U.S. PATENT AND TRADEMARK OFFICE

USPTO Deployed Wireless Capability with Minimal Consideration for IT Security

FINAL REPORT NO. OIG-13-014-A

FEBRUARY 1, 2013

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

FOR PUBLIC RELEASE

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

February 1, 2013

MEMORANDUM FOR: David Kappos
Under Secretary of Commerce for Intellectual Property and
Director of the U.S. Patent and Trademark Office

Teresa Stanek Rea
Deputy Under Secretary of Commerce for Intellectual Property
and Deputy Director of the USPTO

FROM: Allen Crawley
Assistant Inspector General for Systems Acquisition
and IT Security

SUBJECT: *USPTO Deployed Wireless Capability with Minimal Consideration for IT Security*
Final Report No. OIG-13-014-A

Attached is the final report of our audit of USPTO's Public and Enterprise Wireless LAN (PEWLAN) system, which we conducted to meet our obligations under the Federal Information Security Management Act.

We found that USPTO inappropriately connected PEWLAN to USPTO's operational environment and placed PEWLAN into operation without proper authorization.

We recommend that USPTO ensure that the system owners register all systems under development in Cyber Security Assessment and Management during the system's initiation phase and that USPTO rigorously applies its system development life cycle (SDLC) process and NIST's risk management framework to all system development projects. Further, we recommend that system owners, information system security officers, technical leads, project managers, and program managers attend USPTO's SDLC role-based training course on a regular basis. Finally, we recommend that 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.

We are pleased that in response to our draft report, you concurred with our findings and recommendations. We have summarized your response in the report and included the response as an appendix. We will post this report on OIG's website.

In accordance with Department Administrative Order 213-5, please provide us with your action plan within 60 calendar days from the date of this memorandum. The plan should outline actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extended to us by your staff during our audit. Please direct any inquiries regarding this report to me at (202) 482-1855 and refer to the report title in all correspondence.

Attachment

cc: Simon Szykman, Chief Information Officer
John Owens, Chief Information Officer, USPTO
Rod Turk, Director, Office of Cyber Security, and Chief Information Security Officer
Welton Lloyd, Audit Liaison, USPTO
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer

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.

Contents

Introduction

The U.S. Patent and Trademark Office (USPTO) fosters innovation, competitiveness, and economic growth through quality and timely examinations of patent and trademark applications. Patent operations, which account for the vast majority of USPTO's staffing and monetary resources, determine whether inventions claimed in patent applications are new, useful, and non-obvious. The timely granting of quality patents provides inventors with exclusive rights to their discoveries and contributes to the strength and vitality of the U.S. economy.

As part of our FY 2012 Federal Information Security Management Act (FISMA) audit, we evaluated USPTO's Public and Enterprise Wireless LAN (PEWLAN) system, which 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 accessing financial and patent application information. It also provides Internet access to authorized USPTO visitors and guests using their own devices, such as laptops, tablets, and smartphones.

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 this system. However, we independently verified that USPTO had connected PEWLAN to its operational environment (e.g., production systems and critical information). In addition, in late June 2012, USPTO posted documents on its chief information officer's (CIO's) intranet, which informed employees and contractors that the new wireless capabilities were available and described how to use them.

USPTO first connected PEWLAN to its operational environment starting in April 2012 to allow a contractor to perform penetration testing. Three reports issued by the contractor identified significant security weaknesses and vulnerabilities. However, before completely remediating these weaknesses and vulnerabilities, USPTO placed PEWLAN into operation on June 11, 2012.

We determined that USPTO placed PEWLAN into operation despite serious security weaknesses and significant vulnerabilities and had not implemented the required security controls and conducted proper control assessment as defined by FISMA. As a result, on August 7, 2012, we issued a memorandum to the Under Secretary of Commerce for Intellectual Property and Director of the U.S. Patent and Trademark Office, stating that the current security posture of PEWLAN presented significant and undue risks to USPTO's operational systems and information and recommending that USPTO immediately disconnect PEWLAN from USPTO's operational environment. Our memorandum also informed USPTO that we would be issuing an audit report containing additional recommendations. The Under Secretary responded via e-mail that same day, noting that USPTO had disconnected PEWLAN.

On September 19, 2012, USPTO's CIO issued a memorandum acknowledging that USPTO did not fully comply with its system development life cycle (SDLC) process—which places a priority on security participation and authorization—during development of PEWLAN.

