OFFICE OF INSPECTOR GENERAL

Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence

Homeland Security

September 2, 2015

OIG-15-137

DHS OIG HIGHLIGHTS

Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence

September 2, 2015

Why We Did This Audit

U.S. Customs and Border Protection (CBP) developed the Analytical Framework for Intelligence (AFI)—an index of relevant data in existing systems—to augment Department of Homeland Security's (DHS) ability to gather and develop information about persons, events, and cargo of interest. We performed this audit to determine the status of AFI implementation and whether effective controls have been applied to protect the sensitive information processed and stored by the system.

What We Recommend

We recommended CBP address deficiencies identified in AFI configuration settings and system documentation.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

CBP has made significant progress in implementing AFI. CBP fully deployed AFI on schedule and within budget, and has taken measures to secure the sensitive information the system processes and stores from unauthorized access. In addition, CBP developed a privacy impact assessment to ensure that privacy considerations for operating AFI were addressed throughout system deployment. Since deployment, system users have provided positive feedback to the component about AFI's functionality and usefulness.

Despite these positive steps, we identified deficiencies that the component must address to further secure the system. For example, we identified vulnerabilities in CBP's configuration of AFI servers and applications, management of administrative accounts, contingency planning process, and plan of action and milestone process. These vulnerabilities exist because CBP did not implement all security controls according to DHS requirements. Operating AFI without effectively implementing the required security controls increases the risk of inadvertent information disclosures and service disruptions.

CBP Response

CBP concurred with all seven recommendations and has implemented corrective actions to address the findings. We consider the recommendations resolved and closed.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 2, 2015

MEMORANDUM FOR: Charles R. Armstrong
Assistant Commissioner and Chief Information Officer
U.S. Customs and Border Protection

FROM: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence*

Attached for your information is our final report, *Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence*. We incorporated CBP's formal comments into our report. The report contains seven recommendations aimed at improving the security of the Analytical Framework for Intelligence. CBP concurred with all seven recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 7 resolved and closed.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Cybersecurity and Intelligence Division, at (202) 254-5472.

Attachment

Table of Contents

Appendixes

Abbreviations

AFI	Analytical Framework for Intelligence
CBP	U.S. Customs and Border Protection
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
POA&M	plan of action and milestones
TASPD	Targeting and Analysis Systems Program Directorate

Background

U.S. Customs and Border Protection (CBP) is responsible for securing U.S. borders and facilitating legitimate trade and travel. Identifying and developing a comprehensive understanding of criminal threats to the Nation's borders is paramount in accomplishing the CBP mission. To augment intelligence research, analysis, and collaboration capabilities needed for border security, CBP developed the Analytical Framework for Intelligence (AFI), which is an analyst-oriented, web-based application. AFI provides an intelligence platform to support and enhance the component and Department's ability to identify, apprehend, and prosecute individuals who pose potential law enforcement or security risks. AFI consists of a suite of tools that are incorporated into a single platform designed to support intelligence analysts in the integration, research, analysis, and visualization of large amounts of data from disparate sources. Intelligence analysts can access information products within AFI only through the CBP intranet. Figure 1 depicts the AFI system structure.

