

**CBP Has Not Ensured
Safeguards for Data
Collected Using
Unmanned Aircraft
Systems**





DHS OIG HIGHLIGHTS

CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems

September 21, 2018

Why We Did This Audit

U.S. Customs and Border Protection (CBP) uses Unmanned Aircraft Systems (UAS), a surveillance program, to support its law enforcement mission. Our objective was to determine whether CBP is effectively safeguarding information, such as images and video, collected on and transmitted from the UAS. Our work included examining the UAS IT systems security control environment.

What We Recommend

We are making ten recommendations — one to the CBP Privacy Officer and nine to the Chief Information Officer — to promote more effective management of the UAS program and improved security of data collected.

For Further Information:

Contact our Office of Public Affairs at 202-981-6000, or email us at DHS-OIG.OfficePublicAffairs@oigdhs.gov

What We Found

CBP has not ensured effective safeguards for information, such as images and video, collected on and transmitted from its UAS. CBP did not perform a privacy threshold analysis for the Intelligence, Surveillance, and Reconnaissance (ISR) Systems used in the UAS program to collect data because CBP officials were unaware of the requirement to do so. Failure to include ISR Systems in CBP's information technology (IT) inventory enabled system deployment without CBP Privacy Office oversight. Without a privacy assessment, CBP could not determine whether ISR Systems contained data requiring safeguards per privacy laws, regulations, and DHS policy.

Moreover, CBP did not implement the information security controls needed to safeguard ISR Systems. For example, ISR Systems did not have authorization to operate, including a continuity of operations plan. Continuous monitoring to facilitate effective security incident handling, reporting, and remediation was lacking, while system maintenance and oversight of contractor personnel were inconsistent. Additionally, CBP did not implement adequate controls to limit physical access to the ground control station housing ISR Systems data. These information security deficiencies occurred because CBP did not establish an effective program structure, including the leadership, expertise, staff, training, and guidance needed to manage ISR Systems effectively. As a result, ISR Systems and mission operations were at increased risk of compromise by trusted insiders and external sources.

Management Response

The Acting Senior Component Accountable Official of CBP concurred with our recommendations.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

September 21, 2018

MEMORANDUM FOR: The Honorable Kevin McAleenan
Commissioner
United States Customs and Border Protection

FROM: John V. Kelly 
Senior Official Performing the Duties of the
Inspector General

SUBJECT: *CBP Has Not Ensured Safeguards for Data Collected
Using Unmanned Aircraft Systems*

Attached for your action is our final report, *CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems*. We incorporated the formal comments provided by your office.

The report contains 10 recommendations aimed at improving the United States Customs and Border Protection Unmanned Aircraft Systems Program. Your office concurred with all of the recommendations. Based on information provided in your response to the draft report, we consider recommendations 2 through 10 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Recommendation 1 is resolved and closed.

Please send your response or closure request to OIGITAuditsFollowup@oig.dhs.gov.

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 Sondra McCauley, Assistant Inspector General, Information Technology Audits, at (202) 981-6000.

Attachment



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background 4

Results of Audit 9

 Privacy Implications of UAS Data Collection Not Addressed 10

 Recommendations 13

 ISR Systems Lacked IT Security Controls 15

 UAS Program Systems and Operations at Risk 29

 Recommendations 31

Appendixes

Appendix A: Objective, Scope, and Methodology 37

Appendix B: Management Comments to the Draft Report 39

Appendix C: List of Unauthorized Removable Media Devices Used to
Access ISR Systems 45

Appendix D: Office of IT Audits Major Contributors to This Report 46

Appendix E: Report Distribution 47

Abbreviations

AMO	Air and Marine Operations
AMOC	Air and Marine Operations Center
ATO	authorization to operate
CBP	U.S. Customs and Border Protection
FISMA	<i>Federal Information Security Modernization Act</i>
GCS	ground control station
IACS	Information Assurance Compliance System
ISR	Intelligence, Surveillance, and Reconnaissance
ISSO	information systems security officer
IT	information technology
NASO	National Air Security Operations
NASOC	National Air Security Operations Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OSI	Ocean Surveillance Initiative
OTIA	Office of Technology, Integration, and Acquisition
PDO	Privacy and Diversity Office



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

PTA	privacy threshold analysis
UAS	unmanned aircraft systems
USB	Universal Serial Bus
VADER	Vehicle and Dismount Exploitation Radar



OFFICE OF INSPECTOR GENERAL

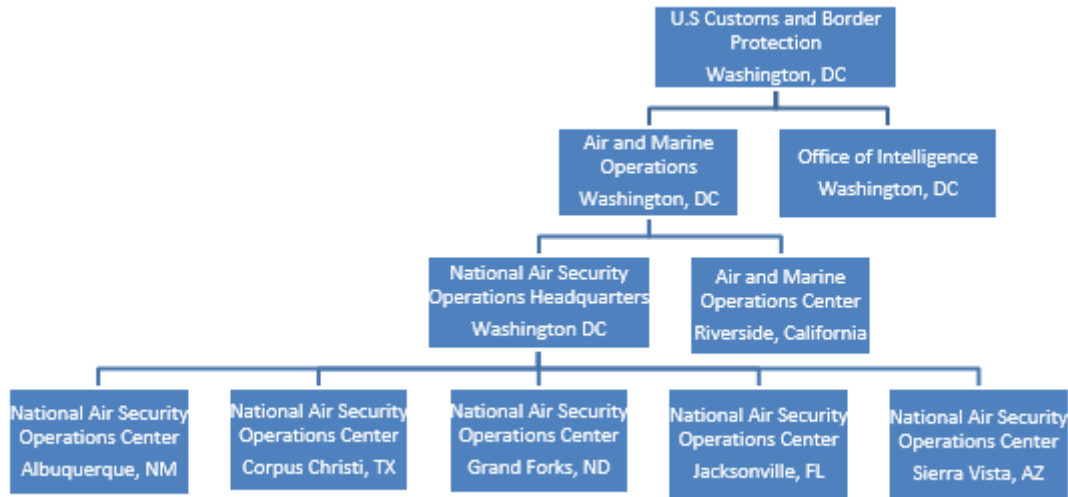
Department of Homeland Security

Background

Within the Department of Homeland Security, U.S. Customs and Border Protection (CBP) takes a comprehensive approach to border management and control by combining customs, immigration, border security, and agricultural protection into one coordinated and supportive activity. CBP guards nearly 7,000 miles of U.S. land border and 2,000 miles of coastal waters surrounding Florida, Texas, and southern California. To accomplish its mission, CBP uses a variety of aircraft to patrol the borders, conduct surveillance, and assess disaster damage. The air assets include helicopters, fixed-wing airplanes, and unmanned aircraft.

