such as jury use or use by visiting EOUSA employees, but they were not labeled to identify those special purposes, nor were there policies in place that explicitly limited their use to such purposes.

- In our review of EOUSA's encryption monitoring scans, there were 8 laptops that were identified as unencrypted and remained so for over a year after having been first identified as needing encryption.

- EOUSA's official equipment inventory was incomplete, contained inaccurate data entries, and was subject to delays in updating information, such as the entry and removal of inventory items. We further determined that EOUSA did not sufficiently track and monitor laptops used for classified processing, causing an increased risk of classified information loss.

- EOUSA did not fully comply with the Department's requirements for using electronic tablets under a waiver from otherwise applicable encryption requirements as part of a pilot program, and it did not adequately monitor or put in place policies sufficient to minimize security risks from the use of such tablets.

- EOUSA had allowed contractors to process Department data on unencrypted equipment after the Department's encryption requirement waiver, allowing this practice, had expired in 2011. Finally, we found that the oversight of these contractors was inconsistent among the USAOs, and that the use of Department data in general was not sufficiently monitored by the USAOs we visited during our review, thereby increasing the risk of data loss.

The OIG made 13 recommendations to assist EOUSA in improving safeguards of Department data on laptops and electronic tablets, and in improving its management oversight to ensure compliance with Department policies. We have closed 1 of these recommendations, and EOUSA agreed with the remaining 12.