U.S. Environmental Protection Agency
Office of Inspector General

11-P-0277
June 23, 2011

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We reviewed prior audit work to highlight unimplemented actions the U.S. Environmental Protection Agency (EPA) should take to protect network resources from the increase of Advanced Persistent Threats (APTs) within the Agency.

Background

An APT is a cybercrime designed to steal or modify information without detection. These attacks are targeted at organizations, businesses, and political entities, and the perpetrators are usually organized and well funded. APTs are typically tailored, using multiple attack methodologies and tools, for specific targets. After an attack on the specific target has been successful, the threat maintains a foothold on the target for future exploitation.

For further information, contact our Office of Congressional, Public Affairs and Management at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2011/20110623-11-P-0277.pdf

EPA Has Taken Steps to Address Cyber Threats but Key Actions Remain Incomplete

What We Found

News publications have reported that APTs are increasingly prevalent throughout the federal government. In November 2009, the Agency reported 14 compromised systems that were associated with an Office of Inspector General investigation of APTs. By September 2010, the Agency reported that over 7,800 of its systems had communicated with known hostile Internet protocol addresses. These Agency systems potentially could have been compromised by APTs due to these communications. The National Institute of Standards and Technology reports that organizations must enhance risk management and information security governance to guard against APTs.

We issued previous reports and made recommendations that could help the Agency strengthen cyber security practices for combating APTs. However, some of those recommendations remain unimplemented, and we continue to find and report on similar weaknesses at other EPA locations. EPA should address open recommendations, be proactive in implementing agreed-upon actions without further delay, and take steps to improve cyber security practices throughout the entire Agency. If EPA does not take these steps, its information security weaknesses could negatively affect the availability and integrity of all Agency data.

What We Recommend

We recommend that the Assistant Administrator for Environmental Information and Chief Information Officer issue a memorandum to Office of Environmental Information executives stressing the importance of and expectation for completing audit recommendations by the agreed-upon milestone date, strengthen management control processes for monitoring and completing all open and future audit recommendations by the agreed-upon milestone date, and update the Enterprise Transition Plan Information Management segment to define the actions the Agency plans to take to achieve its security target architecture.

The Agency agreed with all the recommendations except for the recommendation to update its audit control process to require the Chief Information Officer to approve milestone dates extensions. Management stated that it implemented a new audit control process giving the Chief Information Officer monthly status reports, and we removed the recommendation.