In 2004, CBP conducted a pilot study to determine the feasibility of using unmanned aircraft systems (UAS) to patrol the southwest border of the United States. The study concluded that unmanned aircraft could carry sensors and equipment and remain airborne for longer periods than CBP’s manned aircraft. Subsequently, CBP Air and Marine Operations (AMO) began UAS flight operations in 2006. Since then, CBP has expanded its UAS operations beyond the southwest border of the United States to the northern border, the Caribbean, the Gulf of Mexico, and the southern California coast. Figure 1 illustrates the structure and organizational hierarchy of CBP AMO.

Figure 1: CBP Air and Marine Operations Organization Chart



Source: Office of Inspector General (OIG)-created based on AMO data



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Located in Washington, DC, AMO’s National Air Security Operations (NASO) is responsible for administering the UAS program. The NASO’s responsibilities include management and use of unmanned aircraft, pilots, sensor operators, video cameras, land and maritime radar, communication equipment, and ground control stations. Located in Riverside, California, CBP’s Air and Marine Operations Center (AMOC) is responsible for air and marine surveillance operations, providing direct coordination to AMO; CBP law enforcement officers; and other Federal, state, and local law enforcement agencies.

Intelligence Surveillance and Reconnaissance Systems

Operating within the AMOC is Intelligence Surveillance and Reconnaissance (ISR) Systems, comprising eight interconnected software utilities and computer subsystems. These subsystems facilitate network connectivity and sharing of mission-support data collected from unmanned aircraft among data analysts, field operators, and CBP law-enforcement decision makers. Table 1 lists the eight utilities and computer subsystems that make up ISR Systems.

**Table 1: Software Utilities and Computer Subsystems
Comprising ISR Systems**

Name	Purpose
Vehicle and Dismount Exploitation Radar (VADER)	Radar system for monitoring vehicle and foot traffic over wide areas
Minotaur	Developmental software for airborne surveillance of maritime surface traffic
Multi-INT (Intelligence) Analysis and Archival System	Software providing a scalable, open, service-based platform to capture, exploit, disseminate, and archive intelligence, surveillance, and reconnaissance data
Geospatial eXploitation Products	Data management solution to locate, retrieve, and share geospatial data files
Hawkeye	Application for processing moving target indicator data
Voice Over Internet Protocol Server	Web-based intercom and conferencing solution
Network Attached Storage	Device for network-attached and on-site redundant storage
Ku Hub	Device enabling constant satellite connectivity for voice, video, and data applications

Source: OIG-generated based on CBP data



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ISR Systems constitutes the successor to AMOC Phase B, a system initially instituted to modernize and increase CBP's capacity for air, maritime, and ground domain awareness, as well as intra- and inter-agency communications and coordination. From 2011 to 2015, CBP's Office of Technology Innovation and Acquisition (OTIA) was the designated system owner. However, in August 2015 CBP decided to cancel AMOC Phase B based on its analysis that the system was too costly and not meeting program requirements. As such, CBP Headquarters directed the AMOC to create a new capital investment strategy for system enhancements, essentially consisting of a plan to sustain operations after retiring AMOC Phase B. This strategy resulted in the creation of ISR Systems in September 2015.

National Air Security Operations Centers

The NASO is responsible for the operation of manned and unmanned flights from the following three National Air Security Operations Center (NASOC) sites to support CBP's border security mission:

- Sierra Vista, AZ
- Corpus Christi, TX
- Grand Forks, ND

The three NASOCs became operational by 2011. The Sierra Vista and Grand Forks NASOCs perform surveillance missions using unmanned (MQ-9 Predator B) UAS flights, while the Corpus Christi NASOC performs surveillance missions using both manned (Lockheed Martin P-3 Long-Range Tracker) and unmanned (MQ-9 Predator B) aircraft. Federal Aviation Administration regulations do not permit the NASOCs to fly the UAS below an altitude of 19,000 feet to regulate airspace. This altitude may preclude the UAS' ability to capture personally identifiable features.

UAS operations are a collaborative effort involving a pilot and a technician working from the ground control station (GCS), and a sensor operator separately located within the NASOC to support each UAS flight. Upon detecting ground movement, the sensor operator is able to hone in on a selected target. Each unmanned aircraft, equipped with a range of video, radar, and other sensor technologies, assists CBP in patrolling the border or conducting surveillance as part of law enforcement investigations or tactical operations.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 2 provides pictures of some of the unmanned and manned aircraft currently operated from the NASOCs to accomplish CBP's border security mission.

Figure 2: Unmanned and Manned Aircraft

Unmanned Aircraft System



MQ-9 Predator B

Manned Long-Range Tracker



Lockheed Martin P-3

Source: CBP website

Initially, a fourth NASOC located in Jacksonville, FL, was tasked with controlling flight operations to support the other three NASOCs although the Jacksonville facility had no UAS of its own. In September 2016, to ensure operational efficiency, CBP's National Air Security Operations Headquarters ceased all UAS operations at the Jacksonville NASOC and relocated its mission support activities to the other three NASOCs. CBP officials said this reorganization resulted in enhanced worker productivity, improved ability for pilots to fulfill annual flight-hour requirements, and increased flexibility in mission response. None of the Jacksonville UAS crewmembers were reassigned, but periodically traveled to the other three sites to assist during surge operations.

Data Collected through the UAS Program

Through ISR Systems, the UAS program provides crucial border security information. ISR Systems network connectivity allows mission-support data to be shared among the UAS; manned aircraft systems; GCS; the various operations centers; and the Processing, Exploitation, and Dissemination cell within CBP's Office of Intelligence. This cell supports daily operational missions to identify and coordinate the interception of drug smugglers and undocumented migrants crossing U.S. borders on foot, land, and sea. In fiscal year 2017, the NASOCs collectively completed 635 missions over 5,625 hours, breaking records for both number of missions and flight hours.

The raw data (e.g., photo images) collected through ISR Systems alone cannot be used to identify a person. However, the data may later be associated with an



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

individual during an encounter with law enforcement officers or agents as part of an active investigation. According to CBP policy, data recorded onboard the UAS aircraft are stored on ISR Systems for up to 5 years, after which time the information is destroyed.

CBP's Office of Intelligence is responsible for reviewing and facilitating each information request that external Federal, state, and local law enforcement agencies submit to AMO to support their respective missions. AMO subjects each request to a standard review process and considers it in terms of the requesting agency's authority to receive the information. When requests are approved, Office of Intelligence transmits the recorded information to the requesting agency minus any unique identifiers such as coordinates, camera location, and date and time of data capture. In emergencies, Office of Intelligence may provide expedited access to recorded videos by allowing external agency representatives to view the videos at a CBP facility or via temporary video streaming through the CBP's secure firewall.