In addition, USPTO initiated PEWLAN as a project in June 2011; however, it did not identify (register[1]) PEWLAN as a system under development in the Department's information system inventory maintained in the Cyber Security Assessment and Management (CSAM) tool. USPTO did not register PEWLAN as a system under development until July 6, 2012—13 months after USPTO began development and 9 days after we began our fieldwork.

Table 1 contains a timeline of USPTO's development and our audit of PEWLAN. We reviewed the security measures USPTO employed during development of PEWLAN. See appendix A for details regarding our objectives, scope, and methodology.

Table 1. Timeline for PEWLAN Development and Audit

Date	Event
June 2011	USPTO initiated PEWLAN project.
April 2012	USPTO connected PEWLAN to its operational environment for penetration testing by contractor.
June 11, 2012	USPTO placed PEWLAN into operation with no authorization to operate.
June 27, 2012	OIG held audit kickoff meeting–USPTO denied wireless was operational.
June 29, 2012	OIG confirmed PEWLAN was operational.
June 29, 2012	USPTO issued interim authorization to test for PEWLAN.
July 6, 2012	USPTO registered PEWLAN as a system under development in Cyber Security Assessment and Management.
August 7, 2012	OIG issued memo to the Director, USPTO, recommending USPTO disconnect PEWLAN.
August 7, 2012	USPTO disconnected PEWLAN.
August 15, 2012	USPTO issued an authorization to operate for PEWLAN.
August 22, 2012	USPTO reconnected PEWLAN.
September 19, 2012	USPTO's CIO responded to OIG's August 7 memorandum.

Source: OIG analysis

[1] Step 1 of the risk management framework described in NIST SP 800-37 requires the system owner to "Register the information system with appropriate organizational program/management offices," which identifies the system in the system inventory.

Background

USPTO's Office of the Chief Information Officer has developed an SDLC process, which includes measures to incorporate IT security early in a system's life cycle. The process intends to ensure that the system is secure and conforms to USPTO and federal IT security standards and guidelines. The National Institute of Standards and Technology (NIST) has developed a risk management framework (RMF)[2] for ensuring integration of appropriate IT security requirements into an organization's enterprise architecture and SDLC process. The goals of USPTO's SDLC are compatible with NIST's RMF. The RMF includes guidance for developing system security plans, conducting security control assessments, and authorizing systems to operate during all phases of a system's life cycle.

System Security Plans

The RMF assigns the system owner responsibility for developing and maintaining the system security plan. The system security plan provides an overview of security requirements and describes the controls in place or planned for meeting those requirements. The plan also describes implementation details for security controls and thus serves as a basis for assessing control effectiveness. The plan further serves as the vehicle for documenting the structured process of planning adequate, cost-effective security protection for a system. System security plans are living documents that require periodic review and modification to reflect the status of the system during the development life cycle. The authorizing official is responsible for approving system security plans.

Security Control Assessments

The RMF also includes guidance for conducting security control assessments throughout the SDLC and recommends conducting them as early as practicable. The purpose of the assessments is to ensure that the security controls, as described in the system security plan, are operating as intended. Therefore, the security plan must document security controls as accurately as possible. The RMF further requires documenting assessment results in a security assessment report, used by the authorizing official to make a risk-based decision about the appropriate authorization status of a system, and documenting security weaknesses in plans of action and milestones (POA&Ms).

Security Authorization

The RMF describes the process of granting or denying authorization for an information system to operate based on a determination of risks to organizational operations and assets, individuals, other organizations, and the nation resulting from the operation of the system. The authorizing official uses the system security plan, security assessment report, and POA&M—

[2] NIST outlined a six-step process to manage risks throughout an information system's life cycle. Federal agencies have been required to follow the process for new system development since February 2010. NIST, February 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems,* NIST SP 800-37. Gaithersburg, MD: NIST.

collectively referred to as the security authorization package—along with other available documents, such as a risk assessment report, to determine risks associated with operating the system and the acceptability of these risks. If the risks are acceptable, the authorizing official issues an authorization to operate for a specified period under certain terms and conditions.

The RMF also includes an interim authorization to test (IATT)—a special type of authorization decision allowing an information system to operate in an operational environment in order to test the system with actual operational (i.e., live) data for a specified period. The authorizing official grants an IATT only when the operational environment or live data are required to complete specific test objectives. The IATT allows organizations to assess functional and security requirements within a system's intended environment during development.

