Department of Homeland Security
Office of Inspector General

U.S. Customs and Border Protection Has Taken Steps To Address Insider Threat, but Challenges Remain

(Redacted)

OIG-13-118

September 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 9, 2013

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

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *U.S. Customs and Border Protection Has Taken Steps To Address Insider Threat, but Challenges Remain*

Attached for your action is our final report, *U.S. Customs and Border Protection Has Taken Steps To Address Insider Threat, but Challenges Remain.* We incorporated the formal comments from the U.S. Customs and Border Protection (CBP) in the final report.

The report contains four recommendations aimed at improving CBP's insider threat program. Your office concurred with all of the recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate 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 Richard Saunders, Director, Advanced Technology Division, at (202) 254-5440.

Attachment

Table of Contents

Appendixes

Abbreviations

CBP	U.S. Customs and Border Protection
CERT	Computer Emergency Response Team
DHS	Department of Homeland Security
DLP	data loss prevention
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards Publications
IA	Internal Affairs
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
ITWG	Insider Threat Working Group
JIC	Joint Intake Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
SOC	Security Operations Center
[redacted]	[redacted]

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Executive Summary

We reviewed the efforts of U.S. Customs and Border Protection (CBP) to address the risk posed by trusted insiders. Our objective was to assess CBP's progress toward protecting its information technology assets from threats posed by its employees, especially those with trusted or elevated access to sensitive information systems or data.

CBP has made progress in addressing the risk of insider threats across the organization. Specifically, CBP established a working group and a committee focused on the risk. Further, CBP researches employee behavior, conducts pre-employment screening including polygraph assessments, and participates in border corruption task forces with the Federal Bureau of Investigation. Also, CBP established a Joint Intake Center and Security Operations Center to centrally identify, monitor, and respond to potential insider threat risks or incidents in information systems and networks. While these efforts have resulted in some improvements, CBP has opportunities to improve its security posture against threats posed by employees and contractors.

CBP can establish a framework to further strengthen its insider threat program by implementing policies and procedures that integrate the requirements, standards, and guidance provided by the administration, Department of Homeland Security, and the National Institute of Standards and Technology. In addition, CBP could implement a risk management plan that identifies the broad spectrum of insider threat risks facing CBP and how these risks could be mitigated. The plan will help ensure that the entire agency is risk aware and that the risk is consistently and continually addressed. Furthermore, the current security and awareness training program should be expanded to include insider threat-based training for all agency employees.

Finally, CBP can strengthen the technical processes and controls for its technology infrastructure by applying critical security patches on information systems, reducing the use of unauthorized portable media devices, detecting or even preventing the exfiltration of sensitive information through email applications, and conducting periodic onsite vulnerability wireless security scans and assessments.

We are making four recommendations that, if implemented, should strengthen CBP's management of the threat posed by trusted insiders. CBP concurred with all of the recommendations.

Background

CBP's primary mission is to prevent terrorists and terrorist weapons from entering the United States and to ensure the security of our Nation's borders and ports of entry. As the largest law enforcement agency in the United States, CBP currently has more than 58,000 employees serving nationwide and internationally. These employees include air and marine interdiction agents and enforcement officers, border patrol agents, field operations officers, agriculture specialists, and mission support personnel. From October 1, 2004 to September 30, 2011, 132 CBP employees were arrested or indicted for corruption-related activities. These employees were trusted insiders who had been vetted and cleared by personnel security procedures. They deliberately misused their positions for personal gain by misusing government computer systems, passing sensitive information, stealing money and property, or deliberately circumventing operational procedures. Such actions are a threat to the morale and safety of CBP employees and contractors, the agency's mission, and national security.

According to CBP officials, a malicious insider could do the most harm to CBP in the following areas:

- Unauthorized use or disclosure or modification of information from databases (classified and unclassified), operational information (e.g., manpower surges and operational technology), or operational activity (e.g., sensitive operations);
- Disruption of critical information technology (IT) networks; and
- Border security breaches (e.g., corrupt employees who facilitate the flow of illegal drugs and aliens into the United States and disclose sensor locations and gate codes).

Based on designated job functions or status within the organization, trusted insiders are typically given unfettered or elevated access to mission critical assets. Therefore, they may be thoroughly familiar with internal policies and procedures, electronic building access systems used for physical security, and technical access controls (such as firewalls and intrusion detection systems) used for information security. As a result, employees may also be aware of weaknesses in organizational policies and procedures, as well as physical and technical vulnerabilities in computer networks and information systems. This institutional knowledge poses a continual risk to the organization because in the wrong hands it could be used to facilitate malicious attacks and even collusion with external attackers.

Because of CBP's sensitive mission, any unauthorized disclosure of sensitive information could adversely affect the security of its information systems, assets, resources, employees, and the general public. As a result, the agency must be constantly aware of any adversary, especially those with sophisticated expertise and significant resources to create opportunities for multiple attacks. CBP could be attacked through footholds in the IT infrastructure to steal or destroy information or undermine or impede mission critical assets. Adversaries can carry out any number of attacks at any time through breaches, creating a persistent threat.

Since 2001, the Computer Emergency Response Team (CERT) Insider Threat Center of the Software Engineering Institute at Carnegie Mellon University has researched and gathered data about malicious insider acts, including IT sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to our Nation's critical infrastructures. CERT has researched approximately 400 insider threat cases, including fraud, sabotage, and theft of intellectual property. All of these cases were prosecuted within the United States.

CERT defines a malicious insider as any current or former employee, contractor, or business partner who:

- Has or had authorized access to an organization's network, system, or data; and
- Has intentionally exceeded or intentionally used that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.[1]

CERT has collaborated with U.S. Secret Service behavioral psychologists to collect approximately 150 actual insider threat cases that occurred in U.S. critical infrastructure sectors between 1996 and 2002. Each was examined from a technical and behavioral perspective. CERT's research helped them to develop best practices that provide a framework for establishing an insider threat program within an organization. In

[1] Carnegie Mellon University Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats* (4th Edition).

addition, CERT devised a list of defensive measures that could help detect or prevent insider attacks. For example, CERT recommends that organizations:

- Include insider threat as part of an enterprise-wide risk assessment;
- Conduct a security awareness campaign to ensure that the insider threat is understood across the organization;
- Develop and clearly define organizational policies relevant to the insider threat, enforcing those policies consistently and fairly; and
- Secure both the physical and electronic environment, including account and password management, separation of duties, controls for the software development process, change controls, remote access, and privileged user accounts, especially those used by system administrators.

