Report In Brief

FEBRUARY 1, 2013

Background

The Public and Enterprise Wireless LAN (PEWLAN) system provides wireless access on USPTO's Alexandria, Virginia, campus. PEWLAN provides USPTO employees and contractors access to internal USPTO systems and information as if they were using a wired connection to perform their work, which can include financial and patent application information.

When we began our audit on June 27, 2012, USPTO insisted that PEWLAN was under development and was not operational and requested that we wait until 2013 to review the system. However, we independently verified that USPTO had connected PEWLAN to its operational environment.

Why We Did This Review

We evaluated PEWLAN as part of our FY 2012 Federal Information Security Management Act of 2002 (FISMA) audit.

Our objective was to assess the effectiveness of USPTO's IT security program by determining whether key security measures adequately protect its systems and its information. To do so, we assessed security measures USPTO employed during development of its PEWLAN system.

U.S. PATENT AND TRADEMARK OFFICE

USPTO Deployed Wireless Capability with Minimal Consideration for IT Security

OIG-13-014-A

WHAT WE FOUND

PEWLAN was inappropriately connected to USPTO's operational environment. In April 2012, USPTO first connected PEWLAN to its operational environment. Over the next 3 months, PEWLAN remained connected intermittently to USPTO's operational environment. However, before connecting PEWLAN, USPTO did not identify, implement, and document security controls required to protect the system. As a result, USPTO was unable to assess appropriate security controls, which is a critical step to understanding the security risks when introducing a new system into an operational environment. Thus, USPTO put its critical operational systems at risk.

PEWLAN was placed into operation without proper authorization. USPTO placed PEWLAN into operation in early June 2012 and made the system available to users without having the required authorization to operate the system. USPTO granted an interim authorization to test (IATT) for PEWLAN based solely on the risks identified in penetration test reports and without assurance that security controls were properly implemented. Furthermore, USPTO should have issued an IATT before conducting penetration testing.

WHAT WE RECOMMEND

We make the following recommendations to the Under Secretary of Commerce for Intellectual Property and Director of the U.S. Patent and Trademark Office:

1. Ensure that system owners register all systems under development in Cyber Security Assessment and Management during the initiation phase of the SDLC.
2. Ensure that USPTO rigorously applies its SDLC process and the RMF to all IT system development projects. This should include ensuring that required system security documents are appropriately developed and updated and that security controls required to protect a system are implemented and assessed.
3. Ensure that system owners, information system security officers, technical leads, project managers, and program managers attend the SDLC role-based training course regularly.
4. Ensure that the Cybersecurity Division representatives have a role in deciding whether IT system development projects should transition to a subsequent phase in the SDLC, based on their assessment of the effectiveness of incorporating security into the process.