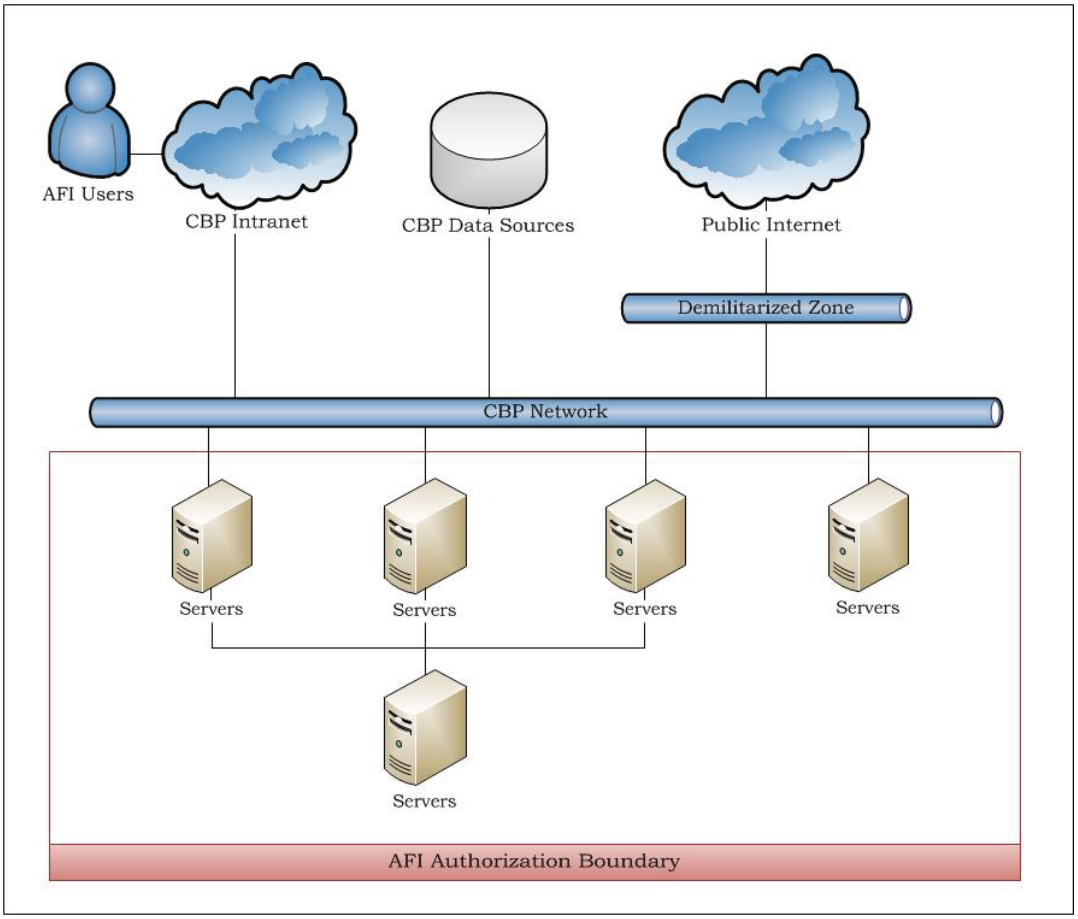

Figure 1: AFI System Structure
Source: Office of Inspector General (OIG)

AFI augments the Department of Homeland Security's (DHS) ability to gather and develop information about persons, events, and cargo of interest by creating an index of the relevant data in existing systems and providing intelligence analysts with different tools to identify non-obvious relationships. Specifically, AFI allows a federated search across selected law enforcement and intelligence systems, as well as automated visualization and analysis capability, with the goal of producing actionable, finished intelligence products that can be disseminated across Federal agencies and state, local, and tribal law enforcement partners.

The Office of Targeting and Analysis Systems Program Directorate (TASPD) within CBP's Office of Information and Technology administers and maintains AFI. AFI became fully operational in August 2012 and has more than 2,600 active users. Most AFI users are assigned the "consumer" role, which allows them to browse and conduct keyword searches of published intelligence products and set up automated notifications for specific topics. Other user roles (e.g., researcher, analyst, or product author) have the capability to search data sources, access analytical and visualization tools, and create and disseminate intelligence products across CBP.

Instead of collecting information from the public, AFI gathers its data by querying available information already stored in existing government systems and commercial data sources. Additionally, AFI analysts can upload any information that is relevant to a project, including information publicly available on the internet. Examples of the data elements are full name, date of birth, gender, travel information, passport information, country of birth, physical characteristics, familial and other contact information, importation/exportation information, and enforcement records.

The National Institute of Standards and Technology (NIST) requires agencies to categorize information systems as low impact, moderate impact, or high impact for the stated security objectives.[1] The security categories are based on the potential impact on an organization should certain events occur that may jeopardize the information and information systems needed by the organization to accomplish its assigned mission and day-to-day functions. As part of the security categorization process, CBP determines the criticality and sensitivity of information that AFI processes and stores. This helps ensure that AFI security controls are commensurate with the potential adverse impact on CBP operations and assets if there is a loss of confidentiality, integrity, or

[1] The process for determining the security category of an information system is outlined in Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004.

availability of the system. According to AFI's system security plan dated December 2014, AFI's confidentiality and integrity impact levels were both categorized as high, while its availability impact level was moderate. These impact levels are used to determine baseline security controls needed for the system.