Executive Order 13587 – *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, issued in 2011, requires agencies that operate or access classified computer networks to implement an insider threat detection program consistent with guidance and standards developed by an interagency, government-wide insider threat task force. Agencies, such as CBP, will be responsible for implementing an insider threat detection and prevention program consistent with guidance and standards developed by the task force. Further, in November 2012, the administration announced the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* that provides direction and guidance to promote the development of effective insider threat programs within departments and agencies.

The initial public draft of National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, includes new requirements for agencies to address the risk posed by the insider threat. NIST anticipated releasing this final publication in April 2013. Federal agencies will have up to 1 year from the release of the final publication to comply with the new requirements.

Results of Audit

CBP Has Taken Steps To Address and Mitigate the Risk of Insider Threats

CBP has made progress in addressing the risk of insider threats across the organization. The agency established an Insider Threat Working Group (ITWG) and Integrity Integrated Planning and Coordination Committee (Integrity IPCC). CBP also researches employee behavior, conducts pre-employment screening including polygraph assessments, and participates in border corruption task forces with the Federal Bureau of Investigation (FBI). Additionally, CBP established a Joint Intake Center and Security Operations Center to centrally identify, monitor, and respond to potential insider threat risks or incidents in information systems and networks. Together, these steps provide opportunities for CBP to improve its security posture against the threat posed by employees and contractors. This includes decreasing the likelihood of unauthorized disclosure, modification, theft, or destruction of sensitive information or disruption of critical information technology networks and services, and increasing the likelihood of detecting and responding to computer security incidents and breaches, especially those at critical sites such as field offices along the U.S. borders.

Insider Threat Working Group

In January 2012, CBP established the ITWG to review existing insider threat mitigation efforts and establish a cohesive, responsive, and robust insider threat program. The ITWG included agency personnel from various offices, including the Office of Internal Affairs (IA), Office of Information and Technology (OIT), and Office of Intelligence and Investigative Liaison. The group's primary objectives were to:

- Review CBP security policy and revise as needed;
- Create and update training for employees;
- Draft an insider threat working group charter;
- Examine insider threat detection tools and capabilities; and
- Formulate incident reporting protocols.

In April 2012, CBP suspended the ITWG while awaiting guidance from the Department of Homeland Security (DHS) based on the administration's *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* and the *DHS Insider Threat Policy and Minimum Standards*. At the time of our audit, CBP had not formally approved any insider threat-specific policies and procedures to further develop the program.

Integrity Integrated Planning and Coordination Committee

According to IA, drug trafficking organizations have been seeking to infiltrate CBP and actively recruit CBP employees to help them carry out unlawful activities. Examples of insider threat related corruption includes such offenses as alien smuggling, allowing loads of narcotics through a port of entry or checkpoint, providing sensitive information to a drug trafficking organization, selling immigration documents, or circumventing CBP's detection systems. Trusted CBP employees have been arrested or indicted for corrupt acts that involved their abuse of their knowledge, access, or authority granted by virtue of their official position.

To address the corruption and misconduct in CBP's workforce, in 2011, CBP created the Integrity IPCC to facilitate ongoing integrity-related operations of individual offices within CBP. This committee is responsible for ensuring that CBP fully implements integrity-related initiatives. Through this collaborative effort, committee members, including internal CBP offices and external law enforcement partners, discuss integrity-related issues, ideas, and best practices.

The committee reviewed and evaluated recommendations from the Homeland Security Studies and Analysis Institute's December 2011 study, including recommendations on integrity-related areas such as:

- CBP operational and organizational structure;
- Employee recruitment and vetting process;
- Integrity training process and programs;
- Metrics and information sharing; and
- Prevention, detection, monitoring, and investigative programs and initiatives.

CBP made progress in complying with the institute's recommendations, some of which are directly applicable to an insider threat program. For example, CBP implemented polygraph testing of all law enforcement officer applicants that could identify potential behavior issues and insider threat risks before being hired. The polygraph exam includes questions on topics including espionage, sabotage, terrorism, unauthorized disclosure of classified information, unreported foreign contacts, and deliberate damage to or malicious misuse of U.S. Government information or defense systems. CBP is also developing an integrity-related communications strategy for CBP employees that would help reinforce professional conduct, integrity, and ethical behavior.

CBP has a comprehensive integrity strategy that may identify a potential insider threat risk. The strategy includes a thorough initial screening of applicants, pre-employment polygraph examinations of law enforcement candidates, and an extensive background investigation that commences upon the initial selection of a prospective employee. Periodic reinvestigations of an employee's background are conducted every 5 years and may identify emerging integrity, conduct, and insider threat concerns that have the potential to affect the CBP mission.

Behavioral Research

The Behavioral Research Branch provides situational awareness to CBP executives on CBP employee activities, such as the insider threat risk, and to identify potential insider threat risks over a period of time. The purpose of the research is to understand how and why employees are engaged in corruption and to provide data-driven research for personnel security, analysts, investigators, and supervisors. This will help ensure that CBP's prevention, detection, and investigative efforts are grounded in scientific evaluation of known corruption cases.

The Behavioral Research Branch maintains a database of all incidents of employee delinquency including arrests, indictments, citations, and detainments for violations of law reported to the Joint Intake Center between fiscal year 2005 and the present. The branch routinely analyzes information in the employee delinquency database and produces weekly status reports for the IA Assistant Commissioner. The branch also provides monthly status reports to the CBP

Commissioner's office and the IA Assistant Commissioner. Although it did not send weekly or monthly reports to any external entities, the branch also responds to ad hoc requests for information from the media and Congress.

To understand how and why employees engage in corrupt activities, the Behavior Research Branch also examined cases of known CBP employees arrested and convicted of such activities between fiscal years 2005 and 2011. This research and analysis is being used to understand the effect that certain policies had on misconduct and corruption in CBP.

The Behavioral Research Branch also produced interim reports that include information on corruption in CBP, background investigations, and periodic reinvestigations. The branch concluded that CBP-wide steps should be taken to reduce corrupt activity.