Privacy and IT Security Control Requirements

Given the nature of the UAS surveillance data collected, certain security and privacy protections may be warranted. For example, the *E-Government Act of 2002* requires privacy assessments on systems of record, including information technology (IT) systems containing personally identifiable information and other activities with potential privacy impacts. Privacy Policy Guidance Memorandum 2008-02, *DHS Policy Regarding Privacy Impact Assessments*, December 30, 2008, and the *DHS Instruction 047-01-001, Privacy Policy and Compliance*, implement this legislation within the Department. Similarly, departmental policy on managing sensitive IT systems requires that whenever a new information system is developed, the system owner must submit a privacy threshold analysis (PTA) to the DHS Privacy Office for review.¹ Compliance with such requirements can help ensure that Federal Aviation Administration regulations are met. However, the restriction that UAS be flown at altitudes of 19,000 feet and above may preclude the capture of personally identifiable images or videos during UAS missions.

Further, DHS Directive 4300A outlines various information security requirements, based on National Institute of Standards and Technology (NIST) guidelines. These requirements include developing and maintaining a system security plan and a contingency plan, publishing computer security incident response plans and procedures, and designating an information systems

¹*DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

security officer (ISSO) to serve as the point of contact for system security matters.

Related Audits

In December 2014, OIG previously reported on the effectiveness and cost of the UAS program.² Our report disclosed CBP had not developed performance measures needed to accurately assess program effectiveness and make informed decisions. CBP also did not recognize all UAS operating costs and, as such, the Congress and public may be unaware of the amount of resources invested in the program. Overall, CBP could not demonstrate how much the program had helped improve border security.

We conducted our audit to determine whether CBP is effectively safeguarding information, such as images and video, collected on and transmitted from the UAS.

Results of Audit

CBP has not ensured effective safeguards for surveillance information, such as images and video, collected on and transmitted from its UAS. CBP did not perform a PTA for ISR Systems used in the UAS program to collect data because CBP officials were unaware of the requirement to do so. Failure to include ISR Systems in CBP's information technology inventory enabled system deployment without CBP Privacy Office oversight. Without a privacy assessment, CBP could not determine whether ISR Systems contained data requiring safeguards per privacy laws, regulations, and DHS policy.

Moreover, CBP did not implement the information security controls needed to safeguard ISR Systems. Specifically, ISR Systems did not have authorization to operate, including a continuity of operations plan. Continuous monitoring to facilitate effective security incident handling, reporting, and remediation was lacking, while system maintenance and oversight of contractor personnel were inconsistent. Additionally, CBP did not implement adequate controls to limit physical access to the ground control station housing ISR Systems data. These information security deficiencies occurred because CBP did not establish an effective program structure, including the leadership, expertise, staff, training, and guidance needed to manage ISR Systems effectively. As a result, ISR Systems and mission operations were at increased risk of compromise by trusted insiders and external sources.

² U.S. Customs and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations, DHS OIG-15-17, December 24, 2014
www.oig.dhs.gov



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Privacy Implications of UAS Data Collection Not Addressed

CBP has not determined the privacy implications of collecting and transmitting information, such as images and video, via its UAS. CBP officials did not perform a PTA for ISR Systems used to collect surveillance data because they were unaware of the requirement to do so. Failure to include ISR Systems in CBP's IT inventory enabled system deployment without a privacy determination. Without conducting a PTA, CBP cannot definitively determine whether ISR Systems contains data requiring safeguards per privacy laws, regulations, and DHS policy.

No Privacy Threshold Analysis Performed as Required

AMO did not conduct a PTA for the ISR Systems as Federal and DHS policy require. According to the DHS Directive 4300A, whenever a new information system is developed, system owners must perform a PTA and submit it to the DHS Privacy Office for review and approval. Conducting a PTA demonstrates compliance with privacy laws and entails identification and examination of the data a system collects and stores to determine whether the system should be subject to a higher-level privacy impact assessment. This higher-level assessment helps identify the specific privacy controls needed to safeguard the data. For example, a PTA can help ensure compliance with privacy laws and regulations even though current Federal Aviation Administration regulations may preclude the capture of personally identifiable information for UAS flying at 19,000 feet and above.

Additionally, the *CBP Privacy Policy, Compliance, and Implementation Directive* makes each system owner responsible for coordinating with CBP's Privacy Officer to ensure privacy is addressed appropriately.³ Such coordination involves drafting all privacy documentation required when proposing, developing, implementing or changing an IT system. Despite these requirements, our audit interviews disclosed that AMO performed no PTA prior to deploying and beginning to use ISR Systems in 2017.

Lack of Awareness of PTA Requirements

Various CBP officials told us they were unaware of the requirement to complete a PTA before deploying ISR Systems. Specifically, prior to our November 2017

³*CBP Privacy Policy, Compliance, and Implementation*, CBP Directive No. 2120-010, January 2015



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

site visit, we requested that AMO provide a PTA for ISR Systems. In response, AMO sent us a PTA for another system, but not for ISR Systems. During our fieldwork, we requested a PTA from senior AMO officials. The system owner confirmed there was no PTA for ISR Systems, attributing it to the lack of an ISSO at the AMOC to provide guidance needed for such an assessment. In general, AMO officials asserted that ISR Systems did not collect and store personally identifiable information and, as such, no PTA was necessary.

Although new ownership did not absolve him of responsibility, the ISR Systems owner attributed noncompliance to his predecessor not informing him of the PTA requirement. This official emailed us that OTIA had not informed him of requirements to conduct a PTA or of any progress OTIA had made in performing a PTA for the surveillance system. During onsite interviews, the system owner used some of the same arguments as senior AMO officials, including the lack of an ISSO and an assertion that no personally identifiable information was collected and stored in ISR Systems, to explain why they conducted no PTA.

AMO officials requested the establishment of an ISSO in September 2015; however, given difficulties hiring a Government employee, they ultimately contracted out to fill this position in January 2017. During our November 2017 site visit, we discussed with this contractor the challenges of addressing ISR Systems security requirements, but found that he had not dealt with the need for a PTA since he came onboard. Like other AMO officials, the ISSO did not consider information collected and stored in ISR Systems to be privacy data.

ISR Systems Not Included in CBP Inventory to Ensure Privacy Oversight

AMO officials did not include ISR Systems in CBP's IT inventory and, as such, the CBP Privacy and Diversity Office (PDO) was unaware that the system existed and that no PTA had been performed. PDO officials did not learn of the system's existence until we interviewed them in October 2017 to discuss system privacy concerns.