Findings and Recommendations

I. PEWLAN Was Inappropriately Connected to USPTO's Operational Environment

In April 2012, 10 months after initiating the PEWLAN project, USPTO first connected PEWLAN to its operational environment to conduct penetration tests, which identified serious security weaknesses in the system's architecture and security controls. Over the next 3 months, PEWLAN remained connected intermittently to USPTO's operational environment. However, before connecting PEWLAN to the operational environment, 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 while conducting penetration tests, remediating weaknesses, and implementing architectural changes associated with PEWLAN.

While the penetration testing provided some visibility of the security risks associated with PEWLAN, it is only part of the security control assessments required by the RMF. It does not constitute a full assessment of security control implementations, nor does it convey all risks to USPTO's operational environment. Nonetheless, the tests did identify the following risks, which most concerned us:

1. Internal infrastructure components were visible to public users.
2. Authentication of users did not function as intended.
3. Credentials used to log on to USPTO systems were vulnerable on the public portion of PEWLAN.
4. The wireless intrusion prevention system did not appropriately detect and provide alerts for security events.

As a result, the penetration testing itself, by directly connecting PEWLAN to the operational environment, increased the risk of compromise due to the presence of these vulnerabilities.

In addition, before performing these penetration tests, USPTO should have selected and implemented the appropriate required set of security controls and described their implementation in a system security plan, which serves as a foundation for conducting security control assessments and documenting risk throughout a system's life cycle. However, USPTO made little progress toward identifying security requirements, developing the system security plan, or conducting control assessments in the 10 months following PEWLAN's initiation. Without a fully developed system security plan and adequate security control assessments, USPTO did not have an accurate perspective of associated risks to support its decision to put PEWLAN into its operational environment. In fact, when penetration testing started, an internal preliminary risk assessment report issued by USPTO's Cybersecurity Division, on April 17, 2012, indicated that "*there is no documentation*

available associated to PEWLAN.…Therefore the current security features and posture are unknown to internal stakeholders."

II. PEWLAN Was Placed into Operation Without Proper Authorization

USPTO placed PEWLAN into operation in early June 2012 and thus made the system available to users without having the required authorization to operate the system[3]. On June 29, 2012—2 days after our audit kickoff meeting—USPTO's CIO issued an IATT for PEWLAN with an expiration date of September 29, 2012.

However, USPTO granted the IATT for PEWLAN based solely on the risks identified in the penetration test reports and without assurance that security controls were properly implemented. Furthermore, USPTO should have issued an IATT before conducting the penetration testing in April 2012.

Although the IATT identified the need to remediate vulnerabilities discovered during penetration testing and to finalize documentation for the system, it did not address key elements to support the authorization decision. For example, the IATT did not identify specific test objectives and did not specifically identify the need to conduct security control assessments and develop a complete security authorization package before expiration of the IATT. When USPTO issued the IATT, the only system security plan that existed was a preliminary draft, which did not include implementation descriptions for security controls and did not allocate them to PEWLAN system components. Without fully addressing these key elements, USPTO could not realistically determine risks associated with operating PEWLAN during the IATT.

Conclusion

We found that USPTO did not develop appropriate security documents, perform security control assessments, or assess risks before conducting penetration testing or beginning deployment of PEWLAN.

According to USPTO's SDLC process, persons with system development roles (e.g., project managers, system owners, and technical leads) are responsible for coordinating with representatives from the Cybersecurity Division to ensure that security-related documents are developed and updated and that appropriate authorization actions, including control assessments, are completed throughout a system's life cycle. We found that security missteps during PEWLAN's development occurred largely because this coordination was ineffective. Furthermore, based on interviews with USPTO officials and our analysis, pressure from an aggressive project schedule likely contributed to lapses in following the SDLC process.

[3] Security control CA-6, Security Authorization, specifies that the organization should ensure that the authorizing official authorizes the information system for processing before commencing operations. NIST, August 2009. *Recommended Security Controls for Federal Information Systems and Organizations,* NIST SP 800-53. Gaithersburg, MD: NIST.