Anti-Border Corruption Act Requirements

The *Anti-Border Corruption Act of 2010* requires CBP to implement integrity-related controls to prevent and detect potential insider threat risks, such as employee misconduct and corruption.[2] According to the act, by January 2013, all CBP law enforcement applicants must pass a polygraph examination before being hired. The law further requires that CBP initiate all periodic personnel reinvestigations and report to Congress every 6 months on its progress toward meeting these requirements by January 2013.

CBP's pre-employment polygraph examinations of law enforcement applicants and background investigations can thoroughly vet individuals who are seeking employment with, or employed by, CBP. As of January 2013, CBP had met the requirements of the act, including administering polygraph exams for all new law enforcement applicants.

CBP also developed a periodic polygraph examination customized to address CBP's mission-specific and insider threat risks. According to the Credibility Assessment Division, the polygraph is a proven technique used in the intelligence community to mitigate insider threat risk. The examination combines

[2] Public Law 111-376.

techniques used by the FBI, Defense Intelligence Agency, and Central Intelligence Agency, as well as the National Center for Credibility Assessment's standards and best practices. CBP began a pilot study, endorsed by the center, to confirm the validity and reliability of this new examination procedure.

In July 2012, IA developed a plan that identified the risk of corruption in non-law enforcement positions and the need to expand Office of Personnel Management requirements for pre-employment polygraphs to other critical, sensitive positions. These critical positions include agriculture specialists, import specialists, seized property specialists, intelligence analysts, OIT personnel, and certain personnel assigned internationally.

According to CBP officials, certain OIT personnel, specifically system and database administrators, could have the greatest potential negative effect on national security than any other positions in CBP. Based upon assigned job duties, these employees are typically given the highest level of access to information systems under their purview. Given that they possess the knowledge and ability to safeguard these systems, they also possess institutional knowledge to know whether and where critical systems vulnerabilities might exist, and how to best exploit those vulnerabilities.

There is an advanced persistent threat that CBP must protect itself against. This comes from CBP's employees and contractors responsible for safeguarding and protecting its own IT assets. Significant harm to CBP's information systems and operations could occur through unauthorized modification of hardware or software, unauthorized modification of system logs to conceal harmful activity on IT assets, planting viruses and logic bombs to destroy or covertly remove sensitive information, or creating backdoor system accounts that could be used to facilitate future attacks. Successfully carrying out any one of these activities could result in significant loss, theft, or destruction of mission sensitive information. This in turn could have adverse effects on the organization internally or externally through negative publicity and the potential loss of public confidence in the organization.

Border Corruption Initiatives

CBP implemented a number of border corruption initiatives that may identify insider threat risks within CBP. In June 2010, CBP IA signed a memorandum of understanding with the FBI delineating the responsibilities of the National Border Corruption Task Force participants, designed to maximize inter-agency cooperation and formalize relationships between the participating agencies for policy guidance, planning, training, and public and media relations. These multi-jurisdictional and multi-agency task forces share information, intelligence, and investigative resources in an effort to combat workforce corruption. Twenty-eight full time IA agents participate on 22 FBI-led Border or Public Corruption Task Forces. As of August 2012, IA was working on approximately 121 cases under the auspices of these Border or Public Corruption Task Forces.

In addition, the FBI's National Border Corruption Task Force at its headquarters oversaw national investigative efforts and gathered operational information and tactical and strategic intelligence related to border corruption issues. As a result, several instances of CBP employee corruption were uncovered, investigated, and adjudicated.

Counterintelligence Operations and Liaison Initiatives

To protect against illicit foreign intelligence services and transnational criminal organizations, the Counterintelligence Operations and Liaison Group established procedures and training for CBP employees within the United States and while on official or non-official travel outside the United States. Trusted employees could be targeted by foreign entities and criminal organizations to obtain sensitive information about CBP's operations and activities.

The group reviews foreign travel by employees, shares information with intelligence community partners, and conducts counterintelligence awareness training that includes information about espionage indicators and reporting of suspicious activity. Counterintelligence awareness training was designed for CBP personnel who may be targeted by foreign intelligence services and transnational criminal organizations while traveling abroad officially or non-officially.

In addition to its international travel-related activities, the group initiated "Project Red Flag," which includes representatives from IA divisions, and identifies potential insider threat risks; chaired the ITWG and is the point of contact for the DHS Intelligence and Analysis' ITWG; and attends intelligence community insider threat seminars, conferences, and meetings.

Joint Intake Center

In March 2004, CBP and U.S. Immigration and Customs Enforcement (ICE) formed the Joint Intake Center (JIC) for the receipt and processing of allegations of misconduct and other reported incidents (including potential insider threat risks or incidents in information systems and networks) involving personnel and contractors employed by both agencies. Establishment of the JIC helped ensure the integrity and professionalism of the CBP and ICE workforces through the creation of an effective allegation referral process and the establishment of reporting and tracking processes that guarantee accountability throughout both organizations.

The JIC provides both agencies with a centralized, collaborative, and uniform system for processing incident reports and alleged misconduct including criminal activity that violates State or Federal criminal laws, such as employee arrests and serious misconduct. The JIC also serves as the conduit to the DHS Office of Inspector General (OIG). The OIG retains the "right of first refusal" on all allegations of misconduct involving DHS personnel and contractors. The OIG accepts certain allegations for investigation; those that are not accepted are referred back to the JIC for investigation, fact finding, or immediate action by CBP or ICE management.

In addition, the JIC maintains a CBP internal website, "Trust Betrayed," which presents examples of criminal misconduct by CBP employees. These examples remind employees of the personal and professional costs associated with integrity misconduct.

DHS Security Operations Center and CBP Office of Information and Technology

To improve identification of suspicious insider activity, the DHS Security Operations Center (SOC) monitors computer networks and information systems and data on a day-to-day basis. According to CERT research, monitoring and logging employees' behavior while they are using government-issued computers or network resources helps to better identify suspicious insider activity before a serious breach of security can occur. SOC activities include analyzing computer system security event logs and responding to computer security incidents as needed.