After conducting more in-depth research subsequent to our October 2017 meeting, PDO officials determined that ISR Systems was a major system that should have been included in inventory. PDO staff emailed this information to us and described the situation as troubling. PDO communicated the omission to CBP's Office of Information Technology, and this office added the system to its inventory in November 2017 as a developmental system. The IT office designated the system as developmental because no system assessment had been performed, even though it was in fact operational at the AMOC.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

When asked who was responsible for the lack of a PTA, a PDO official said that it might have been a joint failure between AMO and CBP's Office of Information and Technology. A PDO official indicated that the PDO had a small staff that relied on CBP program offices to perform due diligence in privacy matters, such as notifying the PDO when implementing new systems.

Potential Risks to Privacy Data in the Absence of a PTA

By AMO officials not completing a PTA for ISR Systems, the PDO could not make an informed determination as to whether a higher-level privacy impact assessment was required. AMO officials also could not state with certainty whether or not ISR Systems contained privacy information necessitating privacy safeguards. Without proper privacy protections, any sensitive privacy information in existence could be lost, stolen, or compromised.

Recent Corrective Actions

AMO has recently begun steps to address the privacy concerns regarding ISR Systems that we raised during our audit. However, these corrective actions were not initiated until 2 years after the interconnected software utilities and subsystems were deployed and put into mission use prior to designation as ISR Systems. Specifically, in November 2017, in the middle of our audit fieldwork, AMO added ISR Systems to CBP's IT inventory, officially subjecting the system to PDO oversight and the need to fulfill privacy requirements. AMO officials also performed a PTA and submitted it to the PDO for review and approval. As of March 2018, a PDO decision regarding the PTA for ISR Systems remained pending. To the extent that the PDO ultimately determines that privacy safeguards are required, the data collected and stored in ISR Systems will have remained unprotected for more than 2 years. Subsequently, PDO completed a PTA for ISR Systems on May 21, 2018, and determined ISR Systems was a privacy sensitive system. PDO found that while ISR Systems does not contain personally identifiable information, the system is privacy sensitive technology because it tracks radar and collects still images and full motion video that may detect the presence of an individual. Additionally, ISR Systems collects data that may be used as part of an investigation should a law enforcement event take place.

The timeline at figure 3 shows the life cycle for the UAS surveillance system, from the initial AMOC Phase B to its transition to ISR Systems. The timeline illustrates how AMO actions to address ISR Systems privacy requirements were initiated out of order, long after the system was operationalized.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 3: AMOC Phase B and ISR Systems Timeline



Source: OIG-compiled information from CBP AMO documentation

Recommendations

We recommend the CBP Privacy Officer:

Recommendation 1: Provide documentation showing completion of a privacy threshold assessment with a determination regarding privacy requirements for ISR Systems.

We recommend the CBP Chief Information Officer:

Recommendation 2: Develop a process for ensuring all information systems are included in the CBP Office of Information Technology inventory, along with notification to the CBP Privacy and Diversity Office when a system is added.

OIG Analysis of Management Response to Recommendations

We obtained management comments to the draft report recommendations from the Acting Senior Component Accountable Official of CBP. We included a copy of those comments, in their entirety, in appendix B. Following is a summary of their management response to each recommendation and our analysis of their proposed corrective action plan.

Recommendation 1: Provide documentation showing completion of a privacy threshold assessment with a determination regarding privacy requirements for ISR Systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Response

Concur. On May 14, 2018, the DHS Privacy Office approved a Privacy Threshold Assessment conducted by the CBP Privacy Office for the CBP Intelligence, Surveillance, and Reconnaissance (ISR) Systems. The DHS Privacy Office determined that the CBP ISR Systems do not contain Personally Identifiable Information.

Supporting documentation was previously provided to OIG under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation as a privacy threshold assessment was provided. This recommendation will be considered resolved and closed.

Recommendation 2: Develop a process for ensuring all information systems are included in the CBP Office of Information Technology inventory, along with notification to the CBP Privacy and Diversity Office when a system is added.

Management Response

Concur. CBP's Office of Information and Technology (OIT) will develop a process for ensuring all information systems are included in the official CBP OIT Federal Information Security Management Act (FISMA) system inventory.

CBP's Cyber Security Directorate Security Operations Center Vulnerability Assessment Team will create a bi-weekly dashboard showing detected, unauthorized systems. Cyber Security Directorate will reach out to CBP Privacy and Diversity Office to discuss its role and inclusion in the updated FISMA Inventory Standard Operating Procedure and will update the FISMA Inventory SOP. Estimated Completion Date of December 31, 2019.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until the component



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

provides documentation to support that the planned corrective actions are completed.

ISR Systems Lacked IT Security Controls

CBP did not implement the information security controls needed to safeguard ISR Systems. Specifically, AMO did not:

- obtain authorization to operate the system;
- ensure compliance with Federal technical security control requirements;
- continuously monitor the system for security breaches;
- provide adequate oversight of employees and contractor personnel; and
- institute sufficient measures to limit physical access to the GCS housing surveillance data.

These security control deficiencies occurred because CBP focused on UAS mission operations and did not adequately address key management and security requirements for ISR Systems and its operations. As a result, ISR Systems and mission operations may be at risk of unauthorized access, misuse, and compromise by trusted insiders and external sources.

No Authorization to Operate

AMO has operated ISR Systems since its inception without a valid authorization to operate (ATO). According to NIST, an ATO is an official management decision by a senior organizational official to authorize operation of an information system. An ATO explicitly accepts the risk to organizational operations, organizational assets, individuals, other organizations, and the public based on a proper implementation of an agreed-upon set of security controls. Further, according to *DHS Sensitive Systems Handbook 4300A*, departmental components are prohibited from operating sensitive information systems without ATOs.

To obtain an ATO, a package of supporting documents must be compiled and submitted to the appropriate authorizing official for approval. ATO package documentation includes a system security plan, security assessment report, plan of action and milestones, final risk assessment, and a continuity of operations plan. Each item should be reviewed and approved, as well as the package in its totality. Upon completing ATO package review, the authorizing official provides a decision in the form of an ATO or Denial of ATO letter.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Despite these requirements, AMO operated interconnected software utilities and subsystems now designated as ISR Systems since 2015 without a valid ATO. AMO did not complete the required steps to obtain DHS approval for the system until we began our audit. As previously indicated, AMO did not obtain authority to test the system until September 2017, treating ISR Systems as a developmental system even though it had been operational for more than 2 years. AMO officials were aware that an ATO could not be granted as long as the system or any of its subsystems operated on an unsupported operating system. As such, they requested authority to test ISR Systems, including all of the software utilities listed in table 1, with the exception of the Ocean Surveillance Initiative (OSI) sub-system that continues to operate on an unsupported operating system.