To promote an understanding of the relationship between USPTO's SDLC process and the RMF and to improve group coordination during system development, USPTO recently implemented an SDLC role-based training course for information system security officers, system owners, technical leads, project managers, and program managers. The course maps the phases of USPTO's SDLC to the general life cycle referred to in descriptions of NIST's RMF and identifies security documents and the roles associated with their production during the various SDLC phases. Specifically, it reinforces the role of facilitation points of contact, who are representatives from the Cybersecurity Division tasked with assisting system owners, information system security officers, and technical leads in developing and maintaining system security documentation, updating and maintaining security information in system design documents, and implementing continuous monitoring.

Institutionalizing the SDLC role-based training course should significantly increase the likelihood of appropriately incorporating security into USPTO's SDLC. Furthermore, USPTO has indicated that because of our audit, it has started implementing a procedure where 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.

Since issuing the IATT on June 29, 2012, USPTO has developed system design documents and an approved system security plan, developed procedures for assessing security controls, and conducted security control assessments for PEWLAN. On August 15, 2012, USPTO's CIO issued an authorization to operate for PEWLAN based on his review of a complete security authorization package. Our review of the authorization package noted several issues in the system's POA&M—most notably, excessive remediation times for several critical controls and inappropriate prioritization of a POA&M item related to account management. We discussed these issues with USPTO security officials, who addressed our concerns.

Recommendations

To help ensure that USPTO appropriately considers IT security in future IT system development efforts, we make the following recommendations to the Under Secretary of Commerce for Intellectual Property and Director of the United States 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 on a regular basis.

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.

Summary of Agency Response and OIG Comments

In response to our draft report, USPTO concurred with our findings and recommendations. In addition, USPTO indicated that it has remediated many of the issues related to our findings.

Appendix A: Objectives, Scope, and Methodology

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 recently deployed Public and Enterprise Wireless LAN (PEWLAN) system by

- reviewing system-related documents, including project development documentation, policy and procedures, planning documents, security assessment documents, and other material supporting the development of PEWLAN and
- interviewing USPTO IT security personnel.

We reviewed USPTO's compliance with the following applicable provisions of law, regulations, and mandatory guidance:

- the Federal Information Security Management Act of 2002
- IT Security Program Policy and Minimum Implementation Standards, U.S. Department of Commerce, introduced by the Chief Information Officer on March 9, 2009, and applicable Commerce Information Technology Requirements
- NIST Federal Information Processing Standards publications:
    - 199, Standards for Security Categorization of Federal Information and Information Systems
    - 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Special Publications:
    - 800-18, Guide for Developing Security Plans for Information Technology Systems
    - 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
    - 800-53, Recommended Security Controls for Federal Information Systems and Organizations
    - 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
    - 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes I and II

- 800-70, Security Configuration Checklists Program for IT Products
- 800-115, Technical Guide to Information Security Testing and Assessment

We conducted our fieldwork from June to October 2012. We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated August 31, 2006. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Appendix B: Agency Response

UNITED STATES PATENT AND TRADEMARK OFFICE

CHIEF FINANCIAL OFFICER

JAN 18 2013

MEMORANDUM FOR: Allen Crawley
Assistant Inspector General for System Acquisition and IT Security, Office of Inspector General

FROM: Anthony P. Scardino
Chief Financial Officer

SUBJECT: Response to Draft Report "*USPTO Deployed Wireless Capability with Minimal Consideration for IT Security*" (December 2012)

Thank you for your draft report dated December 14, 2012, detailing your findings and recommendations. We appreciate the effort your staff has made in evaluating the effectiveness of our PEWLAN Information System. We have carefully considered and concur with the recommendations made in the subject draft report. The United States Patent and Trademark Office (USPTO) provides the following attachment as our response to the audit report findings.

Again, we thank the Assistant Inspector General for System Acquisition and IT Security for the report. We intend to meet the recommendations in a diligent manner, and we will gratefully accept suggestions as we move forward to ensure that an effective security program is in place that will enable us to securely maintain systems in support of the USPTO.