Results of Audit

CBP has made significant progress in implementing AFI. CBP fully deployed AFI on schedule and within budget and has taken measures to secure the sensitive information the system processes and stores from unauthorized access. Despite these positive steps, we identified deficiencies that the component must address to further secure the system. For example, we identified vulnerabilities in CBP's configuration of AFI servers and applications, management of administrative accounts, contingency planning process, and plan of action and milestone process. These vulnerabilities exist because CBP did not implement all security controls according to DHS requirements. Operating AFI without effectively implementing the required security controls increases the risk of inadvertent information disclosures and service disruptions.

Progress in Deploying AFI

AFI, which operates on an annual budget of $23 million, became operational in August 2012. Since deployment, CBP has received positive feedback from its users about AFI's functionality and usefulness. For example, an intelligence analyst reported that AFI's ability to link travel and inspection records with law enforcement records played a role in answering key questions relating to bulk cash smuggling. Although CBP had plans for classified use of the system, management decided to implement AFI only to process and store sensitive but unclassified data. CBP has taken the following actions to safeguard sensitive AFI data and address privacy concerns of operating the system:

- developed a privacy impact assessment to assess how personal data are collected, used, disseminated, and maintained in AFI. In June 2012, the DHS Privacy Office approved and published AFI's privacy impact assessment and system of records notice;[2]

[2] A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The *Privacy Act of 1974* requires each agency to publish notice of its systems of records in the Federal Register. This notice is generally referred to as a system of records notice.

- compiled the required system security plans and other documentation needed to grant AFI the authority to operate for a period of 3 years in April 2013. CBP also updated AFI's system security plan and performed security control assessments on the system in accordance with applicable DHS policy in 2014;
- implemented a process to track AFI configuration changes. CBP can also use this process to identify insider threats or compromised user accounts;
- ensured that AFI's system administrators received specialized training to perform their significant security responsibilities;
- implemented a process to ensure security patches are deployed to AFI servers timely; and
- performed vulnerability scans on AFI servers monthly and on databases and the browser-based application on an ad hoc basis to identify and mitigate potential threats to the information processed and stored by the system.

Overall Issues to Be Addressed

While CBP has deployed AFI as scheduled and implemented controls to protect information processed and stored by the system, we found deficiencies that the component must address to further secure the system. For example, we identified vulnerabilities in CBP's configuration of AFI servers and applications, management of administrative accounts, contingency planning process, and plan of action and milestone process. These vulnerabilities exist because CBP did not implement all security controls according to DHS requirements. Operating AFI without effectively implementing the required security controls increases the risk of inadvertent information disclosures and service disruptions.

Configuration Vulnerabilities Pose Unnecessary Risk to AFI

Overall, CBP has implemented strong controls to protect information processed and stored by AFI. However, we identified several configuration vulnerabilities that should be mitigated to further protect AFI from unnecessary risk. As part of our audit, we performed security assessments on selected AFI servers and databases, as well as the browser-based application. The results from our vulnerability assessments revealed only two instances of missing high-risk patches. In addition, CBP must address system configuration vulnerabilities that may be exploited to gain unauthorized access to the system. Specifically, we identified the following:

- Two database accounts were configured with an easily guessed

password. DHS requires passwords to meet complexity requirements. Using easily guessable passwords allow unauthorized users to gain access to the database.

- Excessive privileges have been granted to the public role in AFI databases. Without properly restricting access to privileged commands, current users with an AFI database account may inadvertently or intentionally modify the database. While CBP does not have any basic user accounts for their database, DHS requires that privileges granted to the public role be removed.
- A cross-frame scripting vulnerability was identified on the browser-based application.[3] DHS requires that regular testing be performed to mitigate potential system vulnerabilities. While the AFI application is not accessible from the public-facing internet, this vulnerability may allow information being sent to the AFI application to be viewed by unauthorized individuals on the CBP network.
- An outdated encryption protocol is allowed to encrypt AFI network traffic. DHS requires that encryption be Federal Information Processing Standards 140-2 compliant. Using an outdated encryption protocol that is vulnerable may allow an attack to decrypt AFI network traffic.

According to CBP, the configuration vulnerabilities were caused by the inadvertent reversal of previously implemented security settings during an AFI database update. By default, databases are installed with specific configuration and access controls such as the permissions granted to the public role. These controls often do not meet the security standards required by DHS and must be modified by administrators.

In addition, new vulnerabilities were discovered in October 2014 on an encryption protocol used by AFI. Specifically, exploiting this vulnerability could allow unauthorized individuals to decrypt network traffic. This vulnerability in the encryption protocol has always been present; however, recent advances in cryptography have identified critical flaws that make the protocol insecure. While CBP uses a stronger encryption by default, this weaker protocol is still being used to ensure compatibility with older systems.