In September 2017, the authority to test ISR Systems was approved, as a precursor to determining what controls are necessary to adequately secure the system. Typically, obtaining authority to test is followed by time needed to operate the system in a test environment before pursuing ATO. However, AMO proceeded with developing a number of the various documents needed to request ATO, given that the system was already operational. Following is a discussion of the status of AMO's progress in developing the key items required for an ATO package.

System Security Plan

In November 2017, AMO provided a draft system security plan to demonstrate to us its progress toward completing a final version for approval. The purpose of the plan is to provide an overview of the *security* requirements of the *system* and describe the controls in place or planned for meeting those requirements. The *system security plan* also delineates responsibilities and expected behavior of all individuals who access the *system*. Once approved by a designated authority, the system security plan is maintained by the system owner, who may delegate certain responsibilities to other individuals in the organization. As of March 2018, AMO had not finalized its ISR Systems security plan.

Security Assessment Report

AMO officials could not provide us a security assessment report for ISR Systems during our audit fieldwork. A security assessment report is a comprehensive test and evaluation of the management, operational, and technical security controls of an information system and summarizes the results of the security control assessment. It also should indicate the system's level of compliance with the security controls defined in its system security



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

plan. As of March 2018, a security assessment report for ISR Systems was not available for our review.

Plan of Action and Milestones

As of November 2017, AMO officials had not created a plan of action and milestones for ISR Systems. A plan of action and milestones documents any weaknesses identified with the system and the corrective actions that must be taken to mitigate them. The document details required resources, milestones, and scheduled completion dates, and assigns specific actions to individuals responsible for the system. As of March 2018, no plan of action and milestones for ISR Systems was in place.

Final Risk Assessment

During our audit fieldwork, AMO could not provide a final risk assessment for ISR Systems. This assessment documents the process of identifying risks to system security, determining the probability of occurrence and the resulting impact, and identifying additional safeguards that would mitigate that impact. As of March 2018, a final risk assessment remained unavailable.

Continuity of Operations Plan

AMO operated ISR Systems without establishing a continuity of operations plan. *DHS 4300A Sensitive Systems Handbook* states that a continuity of operations plans is vital to the success of the Department's information security program. This plan is designed to ensure the continuation of mission-essential operations during times of emergency, disaster, or service disruption. The plan needs to be developed, tested, exercised, and maintained on an ongoing basis. As of March 2018, no continuity of operations plan had been established for ISR Systems.

Technical Security Controls Deficiencies

AMO needed to make improvements regarding several key technical security controls for ISR Systems. We conducted technical testing that focused on patch management and the use of unauthorized media devices on the system. Due to the lack of a system security plan and a risk assessment for ISR Systems, we



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

had no baseline to test the system for compliance with NIST's full array of system security controls.

Patch Management Could Be Improved

AMO's patch management program was generally effective but could be improved to prevent a few problems that we identified. Patch management involves acquiring, testing, and installing fixes, known as patches, to remedy known vulnerabilities or deficiencies in a system's software or operating system. According to NIST 800-40, *Guide to Enterprise Patch Management Technologies*, patches are usually the most effective way to mitigate software vulnerabilities.⁴

Generally, AMO had an effective patch management program that ensured identification and remediation of security vulnerabilities on workstations and servers within ISR Systems' authorization boundary. Using a commercially available off-the-shelf application, AMO scanned ISR Systems on a monthly basis to mitigate system vulnerabilities and update the system with the latest security patches, as appropriate. AMO technicians patched most servers and workstations on 30-day cycles; however, VADER and Minotaur systems were patched on a 90-day cycle, which was not in accordance with DHS policy that requires timely installation of software patches.

Despite AMO's patch management efforts, we identified a low number of critical and high-risk vulnerabilities on AMO workstations and servers that needed corrective action. Specifically, we identified one unique critical vulnerability, and seven unique high-risk vulnerabilities on Windows 7 workstations. While Windows Server 2008 had no unique critical vulnerabilities, we found one unique high-risk vulnerability. Collectively, these vulnerabilities provided the potential for:

- Remote code execution: Exploits that take advantage of software that allows the execution of machine code and injects shellcode to allow the attacker to run arbitrary commands on another user's computer.
- Privilege escalation: A system user gets access to more resources or functionality than normally allowed, though the application should have been prevented such access.
- Information disclosure and security feature bypass: An information disclosure vulnerability exists when Outlook fails to establish a secure connection. An attacker can exploit the vulnerability to obtain the email

⁴ NIST 800-40, *Guide to Enterprise Patch Management Technologies*, Revision 3, July 2013
www.oig.dhs.gov



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

content of a user. A security feature bypass vulnerability exists when Microsoft Office improperly handles objects in memory. In a file-sharing attack scenario, an attacker can provide a specially crafted document file designed to exploit the vulnerability, and then convince users to open the document file and interact with the document.

- Denial of service: Such attacks prevent authorized access to resources or cause delays in time-critical operations.
- Reboot required to install a Windows update: Pending security-related system changes, the host remains vulnerable to attack until reboot occurs.

We determined the Windows 7 workstation vulnerabilities were due to insecure programs, including Microsoft Office, Outlook, and protocols used by these software, as well as Oracle Java, anti-virus, and network monitoring software. The Windows server vulnerabilities were due to an anti-virus client and services such as a .NET framework used by the servers that could be exploited if they remained unpatched. AMO's ISSO and systems administrators reviewed our system test results and undertook efforts to remediate the problems found.

Unauthorized Removable Media Devices Found on the System

AMO could improve controls to prevent employees from using unauthorized equipment to access ISR Systems. As required in DHS policy, only authorized, Government-issued removable devices should be used to connect to systems and the data they contain. ISR Systems maintained audit logs of all access and activity on the system. By examining the logs, we identified 24 devices that employees had used to connect to ISR Systems workstations, including Universal Serial Bus (USB) flash drives, external hard drives, and mobile phones.⁵ The unauthorized devices provided the capability to introduce or remove information, such as images and videos captured by the UAS. Specifically, we found:

- 9 types of USB flash drives that did not meet DHS encryption requirements for safeguarding data;
- 10 types of unauthorized external hard drives; and
- 3 types of unauthorized mobile phones had been connected to ISR Systems.

Appendix C provides a list of the media devices we identified that provided access to ISR Systems workstations. Two of the devices were included on

⁵ A USB flash drive, also known as a thumb drive, is a small, readily available, and portable device for storing and transporting data.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

AMO's list of authorized media devices that could be used to download and transfer files. Our tests did not identify any USB removable media devices connected to ISR System servers.