Attachment

P.O. Box 1450, Alexandria, Virginia 22313-1450 - WWW.USPTO.GOV

USPTO Cyber Security's Response to FY 2012 FISMA Assessment of the Public and Enterprise Wireless LAN (PEWLAN) (PTOI-014-00), Draft Report December 2012

OIG Finding:

1. *PEWLAN was inappropriately connected to USPTO's operational environment.*

   - *USPTO connected PEWLAN to its operational environment to conduct penetration tests, which identified serious security weaknesses in the system's architecture and security controls. PEWLAN remained intermittently connected to the USPTO operational environment over the next three months following the completion of the penetration testing.*

   - *USPTO did not identify, implement, and document security controls required to protect the system prior to connecting PEWLAN to the operational environment. As a result, the USPTO was unable to assess appropriate security controls leaving critical operational systems at risks while conducting penetration tests, remediating weaknesses, and implementing architectural changes associated with PEWLAN.*

   - *The penetration tests performed do not constitute a full assessment of security control implementations nor does it convey all risks to USPTO's operational environment.*

   - *Penetration tests revealed that by directly connecting PEWLAN to the operational environment, risks were increased due to the presence of the following vulnerabilities:*

     - *Internal infrastructure components were visible to public users*
     - *Authentication of users did not function as intended*
     - *Credentials used to log on to USPTO systems were vulnerable on the public portion of PEWLAN*
     - *The wireless intrusion prevention system did not appropriately detect and provide alerts for security events*

   - *USPTO did not have an accurate perspective of associated risks to support its decision to put PEWLAN into its operational environment due to the fact that the appropriate security controls were not selected and implemented. In addition, a system security plan was not in place in the following ten months since the PEWLAN project was initiated.*

USPTO Response:

USPTO agrees with this finding. The following actions were taken to address the concerns above:

- A System Security Plan (SSP) was created for PEWLAN and was finalized on August 15, 2012. The SSP addressed the implementation and planned implementation of all security controls within NIST Special Publication 800-53 Revision 3.

- Full assessments of the applicable security controls for PEWLAN were completed in accordance with NIST SP 800-37 Revision 1 and NIST SP 800-53A.

- Vulnerability scans were performed on all PEWLAN devices. An analysis was performed on the scan results to ensure that there were no major vulnerabilities and that the latest applicable patches were installed. The analysis was provided to the assessment team to use as artifact evidence.

- Plan of Action & Milestones (POA&M) were created in the Cyber Security Assessment & Management (CSAM) tool for all planned controls. The following are POA&Ms that were created pre and post assessment:

    - CM-2, CM-2(1), CM-2(3) Baseline Configuration
    - CM-6 Configuration Settings
    - CM-7, CM-7(1) Least Functionality
    - MA-2 Controlled Maintenance
    - MA-6 Timely Maintenance
    - SI-2 Flaw Remediation
    - AC-2, AC-2(1), AC-2(2), AC-2(3), AC-2(4) Account Management
    - AC-6, AC-6(1) Least Privilege
    - AU-2, AU-2(3) Auditable Events
    - IA-2, IA-2(1), IA-2(2), IA-2(3) Identification and Authentication
    - AC-8 System Use Notification
    - RA-5 Vulnerability Scanning

- All of the POA&Ms created for PEWLAN have been addressed, remediated and closed as shown in the table below.

- The issue which allowed internal infrastructure components to be visible to public users has been remediated by reconfiguring the Perimeter Firewalls to adequately block discovery scans.

- The issues with weaknesses to public wireless authentication using USPTO credentials have been resolved. The Entrust certificate authority has been incorporated into the authentication process to adequately verify a user.

- The issue pertaining to detection and security alerts for the Wireless Intrusion Protection System (WIPS) has been resolved. Security alerts are now being produced and recorded for PEWLAN as intended.

- The PEWLAN assessment yielded a Risk Assessment Report (RAR) justifying a determination for granting an "Authority to Operate" for the system was based on the risk analysis within the report. The risks were mapped to the appropriate NIST security controls and were acknowledged by the authorizing official.

OIG Finding:

2. *PEWLAN was placed into operation without proper authorization.*

   - *USPTO granted an Interim Authority to Test (IATT) for PEWLAN based solely on the risks identified in the penetration test reports and without assurance that security controls were properly implemented. In addition, the IATT was granted after the system was in operation.*

   - *The IATT identified the need to remediate vulnerabilities discovered during penetration testing and to finalize documentation for the system. However, the IATT did not address key elements to support the authorization decision.*

     - *The IATT did not identify specific test objectives, the need for security control assessments, and a plan to develop a complete security authorization package before the expiration of the IATT.*

     - *The only system security plan that existed at the time the IATT was issued was a preliminary draft, which did not include implementation descriptions for security controls and did not allocate them to PEWLAN system components.*

USPTO Response:

USPTO agrees with this finding. The following actions have been taken to address the issues above:

- A full assessment was performed on PEWLAN in which any security controls that were not implemented or working as intended, were deemed as risks to the USPTO. The vulnerabilities were identified within the Security Assessment Report (SAR) and the risks associated with the vulnerabilities were documented within the Risk Assessment Report (RAR).