Implementing DHS-required configuration settings can help protect AFI from a wide variety of exploits. While CBP has implemented several controls to mitigate potential exploitation of the vulnerabilities identified, the risk of compromise to the system still exists. Operating AFI with known security

[3] Cross-frame scripting allows for a vulnerable website or application to be loaded into a malicious page created by an attacker. A link to the attacker's page is then sent to AFI users in the hope that they will mistake it for the legitimate website.

vulnerabilities may allow unauthorized access to sensitive information processed and stored by the system.

Recommendations

We recommend the Assistant Commissioner and Chief Information Officer:

Recommendation 1: Implement strong passwords on AFI databases in accordance with applicable DHS and CBP requirements.

Recommendation 2: Restrict permissions granted to the public role on AFI databases.

Recommendation 3: Implement configuration controls on the AFI browser-based application to prevent exploitation through cross-frame scripting.

Recommendation 4: Implement a secure encryption algorithm for all AFI network traffic.

CBP Comments to Recommendation 1

CBP concurred with recommendation 1. The accounts that were identified as having weak passwords were locked. AFI databases require strong passwords as a requirement. The CBP Office of Information and Technology has implemented a password verify function on all database profiles. Users are assigned profiles, which account for all users and accounts. Within the verify function, the DHS complex password requirements are enforced. Supporting documentation was previously provided to the OIG. CBP respectfully requests that the OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the steps that CBP has taken satisfy the intent of this recommendation. Based on our review of the supporting documentation provided, we consider this recommendation closed and resolved.

CBP Comments to Recommendation 2

CBP concurred with recommendation 2. The permissions granted to the public role are locked down. Only authorized database administrators have the ability to access the database directly and AFI is only accessible on the CBP intranet, which is not accessible by the general public. Supporting documentation was

previously provided to the OIG. CBP respectfully requests that OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the steps that CBP has taken satisfy the intent of this recommendation. Based on our review of the supporting documentation provided, we consider this recommendation closed and resolved.

CBP Comments to Recommendation 3

CBP concurred with recommendation 3. AFI plan of action and milestones (POA&M) 42, which addressed the cross-frame scripting vulnerability, was remediated on May 14, 2015. The CBP Office of Information and Technology, Targeting and Analysis Systems Program Directorate performed an ad-hoc WebInspect scan, which showed no cross-frame scripting vulnerabilities on the AFI browser-based application. The full results of the WebInspect scan are uploaded in the Information Assurance Compliance System to prove closure for AFI POA&M 42. Supporting documentation for closure of the recommendation will be provided to the OIG under separate cover. CBP respectfully requests that the OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the steps that CBP has taken satisfy the intent of this recommendation. Based on our review of the supporting documentation provided, we consider this recommendation closed and resolved.

CBP Comments to Recommendation 4

CBP concurred with recommendation 4. AFI POA&M 43, which addresses weak encryption algorithms, was remediated on May 20, 2015. AFI only permits strong encryption algorithms. The AFI Information Systems Security Officer also created a security report to monitor the cipher suites used to log into AFI, to ensure that no weak algorithms are permitted. Supporting documentation for closure of the recommendation will be provided to OIG under separate cover. CBP respectfully requests that OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the steps that CBP has taken satisfy the intent of this recommendation. Based on our review of the supporting documentation provided, we consider this recommendation closed and resolved.

CBP Has Created an Excess of Administrative Accounts on AFI Servers

CBP has granted an excessive number of administrators with elevated system access to AFI servers, exposing the system to unnecessary risk. We identified 55 unique active administrator and support accounts, many of which have never been used to log into AFI servers. On one server, 47 of the 55 accounts have never logged in, despite access being granted. In addition, we also identified two local administrator accounts intended for disaster recovery that were not assigned to an individual user.

According to CBP, administrators are granted access to servers throughout the entire enterprise instead of assigning them to specific systems, such as AFI. Specifically, these administrator accounts are needed to ensure full coverage during an emergency. In addition, CBP created the shared local administrator accounts for situations where an administrator may need access to AFI servers to ensure operation of the system in the event that the primary authentication servers fail.

DHS policy requires components to restrict administrator access to the servers they need to perform administration tasks. In addition, user accounts should be disabled after 45 days of inactivity for systems with a high confidentiality security impact level, such as AFI. Finally, DHS requires the Authorizing Official to approve all group accounts and to restrict their use to situations dictated by operational necessity.