OIT also has programs and processes designed to detect unauthorized insider threat actions that, if left unchecked, could pose as a serious threat to CBP's mission and security. These programs and processes included the following:

- Monitoring the DHS external Internet connections using data loss prevention technology to facilitate identifying sensitive information exfiltration;
- Monitoring secure remote access connections to CBP IT assets to detect anomalous authentication attempts from external DHS sites in order to respond to these attempts;
- Blocking access to non-DHS Internet webmail sites on CBP IT assets. As a result, CBP employees cannot access webmail sites such as Gmail, Hotmail, and Yahoo, which a malicious insider could use to transfer sensitive and unauthorized information;
- Establishing a program to help ensure that only authorized modifications to IT systems are executed;
- Separating application developers' duties to ensure that one individual cannot modify code and push it to production systems; and
- Establishing the Computer Security Incident Response Center as a single location for employees to report security incidents, such as suspicious events or unauthorized actions. Incidents reported to the SOC are in turn reported to the U.S. Computer Emergency Readiness Team and other applicable stakeholders, such as the DHS Privacy Office, the DHS Chief Information Officer, and the DHS Chief Information Security Officer.

Although CBP has taken actions to mitigate some of the risks associated with the insider threat, challenges remain in addressing the threat holistically with regards to program, management, and technical aspects of daily operations.

Challenges Remain in Implementing a Robust Insider Threat Program

CBP can establish a framework to further strengthen its insider threat program by implementing policies and procedures that integrate the requirements, standards, and guidance provided by the administration, DHS, and NIST. In addition, CBP could implement a risk management plan that identifies the broad spectrum of insider threat risks facing CBP and how these risks could be mitigated. The plan will help ensure that the entire agency is risk aware and that the risk is consistently and continually addressed. Furthermore, the current security and awareness training program should be expanded to include insider threat-based training for all agency employees. Finally, CBP can strengthen the technical processes and controls for its technology infrastructure by applying critical security patches on information systems, reducing the use of unauthorized portable media devices, detecting or even preventing the exfiltration of sensitive information through email applications, and conducting periodic onsite vulnerability wireless security scans and assessments.

Insider Threat Program and Risk Management Plan

CBP recognizes the need for a centralized, coordinated insider threat program, but has not fully established one agency-wide. An insider threat program should include developing and implementing agency-wide insider threat specific policies and procedures that provide a consistent and clear message to employees regarding their roles and responsibilities for mitigating the insider threat risk. These policies and procedures should integrate the requirements, standards, and guidance provided by the administration, DHS, and NIST.[3]

[3] Requirements, standards, and guidance referred to include: Executive Order 13587 – *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*; *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*; December 2012 draft of the *DHS Insider Threat Policy and Minimum Standards*; and the initial public draft of NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* The CERT Insider Threat Center of the Software Engineering Institute at Carnegie Mellon University has developed best practices that provide a framework for establishing an insider threat program within an organization.

As discussed earlier, the ITWG is responsible for developing such an agency-wide program, but it suspended its activities in April 2012 and is waiting to incorporate DHS policies and guidance into its Insider Threat Detection Program directive. Once approved, this directive will reestablish the ITWG, make agency participation mandatory, and articulate participant roles and responsibilities.

CERT recommends that large organizations, such as CBP, formalize an insider threat program that can monitor and respond to insider threats. This would require establishing policies and procedures for addressing insider threat that require participation from human resources, legal, physical and personnel security, management, and IT. The administration's *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* would provide CBP direction and guidance on developing an agency-wide insider threat program. Further, the initial public draft of NIST Special Publication 800-53, Revision 4 recommends that organizations develop an insider threat program with clearly defined policies and consistent enforcement of these policies to achieve maximum effectiveness.

Finally, as part of the implementation of a formal insider threat program, CBP needs to develop and implement a risk management plan that identifies the broad spectrum of insider threat risks facing CBP and how these risks could be mitigated. A plan would provide a framework to identify mission critical data, business processes, and information systems and a road map to implement appropriate security measures and controls to help counteract the insider threat. Furthermore, a plan should include a provision for periodic evaluation of the security categorization (e.g., low, moderate, or high) assigned to each information system per Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* to determine if each categorization is commensurate with the potential threat impact for each system.

According to CERT, hindrances to risk management and communications throughout organizations may contribute to losses from insider threats. Implementing a risk management plan would help ensure that all employees are aware of and addressing risk consistently and continually across the enterprise.

Expand Employee Training and Awareness to Include the Insider Threat Risk

CBP does not have an agency-wide required training and awareness program that addresses the insider threat. According to the Office of Training and Development, CBP does not have training that covers potential insider threat indicators among the CBP workforce. Further, CBP does not provide insider threat awareness briefings to all CBP employees. As a result, CBP employees may not have the knowledge to recognize insider threat behavior, adversaries' methods for recruiting insiders, and the appropriate process to report potential insider threats or actual attacks.

CERT recommends that insider threat awareness should be incorporated into periodic security training for all employees. The December 2012 draft of the *DHS Insider Threat Policy and Minimum Standards* and the initial public draft of NIST Special Publication 800-53, Revision 4 both recommend that organizations provide awareness training on recognizing and reporting potential indicators of insider threat.

Although CBP employees received training in courses related to insider threat, the agency had not yet fully developed insider threat-specific training. CBP currently requires all employees to complete annual integrity awareness and IT security awareness training. CBP can incorporate CERT recommendations concerning insider threat awareness into both of these annual training requirements.

Security Controls and Processes for Information Technology Assets and Operations

The *DHS 4300A Sensitive Systems Handbook*, *CBP Information Systems Security Policies and Procedures Handbook*, NIST Special Publication 800-53, and FIPS provide guidance and requirements on periodically assessing system risk and applying the required technical security controls. The process of accurately assigning a risk level to an information system and properly applying the required minimum security controls is critical to mitigating organizations' insider threat risk. Diligently applying these controls could reduce the likelihood of a breach or attack by increasing the degree of difficulty, level of effort, or knowledge required to carry out harmful activities.

CBP needs to improve its implementation of the required security controls and processes for IT assets and operations by applying critical security patches, reducing the use of unauthorized portable media devices, preventing exfiltration of sensitive information through email, and conducting onsite vulnerability wireless security scans and assessments.

More Timely Application of Critical [redacted] Security Patches

CBP has not fully implemented security patches for known [redacted] vulnerabilities on IT assets.[4] [redacted] used programming language in system applications and programs. By not implementing these patches, CBP is increasing the likelihood that vulnerabilities could be exploited by an attacker to compromise the confidentiality, integrity, or availability of any IT system that is not properly patched. CERT case studies have shown that malicious insiders will sometimes exploit known technical security vulnerabilities to obtain system access and carry out an attack. Failure to address known vulnerabilities, such as [redacted], in a timely manner provides an insider increased opportunity to carry out such an attack.