- A Plan of Actions & Milestones was created for the risks identified in the RAR in order to adequately track and monitor them in accordance with USPTO policy.

- In addition, the IATT template has been revised to ensure future systems seeking approval to test in a production environment are required to identify the following:

  - Identify specific test objectives

  - Risk associated to security controls

  - Compensating security controls

- Required remedial action performed in conjunction with testing

- The PEWLAN System Security Plan was finalized and approved by the System Owner (SO), Technical Lead (TL), Senior Information Security Officer (SISO) and the Authorizing Official (AO) on August 15, 2012.

This table summarizes the resolution for each POA&M created in CSAM pertaining to PEWLAN:

POA&M ID (CSAM)	FY 2012 Weaknesses / POA&M Title	Detailed Weakness Description	Weakness Criticality	Point of Contact	Scheduled Completion Date	Resolution
54763	PEWLAN-2012; CM-2, CM-2(1), CM-2(3) Baseline Configuration	The baseline configuration for PEWLAN has not been defined or developed. This may lead to vulnerabilities and configuration inconsistencies.	High	PEWLAN Technical Lead/FPOC	Remediated 8/31/2012	Documented baseline configurations in addition to vendor documents which detail the configuration baseline settings. Vendor documentation has been obtained and includes all the infrastructure devices configurations associated with PEWLAN.
54766	PEWLAN-2012; CM-6 Configuration Settings	PEWLAN has not documented mandatory configuration settings within their system documentation. This can lead to configuration inconsistencies and vulnerabilities. PEWLAN Internal infrastructure components were visible to public users.	High	PEWLAN Technical Lead/FPOC	Remediated 12/19/2012	Mandatory configurations settings have been established, implemented, and obtained from the technical lead. This is now documented within the system's detailed design diagram and reviewed on an annual basis at minimum to ensure that the most restrictive settings are implemented into the system.

POA&M ID (CSAM)	FY 2012 Weaknesses / POA&M Title	Detailed Weakness Description	Weakness Criticality	Point of Contact	Scheduled Completion Date	Resolution
54781	PEWLAN-2012; CM-7, CM-7(1) Least Functionality	The ports, protocols, and services are not documented within the PEWLAN SDLC documents. This can leave the system vulnerable to attacks and cause configuration inconsistencies.	High	PEWLAN Technical Lead/FPOC	Remediated 12/19/2012	The open ports, protocols, and services associated with PEWLAN have been established and documented within the system's detailed design diagram. Certain ports, protocols, and services have been restricted in accordance to the USPTO IT Security Handbook.
54783	PEWLAN-2012; MA-2 Controlled Maintenance	PEWLAN has no documented maintenance process and procedures within the DDD and OSP. This prohibits the reconstitution of the system in the event that it fails.	Medium	PEWLAN Technical Lead/FPOC	Remediated 12/19/2012	Maintenance procedures have been documented in PEWLAN's Operational Support Plan (OSP) and details the steps for requesting and approving maintenance on the system. In addition, Cisco's SmartNet maintenance contract has been documented which provides next day service support for its devices.

POA&M ID (CSAM)	FY 2012 Weaknesses / POA&M Title	Detailed Weakness Description	Weakness Criticality	Point of Contact	Scheduled Completion Date	Resolution
54784	PEWLAN-2012; MA-6 Timely Maintenance	PEWLAN does not document timely maintenance requirements within the OSP. This can cause the system administrators to not adequately maintain the system, ultimately leading to system failure.	Medium	PEWLAN Technical Lead/FPOC	Remediated 8/31/2012	Documented the timely maintenance requirements within the implementation statement of the SSP and OSP to reflect the use of Cisco's "SmartNet" service contract and Juniper's "End User Support Agreement". In addition, vendor documentation has been obtained (Cisco and Juniper).
54786	PEWLAN-2012; SI-2 Flaw Remediation	PEWLAN has not documented the flaw remediation process within the OSP. This could lead to inconsistencies and flaws not being remediated in a timely manner.	High	PEWLAN Technical Lead/FPOC	Remediated 8/31/2012	Provided implementation statements within the SSP and OSP documenting the flaw remediation process. In addition, screenshots were obtained of a CR for the system as evidence that the PEWLAN utilizes EAMS as part of their flaw remediation process.
54787	PEWLAN-2012; AC-2, AC-2(1), AC-2(2), AC-2(3), AC-2(4) Account Management	PEWLAN does not adequately document account management within the DDD, OSP. This could lead to vulnerabilities and inconsistencies when issuing accounts.	High	PEWLAN Technical Lead/FPOC	Remediated 9/14/2012	Network Account Procedures were created to adequately document PEWLAN account management.