When we brought this problem to the ISSO's attention, he initially stated via email that GCS operators may have used unauthorized devices to transfer data between the UAS and ISR Systems. However, in a subsequent email, the ISSO could not confirm that this actually occurred, citing an inability to pinpoint the exact date and time of the breaches using standard scanning tools. Nonetheless, the ISSO said CBP's Office of Information Technology security operations center was in the process of creating a policy to prohibit the use of unauthorized devices in the future.

Ineffective System Monitoring and Maintenance

AMO could improve its monitoring and maintenance of ISR Systems for information security purposes. AMO officials did not continuously monitor ISR Systems for network and system-based security breaches as required to ensure ongoing awareness of information security, vulnerabilities, and threats to system and network operations. Officials did not review system audit logs on a regular basis. Further, multiple GCS used an unsupported operating system.

System Events Not Monitored

AMO did not fulfill Federal and DHS requirements for monitoring ISR Systems. Despite DHS Directive 4300A requirements that components conduct continuous monitoring, ISR Systems operated outside of the boundaries of the Security Operations Center responsible for oversight of all CBP systems and networks. As such, CBP could not oversee the system on an ongoing basis to ensure situational awareness and detect unauthorized system activities and events. Although AMO IT professionals audited system logs for events that might be precursors to security incidents or breaches, they did not do so consistently or timely. They also did not regularly monitor a firewall located at the GCS for suspicious network or system activity. This lack of monitoring potentially hindered AMO officials' ability to take immediate and effective action to remediate any breach that might occur.

Use of Obsolete Software

Despite DHS Directive 4300A restrictions, AMO used outdated operating systems for which vendors no longer provided the patches needed for up-to-date security protection. We determined that OSI, a subsystem of ISR Systems



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

that provides airborne surveillance of maritime surface traffic from onboard the UAS, was running on an outdated version of the Linux operating system. As of October 31, 2014, the vendor had ceased providing security patches to protect this version of the Linux operating system from harmful viruses, spyware, and other malicious software. As such, AMO began developing Minotaur, a software utility that would replace the OSI in enabling maritime surface traffic surveillance and run on an up-to-date operating system with adequate security controls. During our fall 2017 audit fieldwork, an AMO official estimated that AMO would be able to deploy Minotaur within 6 months to a year. We determined that Minotaur remained under development as of March 2018.

Similarly, the GCS at all three NASOC locations included in our audit were running Windows XP, an operating system no longer supported by Microsoft since April 2014. The NASOCs also did not patch VADER, the subsystem used with sensor operators to detect ground movement, in a timely manner.

Inadequate Management of Personnel Responsible for ISR Systems

We identified instances where CBP employees were required to perform duties beyond their normally assigned job. In some cases, employees were not cross-trained to perform those duties. In addition, CBP officials did not provide adequate oversight of contractor employees.

Employees Performed Duties beyond Their Job Assignments

AMO did not adequately delineate employee roles and responsibilities critical to successful ISR Systems operations. As such, some employees performed duties beyond their typical job assignments. For example:

- In 2015, an AMO chief engineer was additionally responsible for serving as the ISR Systems owner. Although this was supposed to be a 12-month assignment, at the time of our audit, this official was still performing both the engineering and system owner duties.
- A system engineer performed multiple functions beyond the original job responsibilities to support AMO's Intelligence Systems. After being hired, this employee was tasked to assume helpdesk and system administrator duties for ISR Systems as well.
- An AMOC employee within CBP's Office of Intelligence was responsible for supporting daily mission operations to identify and coordinate the interception of drug smugglers and undocumented migrants crossing the border on foot, land, and sea. Over time, this employee's responsibilities



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

grew to include ISR Systems log auditing, system patching, system administration, and user support.

Employees confided to us that they felt heavily tasked or saturated with additional job responsibilities beyond their normal workloads. They raised concerns that, in these circumstances, their primary work activities might fall behind or not be performed effectively. Further, mandatory tasks in critical areas such as information security might not be completed timely.

Inadequate Contractor Oversight

At one NASOC facility, CBP officials did not ensure proper oversight. Specifically, the NASOC in Corpus Christi relied heavily on contractors to support critical aspects of UAS flight operations, but the contractors sometimes lacked awareness of Government employees assigned to oversee them. DHS Directive 4300A requires that departmental components monitor contractors responsibly and indicates that security is inherently a Government responsibility. Contractors working on behalf of DHS and other sources may assist in performing security functions, but a DHS employee must have foremost responsibility for all security requirements and functions.

Despite these requirements, we observed instances where contractor employees in key operational roles had limited or no Government supervision. For example, a NASOC supervisor indicated that a contractor organization was responsible for maintenance of the Corpus Christi GCS, although Federal guidelines placed this responsibility for information security systems with Government personnel. In other instances, contractors were unsure of who their Government supervisors were. To illustrate, one contractor initially could not tell us which CBP program official he was supposed to report to, although he had worked at the NASOC for some time. After looking into the matter, the contractor eventually provided us the name of his designated supervisor.

Inadequate Physical Access Controls for GCS

We found that the NASO did not ensure secure access to the GCS where the UAS are remotely operated. DHS Directive 4300A requires controls for facilities containing sensitive information systems, as physical security represents the first line of defense against intruders attempting to gain unauthorized access.⁶ We found adequate physical access controls for the rooms containing ISR

⁶ Physical controls include barriers, badges, guard or security forces, supporting infrastructure, contingency and emergency support, lighting, facility intrusion detection systems, and surveillance systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Systems subsystems at both the AMOC and NASOC locations we visited. However, AMO had inadequate physical access controls to safeguard systems and the mission-critical information housed in its three GCS facilities.

For example, we observed that physical access to the GCS trailer in Corpus Christi was not adequately protected. Pilots remotely operate UAS aircraft from the GCS trailer located on an enclosed site that includes the NASOC and a hangar housing UAS aircraft. Anyone can also easily climb over the low fence surrounding the NASOC perimeter. However, one should enter through the NASOC building and the adjacent hangar that are both access-restricted using personal identity verification cards in order to exit onto the grounds where the GCS is housed. The GCS is padlocked overnight when not in operation, but remains unlocked and accessible to anyone on the grounds during normal operating hours (e.g., during pre-flight and flight operations). Visitors and custodial staff are supposed to be escorted to the GCS. However, maintenance technicians and CBP employees involved in the NASOC's manned and unmanned flights have unfettered access during operating hours.

The NASOC maintained no log of those who accessed the GCS. We found no controls in place, such as access cards or cipher locks, to limit GCS access to only those personnel who need it. Furthermore, there were no security guards. While GCS security cameras continually recorded the area surrounding the GCS, these cameras were not regularly manned, and their taped recordings were over-written every 20 days. We did not visit the Sierra Vista and Grand Forks GCS facilities; however, we determined from discussions with NASOC officials that their GCS facilities also lacked adequate physical access controls.