We conducted network security scans of 206,000 CBP IT assets and confirmed the existence of the [redacted] patch vulnerabilities at all geographical locations visited. According to a DHS SOC official, CBP has an estimated [redacted] related vulnerabilities in its IT assets that had not been patched. According to CBP officials, these patches have not been implemented largely because many of CBP's system applications are not compatible with newer versions of [redacted].

According to the *DHS 4300A Sensitive Systems Handbook*, CBP is required to promptly install security patches. Proactively addressing known security vulnerabilities should be a priority to mitigate the risk of insider threats.

[4] A security patch is an update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Reduce the Potential Use of Unauthorized Portable Media Devices

CBP is not consistently enforcing a practice of allowing only authorized portable media devices, such as [redacted] devices and [redacted] to connect to IT assets. The unauthorized downloading of sensitive information through unapproved storage devices is a constant threat to any organization. Threats of data loss increase when trusted insiders have extensive knowledge of the inner workings of the organization and their level of access allows close proximity to the data source. Malicious insiders can carry out attacks on an organization's information systems and networks through unauthorized leakage and transfer of information through portable media or external storage devices.

Our technical testing demonstrated that [redacted] Also, we determined through [redacted] analysis that unauthorized portable electronic devices, such as [redacted] had been connected to and operating on CBP IT assets from time to time.

The *DHS 4300A Sensitive Systems Handbook* prohibits connecting unauthorized portable electronic devices to the agency network. Further, the handbook prohibits DHS personnel and contractors from using non-government issued removable media devices and connecting them to DHS IT assets.

Prevent the Unauthorized Exfiltration of Sensitive Information Through Email

[redacted] effective controls to monitor, detect, and prevent the unauthorized exfiltration of sensitive or personally identifiable information. During testing, [redacted] These test emails [redacted] multiple locations visited.

[redacted]

[redacted] The DHS Trusted Internet Connection has data loss prevention (DLP) hardware in place to provide coverage for the DHS enterprise email content that includes CBP. The DHS SOC [redacted] According to CBP officials, these devices would be able to assist with the detection of unauthorized exfiltration of sensitive information through government email accounts.

According to CERT, malicious insiders could use email to disseminate sensitive information to competitors or conspirators covertly. The *DHS 4300A Sensitive Systems Handbook* requires CBP to secure and filter all email content. The failure to monitor continually and detect unauthorized exfiltration of sensitive information through email provides a malicious insider ample means and opportunity to carry out such an attack, making it more difficult for an organization to protect itself.

Conduct Vulnerability Wireless Security Scans and Assessments of CBP Sites

CBP does not perform sufficient periodic onsite wireless vulnerability security scans and assessments on its IT infrastructure, including wireless routers, wireless access points, and authorized mobile devices. The process of conducting vulnerability assessments includes checking for unauthorized wireless devices connected to or operating on the CBP network. On a limited basis, the CBP Risk Assessment Team and the CBP Systems Test and Evaluation Team conduct onsite security assessments to identify unauthorized wireless access points.

We performed onsite wireless assessments of critical CBP IT operations at multiple geographical locations. Using specialized security tools, our tests detected and identified the physical presence of unauthorized wireless access points and weak wireless encryption protocols being used within sensitive CBP areas at two locations.

According to SOC officials, [redacted] non-authorized wireless access points from being connected to the CBP network. Performing onsite wireless vulnerability scans could identify or prevent unauthorized devices being connected to the CBP network. Without regular onsite vulnerability assessments of information systems and wireless devices, CBP may not detect malicious wireless activities by a trusted insider.

Recommendations

We recommend that the Assistant Commissioner and Chief Information Officer Office of Information and Technology for CBP:

Recommendation #1:

Establish an agency-wide insider threat program responsible for identifying and remediating the risk posed by the insider threat.

Recommendation #2:

Implement an insider threat training and awareness program for the entire CBP workforce.

Recommendation #3:

Strengthen technical security controls and processes of IT assets and operations including applying critical security patches and preventing use of unauthorized devices and exfiltration of sensitive information.

Recommendation #4:

Perform periodic onsite assessments of CBP sites to identify unauthorized wireless networks and devices connected to the CBP network.

Management Comments and OIG Analysis

We obtained written comments on a draft report from the IA Assistant Commissioner. We have included a copy of the comments, in its entirety, in appendix B. CBP concurred with all of the recommendations.

CBP Comments to Recommendation #1

CBP concurs with recommendation #1. CBP stated that the IA Counterintelligence Operations and Liaison Group (IA-CIOLG) will use the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* and the *DHS Insider Threat Policy and Minimum Standards* to reestablish CBP's ITWG and Insider Threat Detection Program.

IA CIOLG will be naming a full time program manager who will be responsible for reestablishing and further developing the ITWG. The manager will be contacting all pertinent CBP internal partners to bring them together to compose an ITWG charter, policy directive, and implementation plan with specific goals and objectives.

The estimated completion date for this recommendation is November 1, 2013.

OIG Analysis

We agree that the actions being taken satisfy the intent of this recommendation. This recommendation will remain open until CBP provides documentation to support that the planned corrective actions are completed.

CBP Comments to Recommendation #2

CBP concurs with recommendation #2. CBP stated upon reestablishment of the ITWG that insider threat training and awareness will be discussed. The ITWG will establish a subgroup focused on the production of a CBP-wide insider threat training and awareness program. The program will be created in coordination with CBP's Office of Training and Development and in conjunction with any DHS guidance in order to produce a training and awareness program that meets the requirements as stated in the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*. The estimated completion date for this recommendation is November 15, 2013.

OIG Analysis

We agree that the actions being taken satisfy the intent of this recommendation. This recommendation will remain open until CBP provides documentation to support that the planned corrective actions are completed.

CBP Comments to Recommendation #3

CBP concurs with recommendation #3. CBP stated that CBP's OIT will continue to patch system vulnerabilities in a timely manner. Per guidance from the Deputy Assistant Commissioner, OIT will implement security patch updates enterprise wide. OIT will continue to work with the program offices to evaluate the feasibility of implementing a 60-day cycle for implementing patch updates due to the large volume of new releases.

In response to preventing the use of unauthorized devices and exfiltration of sensitive information, CBP has installed a data loss prevention solution on over 64,000 workstation systems and it is operational. CBP continues to work with the vendor to improve the functionality of the blocking software and ensure consistent policy enforcement is in place.