Page 9 of 12

POA&M ID (CSAM)	FY 2012 Weaknesses / POA&M Title	Detailed Weakness Description	Weakness Criticality	Point of Contact	Scheduled Completion Date	Resolution
54788	PEWLAN-2012; AC-6, AC-6(1) Least Privilege	PEWLAN does not adequately document the privileges of administrators and who this is assigned to. This could lead to privilege escalation vulnerabilities.	Medium	PEWLAN Technical Lead/FPOC	Remediated 9/10/2012	Screenshots were gathered and documented to demonstrate the implementation of least privilege. Administrative accounts have been segmented and only the minimum level of permissions is granted in order to perform job functions.
54789	PEWLAN-2012; AU-2, AU-2(3), AU-2(4) Auditable Events	PEWLAN does not adequately document the list of auditable events. This can lead to audit log inconsistencies and vulnerabilities. The wireless intrusion prevention system did not appropriately detect and provide alerts for security events.	Medium	PEWLAN Technical Lead/FPOC	Remediated 9/10/2012	Auditable events have been documented within the SSP to reflect the requirements which are configured to be logged by the Security Incident and Event Management (SIEM) system. In addition, screenshots have been gathered as artifacts to display audit trails, alerts, log modules, and system logs for PEWLAN's central management system; Cisco's Network Control System (NCS).

POA&M ID (CSAM)	FY 2012 Weaknesses POA&M Title	Detailed Weakness Description	Weakness Criticality	Point of Contact	Scheduled Completion Date	Resolution
54791	PEWLAN-2012; IA-2, IA-2(1), IA-2(2), IA-2(3) Identification and Authentication (Organizational Users	PEWLAN does not adequately identify the portions of the identifier management process in which accounts are created (TL approval). This could lead to inconsistencies within the organizational policy. Authentication of users did not function as intended. Credentials used to log on to USPTO systems were vulnerable on the public portion of PEWLAN	Medium	PEWLAN Technical Lead/FPOC	Remediated 8/31/2012	Identifiers and authenticators associated with PEWLAN have been documented and identified in the SSP, OSP, and DDD. In addition, screenshots have been gathered as artifacts to display multi-factor authentication methods for gaining access to PEWLAN's central management system and network access.
54930	PEWLAN-2012; AC-8 System Use Notification	The PEWLAN system does not have a system use notification screen before allowing access to the system. This could lead to misconceptions on what is allowed when using the system.	Medium	PEWLAN Technical Lead/FPOC	Remediated 8/31/2012	New implementation statement has been provided in addition to screenshots of the system use notification for the Public, Private, Guest access to the wireless network.
55205	PEWLAN-2012; RA-5 Vulnerability Scanning	Vulnerability scanning has not been performed for the PEWLAN. This can lead to unforeseen vulnerabilities due to the fact that the system is not equipped with the most up-to-date patches.	High	PEWLAN Technical Lead/FPOC	Remediated 9/19/2012	Vulnerability scanning has been performed and analyzed. Artifacts are in the form of scan results (raw and analyzed), a screenshot of an email confirming that the

Page 11 of 12

POA&M ID (CSAM)	FY 2012 Weaknesses/ POA&M Title	Detailed Weakness Description	Weakness Criticality	Point of Contact	Scheduled Completion Date	Resolution
						scans have been performed, and the scanning procedures have been documented in the PEWLAN SSP.

The POA&Ms above correlate to OIG findings and recommendations. With the completion of these POA&Ms, USPTO will satisfy the technical recommendations provided by OIG.

We appreciate the cooperation and courtesies extended to us by your staff. If you would like to discuss any details of this corrective action plan further, please do not hesitate to contact the USPTO Director of Cyber security, John Pardun by phone at (571) 272-4349 or by e-mail John.Pardun@USPTO.GOV.

Page 12 of 12

011200000142