Ineffective Program Structure Contributed to ISR Systems Security Control Deficiencies

The information security control deficiencies we identified were largely due to CBP's failure to ensure an effective program structure to support ISR Systems and its operations effectively. Since 2015, AMO leadership has prioritized funding UAS mission operations over instituting the security controls needed to safeguard ISR Systems and effectively support its operations. Programmatic ownership of ISR Systems has not been clearly established since the system was first put into use. Several key positions responsible for ensuring ISR Systems security were not established as required, and those assigned inappropriately managed the system as a developmental system although it was actually operational. The AMOC had insufficient staff to safeguard and manage ISR Systems. Inadequate training of key personnel to support ISR Systems was evident throughout the program. Further, AMO leadership did not



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

establish and maintain standard operating procedures to ensure security and management of ISR Systems in compliance with Federal and DHS policy.

Funding Priority Given to UAS Mission Operations

An AMO official told us that AMO placed more priority on accomplishing UAS mission operations than on ensuring ISR Systems security controls. The official said that without the funding needed to do both fully, AMO chose the mission first. The AMOC Director of Systems also said that AMO did not consider security requirements when AMO began using ISR Systems.

DHS Directive 4300A discusses the system engineering life cycle and states that it is the responsibility of the system owner to “ensure that adequate funding is available for implementation of security requirements and that adequate budgetary resources for information security requirements are available.” However, AMO officials said that ISR Systems has never received a discrete budget as part of the UAS program. An official indicated that since 2015, when the interconnected software utilities and subsystems were first deployed, they operated with funds reallocated from other programs under AMOC purview. Through interviews, we determined that AMO leadership never developed a plan or strategy to obtain the financial resources needed to support this program specifically.

AMO officials cited budgetary constraints as the largest impediment to ensuring compliance with information security requirements. An AMO official told us it was often necessary to borrow IT equipment and personnel from other units to perform technical functions such as system scanning and patching. Because of a lack of funding, AMO officials were denied requests for security guards to control physical access at the NASOC in Corpus Christi. The lack of a discrete budget relegated the ISR Systems to being staffed at a level that did not ensure effective, efficient, and compliant operations. Inadequate funding also contributed to heavy reliance on contractors who sometimes performed their duties without adequate oversight.

A lack of funding also relegated the Corpus Christi NASOC to employing only one IT person while the Sierra Vista NASOC had to share another office’s IT professional for one day a week. The latter resulted in inadequate IT support during peak mission operations, which in some instances subjected the mission to being grounded until IT issues could be addressed. CBP’s IT



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

resource limitations can cause delays or cancellation of an entire UAS mission, decreasing the ability of border patrol agents on the ground to effectively identify and combat criminal activity.

Unclear Programmatic Ownership of ISR Systems

CBP's delay in establishing organizational ownership of ISR Systems has resulted in little to no assigned responsibility and accountability for the system's management as a whole. Programmatic ownership of ISR Systems has not been clearly established since 2015 when the interconnected software utilities and subsystems were first put into use. Specifically, OTIA ceased organizational ownership after cancellation of AMOC Phase B and inception of ISR Systems.

With its inception, AMO received ownership of ISR Systems, but responsibility for funding and maintenance of the system was not assigned to any single entity within the organization. AMO officials indicated that the ISR Systems replaced its predecessor, AMOC Phase B. As such, CBP units were reluctant to assume programmatic ownership given system funding and management concerns dating back as far as late 2010. During our site visit to the AMOC in November 2017, we learned that AMOC officials were in the process of assuming programmatic ownership of ISR Systems.

Key System Security Leadership Positions Not Established or Assigned

Several key IT positions needed to ensure ISR Systems security were not established or assigned as required. This could result in an inability to address routine IT support requirements, respond to and remediate system security problems, or pinpoint responsibility for systematic failures.

- System owner:
Despite unclear programmatic ownership, an individual has been designated system owner of ISR Systems since September 2015. Per DHS Directive 4300A, system owners are responsible for successful operations of information systems and programs within their program areas, including system security. As previously stated, this official was unclear about his responsibilities for ensuring a privacy assessment of ISR Systems. He had expected OTIA officials to advise him of requirements to bring the system into compliance, but this was not done. Further, when asked why ISR Systems had been operating for more than 2 years



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

without an ATO, the system owner cited the lack of an ISSO as the primary reason why a number of IT security requirements for ISR Systems were not addressed.

- ISSO:
According to DHS Directive 4300A, an ISSO is responsible for overall system security, including development and maintenance of security plans. AMO officials cited difficulty hiring an ISSO for ISR Systems as an impediment to ensuring ATO. Specifically, AMO officials initially had trouble getting the funding for an ISSO position. After they secured the needed funding, they sought to hire a Government official for the ISSO position, but were unable to identify a qualified individual. As such, they had to hire a contractor to fill the position in January 2017.
- Information System Security Manager:
No one was assigned to fill this position. Per DHS Directive 4300A, this official is responsible for overseeing the component's information security program.
- Security Controls Assessor:
This position was vacant as well. Per DHS Directive 4300A, this official is responsible for certifying the results of the security control assessment. Again, AMO officials said they were working to fill this position. During our November 2017 site visit, AMO officials indicated that they were in the process of assigning these roles and responsibilities to AMOC personnel.

ISR Systems Improperly Categorized as a Developmental System

We found disagreement among AMO officials regarding the status of ISR Systems. Specifically, the AMOC Director told us that ISR Systems was operational. Office of Intelligence Staff and a variety of AMOC staff that we interviewed said likewise. As previously stated, PDO officials confirmed that ISR Systems was operational after conducting research following our interviews with them to determine whether the system needed a PTA.

However, the system owner improperly catalogued ISR Systems as a developmental system, excluding it from inventory even though its interconnected software utilities and subsystems had been employed in UAS program operations since 2015. During our interview, the system owner



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

indicated ISR Systems was an ongoing test system, and did not change this view after we told him that other AMOC officials, including the Director of Systems, considered the system operational. Treating the system as developmental precluded it from being subject to CBP oversight, ATO, and all of the necessary security measures, processes, and controls that would otherwise be required for an operational system.

Inadequate Staff

The AMOC did not assign adequate staff to safeguard and manage ISR Systems effectively. Although AMOC officials stated that six contractors and two Government employees were needed, only three contracted IT personnel were assigned to support system operations—an ISSO and two IT specialists. As previously stated, it took the AMOC 15 months, from initial request in November 2015 until January 2017, to fill the ISSO vacancy, and it did so with a contract employee.