The estimated completion date for this recommendation is October 1, 2013.

OIG Analysis

We agree that the actions being taken satisfy the intent of this recommendation. This recommendation will remain open until CBP provides documentation to support that the planned corrective actions are completed.

CBP Comments to Recommendation #4

CBP concurs with recommendation #4. CBP stated that the Risk Assessment Team under the Security and Technology Branch has been performing and will continue to perform periodic onsite assessments of CBP sites to identify unauthorized wireless networks and devices connected to the CBP network.

CBP plans to provide a report documenting results from Security Risk Assessments, Security Compliance Inspections, and any ad hoc testing for unauthorized wireless access points.

The estimated completion date for this recommendation is December 31, 2013.

OIG Analysis

We agree that the actions being taken satisfy the intent of this recommendation. This recommendation will remain open until CBP provides documentation to support that the planned corrective actions are completed.

Appendix A
Objectives, 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.

Our objective was to assess the progress made toward protecting its IT assets from the threat posed by its employees, especially those with trusted or elevated access to these assets. During the audit, we assessed CBP's:

- Insider threat management process;
- Ability of selected employees to monitor and report suspicious employee behavior;
- Insider threat security policies;
- Insider threat security training and awareness; and
- Selected unclassified information systems critical to the mission of CBP.

We reviewed CBP and DHS policies, procedures, processes, management plans, and wireless network security policies and documents. In addition, the assessment team reviewed system and security logs for unauthorized devices and wireless activities. We interviewed selected SOC, OIT, IA, and CBP personnel and management officials at the following fieldwork locations:

- CBP Headquarters, Washington, DC;
- CBP Joint Intake Center, Washington, DC;
- DHS Security Operations Center, Springfield, VA;
- Boeing Facility, Springfield, VA;
- National Targeting Center – Cargo, Herndon, VA;
- National Targeting Center – Passenger, Reston, VA;
- Washington-Dulles Port of Entry, Sterling, VA;
- CBP Joint Field Command, Tucson, AZ;
- Border Patrol Sector Headquarters, Tucson, AZ;
- Nogales Port of Entry, Nogales, AZ;
- CBP Field Operations Office, San Diego, CA;
- Border Patrol Borstar, Brown Field Airport, San Diego, CA;
- Otay Mesa Port of Entry, Otay Mesa, CA;
- San Ysidro Port of Entry, San Ysidro, CA;
- Air and Maine Operations Center, Riverside, CA;

- Border Patrol Sector Headquarters, Chula Vista, CA;
- Miami Seaport, Cargo and Passenger, Miami, FL; and
- Key West International Airport and Seaport, Key West, FL.

Additional fieldwork was performed through teleconferences or data calls with the Border Patrol Sector Headquarters, Blaine, WA; Caribbean Operations Control Center, Punta Salinas, PR; Border Patrol's International Liaison Office, El Paso, TX; Newark Liberty International Airport, Newark, NJ; and the Elizabeth Seaport, Elizabeth, NJ.

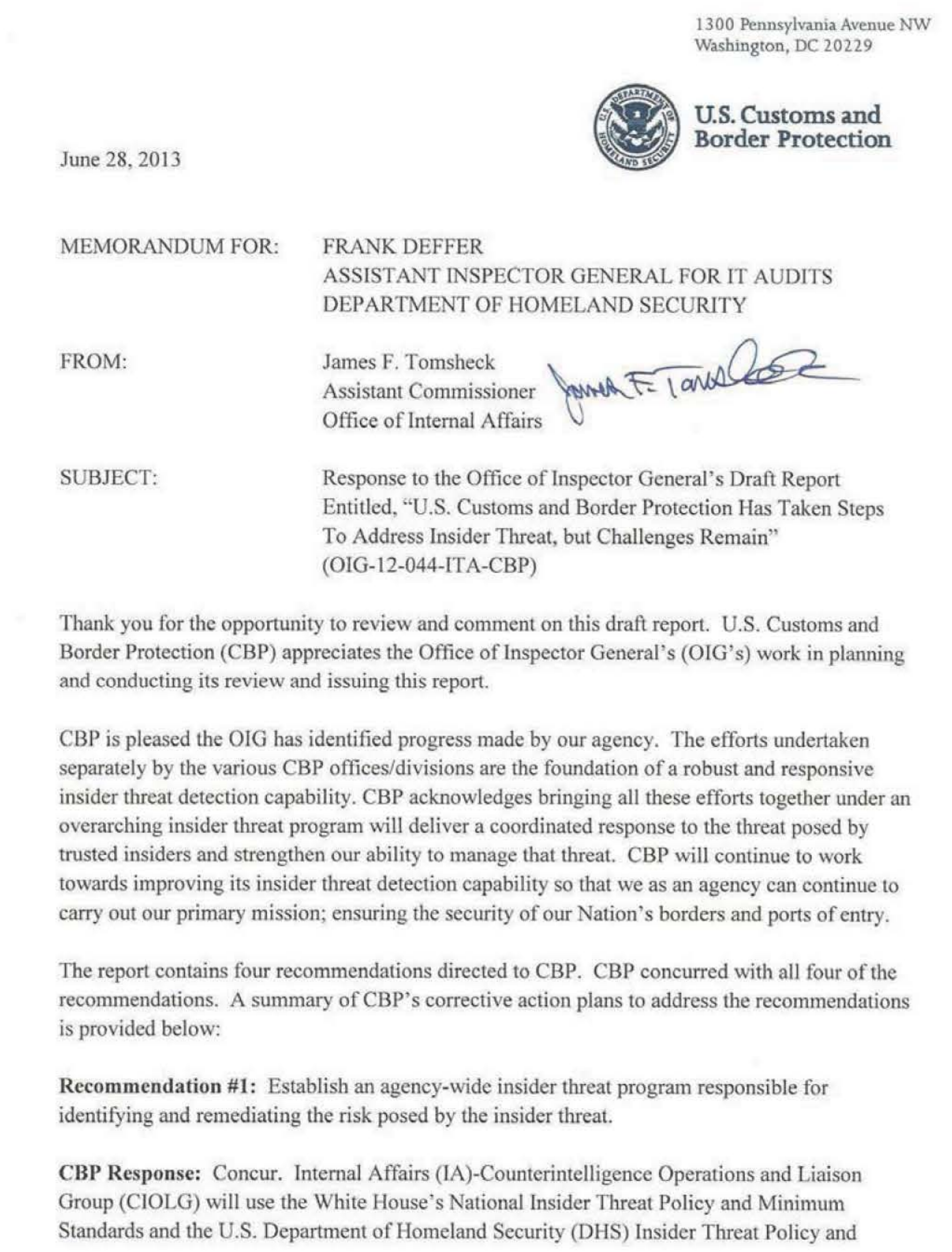
[redacted]

- [redacted]
- [redacted]
- [redacted]

We conducted this performance audit between July 2012 and December 2012 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.