By granting administrators full access to servers throughout the CBP domain and creating shared local administrator accounts, CBP exposes the system to unnecessary security risks. Granting administrators access to multiple systems throughout the CBP enterprise makes it possible for an attacker to take full control of several systems in the event a single account is compromised.

Recommendation

We recommend the Assistant Commissioner and Chief Information Officer:

Recommendation 5: Remove shared administrator accounts and assign administrator access based on the principles of least privilege.

CBP Comments to Recommendation 5

CBP concurred with recommendation 5. AFI revisited best practices of minimizing service accounts and assigning administrator access based on the principles of least privilege. There are a small number of AFI administrators dedicated to the AFI program who perform application specific operation and maintenance functions. CBP has removed administrative access from the additional administrators who had been granted access to manage AFI as one of many enterprise assets. Supporting documentation for closure of the recommendation will be provided to the OIG under separate cover. CBP respectfully requests that the OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the steps that CBP has taken satisfy the intent of this recommendation. Based on our review of the supporting documentation provided, we consider this recommendation closed and resolved.

System Restoration Capabilities Are Not Accurately Outlined in the Contingency Plan

CBP has not updated the AFI contingency plan to address deficiencies identified in the last contingency plan test. As a result, CBP may have difficulty restoring AFI operations in the event of a service disruption. CBP last tested the AFI contingency plan in April 2014. The results of the test revealed that CBP could not restore system functionality by following the procedures outlined in the contingency plan. Specifically, CBP could not restore functionality to AFI servers at the alternate processing site or necessary connections to other applications and databases.

According to TASPD, the recovery team was unable to implement the contingency plan as written because the infrastructure at the alternate processing site is not correctly identified in the plan. Specifically, the AFI

alternate processing location is currently established as a cold site.[4] However, according to AFI's contingency plan, the alternate processing facility is a hot site, and there is a mirrored and real-time updating capability between the primary and alternate sites with the goal of recovering mainframe data production within 4 hours of a disaster occurring.[5] CBP does not consider restoring AFI operations following a service disruption as a high priority because AFI is not a mission essential system. As a result, TASPD does not intend to deploy the restoration capabilities as described in the contingency plan.

Because CBP assigned AFI with a "moderate" impact level for availability, we believe that a service disruption could have a serious adverse effect on CBP's operations. Continuing to regularly review and update the contingency plan can help CBP ensure that accurate information is documented and restoration procedures are revised, as required.

Both DHS and NIST recommend that contingency plans be tested to determine plan effectiveness and organizational readiness to execute recovery procedures, evaluate test results, and initiate corrective actions, as needed. Further, problems encountered during contingency plan implementation or testing can be addressed through periodic contingency plan updates.

Contingency planning is designed to mitigate the risk of service disruptions and improve system availability. Because contingency planning requirements may change as systems evolve to meet mission needs, contingency plans will not be effective unless they are regularly reviewed and updated to ensure that new information is documented and contingency measures are revised if required.

Recommendation

We recommend the Assistant Commissioner and Chief Information Officer:

Recommendation 6: Update the AFI contingency plan to accurately reflect planned recovery strategies and capabilities.

---

[4] A cold site is a backup facility that has the necessary electrical and physical components of a computer facility, but does not have equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the system has to move from its main computing location to an alternate site. Recovery at a cold site could take several days to weeks to complete.

[5] A hot site is a fully operational offsite data processing facility equipped with hardware and software to be used in the event of a system disruption. Mirroring refers to a fully redundant facility with automated real-time information that is identical to the primary site.

CBP Comments to Recommendation 6

CBP concurred with recommendation 6. The AFI contingency plan was updated to accurately reflect the planned recovery strategies; however, updates in the DHS Information Assurance and Compliance System tool could not occur until the AFI self-assessment period began. The DHS Information Assurance and Compliance System tool prevents updates until the annual self-assessment period just prior to the authority-to-operate anniversary date. The AFI annual self-assessment was due and completed on April 8, 2015. Supporting documentation for closure of the recommendation will be provided to the OIG under separate cover. CBP respectfully requests that the OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the steps that CBP has taken satisfy the intent of this recommendation. Based on our review of the supporting documentation provided, we consider this recommendation closed and resolved.