We appreciate CBP's efforts to provide the necessary information and access to accomplish this audit. Major OIG contributors are identified in appendix C.

Appendix B
Management Comments to the Draft Report



1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and
Border Protection

June 28, 2013

MEMORANDUM FOR: FRANK DEFFER
ASSISTANT INSPECTOR GENERAL FOR IT AUDITS
DEPARTMENT OF HOMELAND SECURITY

FROM: James F. Tomsheck
Assistant Commissioner
Office of Internal Affairs

SUBJECT: Response to the Office of Inspector General's Draft Report Entitled, "U.S. Customs and Border Protection Has Taken Steps To Address Insider Threat, but Challenges Remain" (OIG-12-044-ITA-CBP)

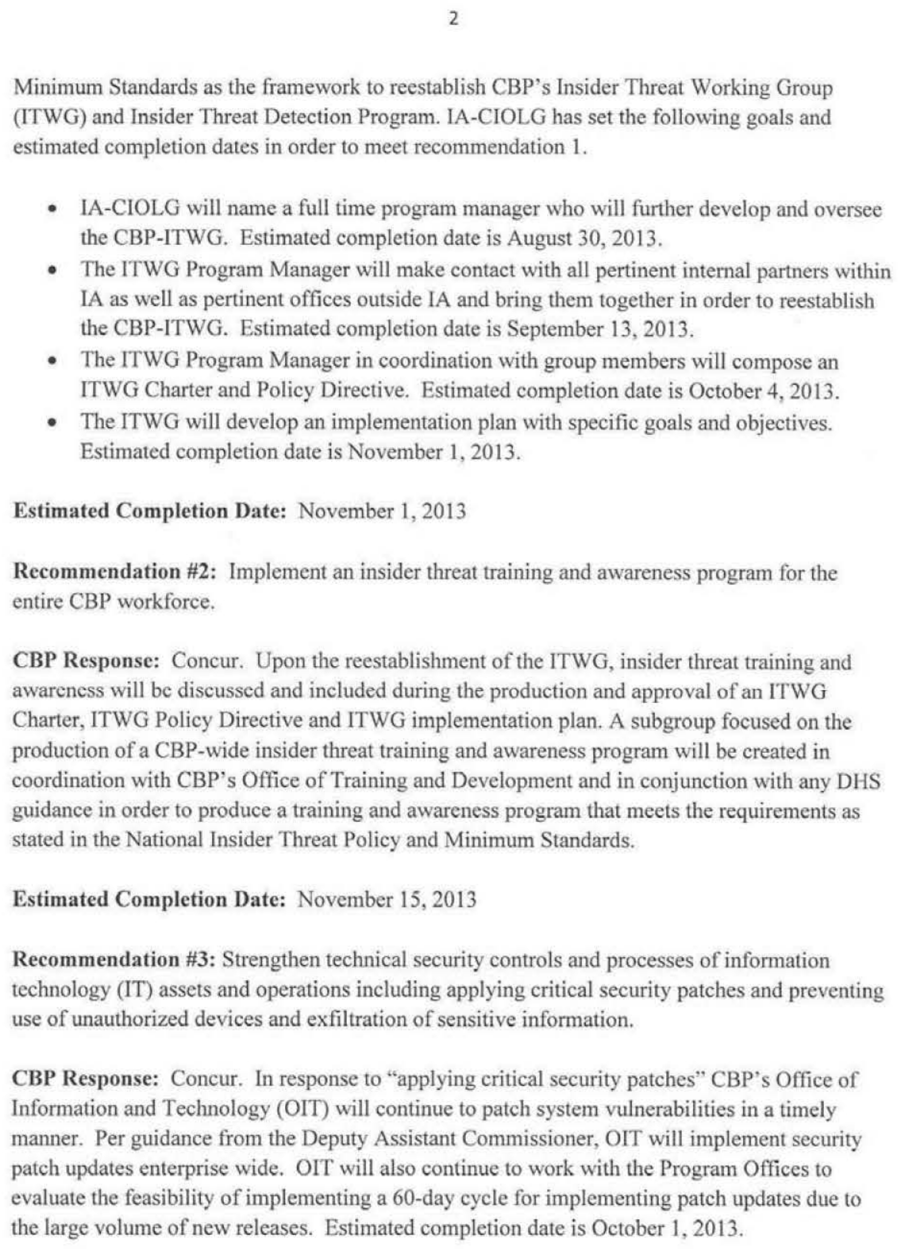
Thank you for the opportunity to review and comment on this draft report. U.S. Customs and Border Protection (CBP) appreciates the Office of Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

CBP is pleased the OIG has identified progress made by our agency. The efforts undertaken separately by the various CBP offices/divisions are the foundation of a robust and responsive insider threat detection capability. CBP acknowledges bringing all these efforts together under an overarching insider threat program will deliver a coordinated response to the threat posed by trusted insiders and strengthen our ability to manage that threat. CBP will continue to work towards improving its insider threat detection capability so that we as an agency can continue to carry out our primary mission; ensuring the security of our Nation's borders and ports of entry.

The report contains four recommendations directed to CBP. CBP concurred with all four of the recommendations. A summary of CBP's corrective action plans to address the recommendations is provided below:

Recommendation #1: Establish an agency-wide insider threat program responsible for identifying and remediating the risk posed by the insider threat.

CBP Response: Concur. Internal Affairs (IA)-Counterintelligence Operations and Liaison Group (CIOLG) will use the White House's National Insider Threat Policy and Minimum Standards and the U.S. Department of Homeland Security (DHS) Insider Threat Policy and



Minimum Standards as the framework to reestablish CBP's Insider Threat Working Group (ITWG) and Insider Threat Detection Program. IA-CIOLG has set the following goals and estimated completion dates in order to meet recommendation 1.

- IA-CIOLG will name a full time program manager who will further develop and oversee the CBP-ITWG. Estimated completion date is August 30, 2013.
- The ITWG Program Manager will make contact with all pertinent internal partners within IA as well as pertinent offices outside IA and bring them together in order to reestablish the CBP-ITWG. Estimated completion date is September 13, 2013.
- The ITWG Program Manager in coordination with group members will compose an ITWG Charter and Policy Directive. Estimated completion date is October 4, 2013.
- The ITWG will develop an implementation plan with specific goals and objectives. Estimated completion date is November 1, 2013.

Estimated Completion Date: November 1, 2013

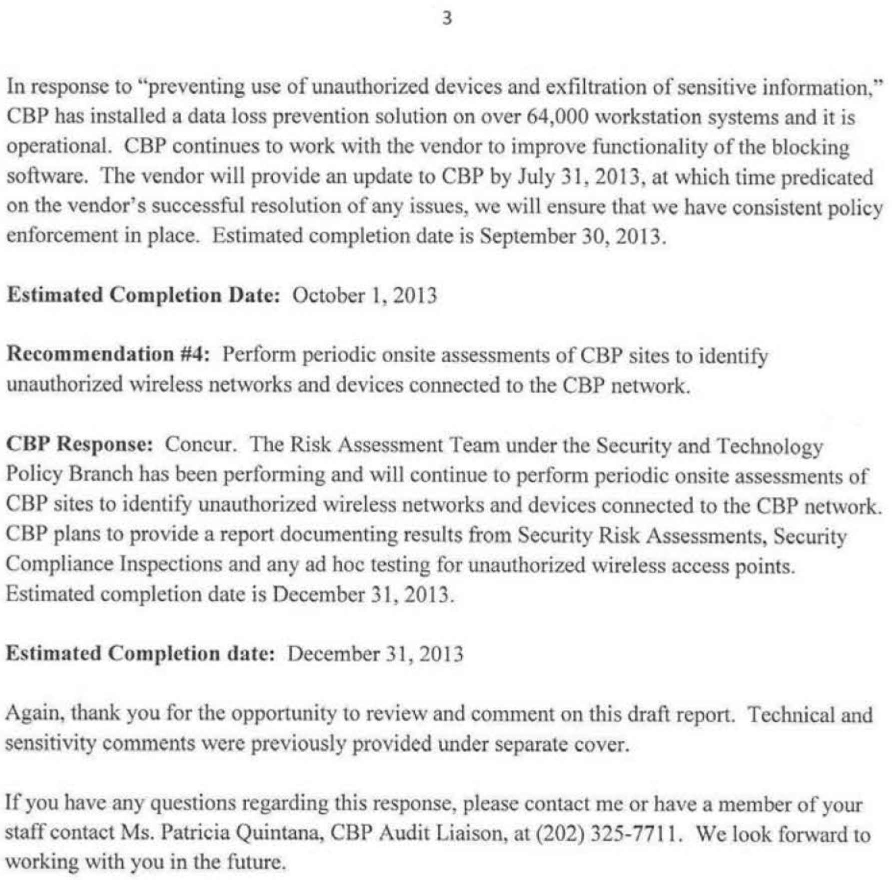
Recommendation #2: Implement an insider threat training and awareness program for the entire CBP workforce.

CBP Response: Concur. Upon the reestablishment of the ITWG, insider threat training and awareness will be discussed and included during the production and approval of an ITWG Charter, ITWG Policy Directive and ITWG implementation plan. A subgroup focused on the production of a CBP-wide insider threat training and awareness program will be created in coordination with CBP's Office of Training and Development and in conjunction with any DHS guidance in order to produce a training and awareness program that meets the requirements as stated in the National Insider Threat Policy and Minimum Standards.

Estimated Completion Date: November 15, 2013

Recommendation #3: Strengthen technical security controls and processes of information technology (IT) assets and operations including applying critical security patches and preventing use of unauthorized devices and exfiltration of sensitive information.

CBP Response: Concur. In response to "applying critical security patches" CBP's Office of Information and Technology (OIT) will continue to patch system vulnerabilities in a timely manner. Per guidance from the Deputy Assistant Commissioner, OIT will implement security patch updates enterprise wide. OIT will also continue to work with the Program Offices to evaluate the feasibility of implementing a 60-day cycle for implementing patch updates due to the large volume of new releases. Estimated completion date is October 1, 2013.



In response to "preventing use of unauthorized devices and exfiltration of sensitive information," CBP has installed a data loss prevention solution on over 64,000 workstation systems and it is operational. CBP continues to work with the vendor to improve functionality of the blocking software. The vendor will provide an update to CBP by July 31, 2013, at which time predicated on the vendor's successful resolution of any issues, we will ensure that we have consistent policy enforcement in place. Estimated completion date is September 30, 2013.

Estimated Completion Date: October 1, 2013

Recommendation #4: Perform periodic onsite assessments of CBP sites to identify unauthorized wireless networks and devices connected to the CBP network.

CBP Response: Concur. The Risk Assessment Team under the Security and Technology Policy Branch has been performing and will continue to perform periodic onsite assessments of CBP sites to identify unauthorized wireless networks and devices connected to the CBP network. CBP plans to provide a report documenting results from Security Risk Assessments, Security Compliance Inspections and any ad hoc testing for unauthorized wireless access points. Estimated completion date is December 31, 2013.

Estimated Completion date: December 31, 2013

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitivity comments were previously provided under separate cover.

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Patricia Quintana, CBP Audit Liaison, at (202) 325-7711. We look forward to working with you in the future.

Appendix C
Major Contributors to This Report

Richard Saunders, Director
Philip Greene, Audit Manager
Scott He, Lead IT Specialist
Jason Dominguez, IT Specialist
Sandra Ho, IT Specialist
David Bunning, IT Specialist
Michael Horton III, Management and Program Assistant
Kelly Herberger, Communications Analyst
Aaron Zappone, 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
Director of Local Affairs, Office of Intergovernmental Affairs
Chief Information Officer
Chief Information Security Officer

Customs and Border Protection

CBP Commissioner
CBP Assistant Commissioner, Internal Affairs
CBP Chief Information Officer
CBP Chief Information Security Officer
CBP Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

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

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.