CBP Has Not Addressed AFI Contingency Planning Deficiencies in a POA&M

CBP has not incorporated all known information security weaknesses in a POA&M process, as required by applicable DHS, Office of Management and Budget, and NIST guidance.[6] TASPD maintains the AFI POA&M and updates it as needed, with the most recent update occurring in July 2014. However, despite assigning AFI a "moderate" impact level for availability, TASPD management officials did not create a POA&M to address contingency planning deficiencies identified after the April 2014 exercise because the contingency plan was regularly updated throughout the year.

DHS and the Office of Management and Budget require that POA&Ms be created and maintained for all known information security weaknesses. DHS requires that POA&Ms be created, tracked, managed, and updated for all known information security weaknesses and entered into DHS' enterprise management tools and reviewed monthly.

POA&Ms are key documents in the security authorization packages for information systems. When POA&Ms are not created and maintained properly,

[6] A POA&M is a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for accomplishing the tasks, and scheduled completion dates for the milestones.

authorizing officials may not have the most accurate information to make credible risk-based decisions about AFI. In addition, authorization officials cannot ensure that all information security weaknesses have been identified and mitigated in accordance with applicable guidance.

Recommendation

We recommend the Assistant Commissioner and Chief Information Officer:

Recommendation 7: Update the AFI POA&M to include all known information security weaknesses.

CBP Comments to Recommendation 7

CBP concurred with recommendation 7. All AFI POAMs are up to date according to *Federal Information Security Management Act* reporting requirements as of May 20, 2015. Supporting documentation for closure of the recommendation will be provided to the OIG under separate cover. CBP respectfully requests that the OIG consider this recommendation resolved and closed.

OIG Analysis

We agree that the steps that CBP has taken satisfy the intent of this recommendation. Based on our review of the supporting documentation provided, we consider this recommendation closed and resolved.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objective of our audit was to determine the implementation status of AFI and whether effective controls have been implemented to protect the sensitive information processed and stored by the system from unauthorized access. Specifically, we determined whether CBP had deployed AFI on schedule and within budget, and implemented effective technical security controls to protect the sensitive information it processes and stores. We also determined whether AFI complies with DHS information security program requirements.

Our audit focused on the requirements specified in the *DHS Sensitive Systems Handbook 4300A*, DHS Oracle configuration guidance, DHS Redhat Linux configuration guidance, DHS Windows 2008 configuration guidance, and *Federal Information Security Management Act*. To accomplish our objective, we interviewed selected personnel and management officials from the Office of Information and Technology and performed field work at offices in the Washington, DC, area. We reviewed DHS policies and procedures for securing servers and virtual machines and protecting the privacy of information processed and stored by information technology systems. We evaluated CBP's compliance with DHS' information security program for AFI in the areas of risk assessments, security control assessments, contingency planning, training, POA&Ms, and continuous monitoring. Finally, we performed vulnerability assessments to evaluate the effectiveness of controls implemented on AFI.

We conducted this performance audit between January and March 2015 pursuant to the *Inspector General Act of 1978*, as amended, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

AUG 0 3 2015

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

FROM: Eugene H. Schied
Assistant Commissioner

SUBJECT: CBP Response to OIG Draft Report – Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence

Thank you for the opportunity to review and comment on the Department of Homeland Security (DHS), Office of the Inspector General (OIG) draft report entitled, "Enhancements to Technical Controls Can Improve the Security of CBP's Analytical Framework for Intelligence," (job code 15-012-ITA-CBP). U.S. Customs and Border Protection (CBP) appreciates OIG's work in planning and conducting its review and issuing this report.

We are pleased to note OIG's recognition that CBP has made significant progress in implementing the Analytical Framework for Intelligence (AFI). As indicated, CBP fully deployed AFI on schedule and within budget, and has taken measures to secure from unauthorized access, the sensitive information the system processes and stores. In addition, CBP developed a privacy impact assessment to ensure that privacy considerations for operating AFI were addressed throughout system deployment. Since deployment, system users have provided positive feedback to CBP about AFI's functionality and usefulness. CBP is committed to securing the AFI system and implementing security controls to avoid the risk of inadvertent information disclosures and service disruptions.

The report contained seven recommendations to which CBP concurred. Below CBP requests closure of all seven recommendations and provides the corrective actions we have taken:

Recommendation 1: Implement strong passwords on AFI databases in accordance with applicable Department of Homeland Security and CBP requirements.

Response: Concur. The accounts that were identified as having weak passwords were locked. AFI databases require strong passwords as a requirement. The CBP, Office of Information and Technology (OIT) has implemented a password verify function on all database profiles. The users are assigned to profiles, and therefore all users and accounts are accounted for. Within the verify function, the DHS complex password requirements are enforced. Supporting documentation was previously provided to the OIG. CBP respectfully requests that OIG consider this recommendation resolved and closed.

Recommendation 2: Restrict permissions granted to the public role on AFI databases.

Response: Concur. The permissions granted to the public role are locked down. Only authorized database administrators have the ability to access the database directly and AFI is only accessible on the CBP intranet which is not accessible by the general public. Supporting documentation was previously provided to the OIG. CBP respectfully requests that OIG consider this recommendation resolved and closed.

Recommendation 3: Implement configuration controls on the AFI browser-based application to prevent exploitation through cross-frame scripting.

Response: Concur. AFI plan of action and milestones (POA&M) 42, which addressed the cross-frame scripting vulnerability was remediated on May 14, 2015. The CBP, OIT, Targeting and Analysis Systems Program Directorate performed an ad-hoc WebInspect scan which showed no cross-frame scripting vulnerabilities on the AFI browser-based application. That artifact was uploaded into the Information Assurance Compliance System (IACS) as an artifact to close out the POA&M. The full results of the WebInspect scan is uploaded in IACS to prove closure for AFI POA&M 42. Supporting documentation for closure of the recommendation will be provided to OIG under separate cover. CBP respectfully requests that OIG consider this recommendation resolved and closed.

Recommendation 4: Implement a secure encryption algorithm for all AFI network traffic.

Response: Concur. AFI POA&M 43, which addresses weak encryption algorithms was remediated on May 20, 2015. AFI only permits strong encryption algorithms. The AFI Information Systems Security Officer also created a security report to monitor the cipher suites used to log into AFI, to ensure that no weak algorithms are permitted. Supporting documentation for closure of the recommendation will be provided to OIG under separate cover. CBP respectfully requests that OIG consider this recommendation resolved and closed.

Recommendation 5: Remove shared administrator accounts and assign administrator access based on the principles of least privilege.

Response: Concur. AFI revisited best practices of minimizing service accounts and assigning administrator access based on the principles of least privilege. There are a small number of AFI administrators dedicated to the AFI program who perform application specific operation and maintenance functions. CBP has removed administrative access from the additional administrators who were granted access to manage AFI as one of many enterprise assets. Supporting documentation for closure of the recommendation will be provided to OIG under separate cover. CBP respectfully requests that OIG consider this recommendation resolved and closed.

Recommendation 6: Update the AFI contingency plan to accurately reflect planned recovery strategies and capabilities.

Response: Concur. The AFI contingency plan was updated to accurately reflect the planned recovery strategies; however, updates in the DHS IACS tool could not occur until the AFI self-assessment period began. The DHS IACS tool prevents updates until the annual self-assessment period just prior to the Authority to Operate anniversary date. The AFI annual self-assessment was due and completed on April 8, 2015. Supporting documentation for closure of the recommendation will be provided to OIG under separate cover. CBP respectfully requests that OIG consider this recommendation resolved and closed.

Recommendation 7: Update the AFI POA&M to include all known information security weaknesses.

Response: Concur. All AFI POAMs are up to date according to Federal Information Security Management Act reporting requirements as of May 20, 2015. Supporting documentation for closure of the recommendation will be provided to OIG under separate cover. CBP respectfully requests that OIG consider this recommendation resolved and closed.

CBP remains committed to improving its program effectiveness and looks forward to working with you on future homeland security matters. Technical and sensitivity comments will be provided under separate cover.

If you have any questions, or would like additional information, please contact me at (202) 344-2300, or have a member of your staff contact Ms. Patricia Quintana, CBP Audit Liaison, Management Inspections Division at (202) 325-7711.

Attachment

Appendix C
Office of IT Audits Major Contributors to This Report

Chiu-Tong Tsang, Director
Mike Horton, IT Officer
Bridget Glazier, Team Lead
David Bunning, IT Specialist
Pachern Thapanawat, IT Auditor
Charles Twitty, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commissioner, CBP
Chief Information Security Officer, DHS
Chief Information Officer, CBP
Executive Director, Targeting and Analysis Program Directorate, CBP
Deputy Executive Director, Targeting and Analysis Program Directorate, CBP
Audit Liaison, CBP

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305