Further, the Corpus Christi NASOC had only one employee to provide IT support for the entire location, while the Sierra Vista NASOC had to utilize the services of another office's IT specialist, who was only available one day per week. Neither NASOC had back-up IT personal.

Our interviews with AMO staff disclosed additional personnel were needed to complete mandatory tasks in a timely manner and ensure a clear separation of duties, which is a key security requirement. A staff member felt overburdened and expressed difficulty completing assigned duties. This employee said that additional staff would help to ensure that system security was not ignored. To illustrate, the employee suggested that additional staff could help complete overdue ISR audit log reviews, compile the ATO package, and provide better IT user support.

Insufficient IT Security and Systems Training

According to DHS Guidelines, training for new system users must occur before allowing them system access. DHS requires that personnel and contractors with significant security responsibilities receive specialized training annually, including role-based training that addresses management, operational, and technical roles and responsibilities. A DHS component's Chief Information Security Officer is responsible for ensuring that training for personnel with significant responsibilities for information security occurs.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We found that all AMO employees and contractor personnel were required to take DHS Annual Security Awareness and Privacy training, regardless of the employee's role in IT security. Such training is fundamental for all individuals who access and use DHS IT systems. However, a lack of specialized training for key personnel responsible for supporting ISR Systems was evident throughout the UAS program. For example:

- During our audit, the ISSO for ISR Systems failed to provide the audit team with evidence of his completion of the mandatory annual training specific to his assigned security responsibilities. Such training is critical for those that have significant security responsibilities, as it allows them the opportunity to stay abreast of changes and advances in security policies and procedures.
- Specialized role-based training, designed to include the steps necessary to complete and obtain a valid and current ATO, was not offered to personnel responsible for supporting ISR Systems.
- The curriculum for ISR Systems operators varied by location and was described as being more comprehensive at NASOC Sierra Vista than at NASOC Corpus Christi.

No Standard Operating Procedures

AMO officials did not establish and maintain standard operating procedures to ensure that ISR Systems complied with information security policy. Federal internal control standards require managers to design control activities to achieve an effective internal control system. These activities include policies, procedures, techniques, and mechanisms that enforce management directives to achieve the entity's objectives and address related risks.

As a system-of-systems, ISR Systems comprises multiple software utilities, advanced technologies, complex programs, and key roles. Such complexity requires documented procedures that fully explain how IT managers and professionals should carry out their assigned duties for managing the technology. AMO personnel said that such procedures should address IT matters such as user account creation, user access, roles of contractors, locations of systems, and network topology. However, such guidance was lacking. In November 2017, AMO officials indicated they would begin to take the steps necessary to put such operating procedures in place.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

UAS Program Systems and Operations at Risk

CBP's failure to implement adequate security controls according to Federal and DHS policy could result in potential loss of confidentiality, integrity, and availability of ISR Systems and its operations. Specifically:

- Without a current and valid ATO, AMO has no reasonable assurance it has implemented effective controls to protect ISR Systems and the data it processes and stores from potential compromise, loss, or theft by both outside and inside sources. In addition, the lack of a valid and current ATO leaves the system owner and senior management without a baseline from which to make sound risk management decisions to ensure the system is adequately safeguarded from a potential breach.
- Without a continuity of operations plan, AMO has no assurance of minimal downtime and smooth resumption of operations should a disruption of service or an unforeseen event such as a natural disaster occur.
- By not adhering to federally-mandated requirements for patch management of systems and workstations, CBP cannot ensure it has taken steps needed to reduce the risk of loss, theft, or destruction of data to a reasonable level. Individuals with malicious intent can target systems without the latest security updates patches, resulting in lost confidentiality, integrity, or availability of mission-critical data.
- Inadequate controls to prevent and detect the loss of data through unauthorized portable media devices make ISR Systems and the data it collects and stores more susceptible to compromise.
- Lacking continuous diagnostics and monitoring of the system, AMO cannot maintain an up-to-date picture of ISR Systems' security posture as needed to identify vulnerabilities and take immediate action to address risks to mission-critical operations and data. Officials cannot readily detect unusual user or system events and provide appropriate response to address security risks, attacks, or anomalies as necessary. Left undetected, anomalous user behavior and unusual system events can result in operational disruptions and unauthorized disclosure or theft of information.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- ISR Systems sub-systems operating with unsupported operating systems may be out-of-date and have decreased functionality. Inability to ensure vendor patches for the obsolete software leaves the sub-systems susceptible to security breaches, virus, and possible attack.
- Employees performing tasks beyond their job functions can adversely affect AMO's ability to fulfill the UAS mission. Employees may lack the requisite training and knowledge to adequately perform those job functions and their primary responsibilities may go unfulfilled. Employees also may be overburdened, susceptible to burn-out, and less satisfied with their jobs, all of which can affect their performance.
- Contractors filling key security and operations roles, without adequate oversight of their access to and use of Government systems and information, increase the insider threat risk. There may be no assurance that contractors are performing according to their statements of work and in the Government's best interest. Contractors performing tasks outside of their negotiated scope of work can also pose legal and financial risks for both the contracting firm and the Department, per the Federal Acquisition Regulations.
- Without standard operating procedures, IT employees lack guidelines for sustaining operations and ensuring ISR Systems comply with Federal and DHS information security policy.
- Physical security of GCS facilities and systems is important to protect UAS mission operations and the data collected and stored from unauthorized access.

In conclusion, AMO has much work to do to meet Federal and DHS requirements for safeguarding ISR Systems and its operations. This begins with establishing an effective IT program management structure and making system funding and security as much of a priority as accomplishing the UAS flights alone. Assigning clear system ownership and filling IT leadership positions with individuals possessing the knowledge and skills needed to fulfill IT security control requirements is also key. Such individuals can take the lead in ensuring ISR Systems is properly included in inventory; receives appropriate oversight; and is supported by sufficient, well-trained staff and standardized guidance for sustaining IT operations. Taking such corrective actions to ensure the information security of ISR Systems and the data it collects and stores will go a long way in undergirding overall UAS program operations and supporting the accomplishment of CBP's border protection mission.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendations

We recommend the CBP Chief Information Officer:

Recommendation 3: Create a plan to establish programmatic and system ownership and ensure appropriate oversight of ISR Systems.

Recommendation 4: Provide a plan, including timelines, for fulfilling supporting requirements and obtaining authorization to operate ISR Systems.

Recommendation 5: Create and implement a process according to DHS policy for timely installing software patches on the VADER and Minotaur systems.

Recommendation 6: Create and implement a process to update all ISR System sub-systems currently running on unsupported operating systems.

Recommendation 7: Create a plan for filling key IT positions and allocating sufficient budget and staff resources to perform duties required to safeguard ISR Systems and the data it collects and stores.

Recommendation 8: Create a plan for providing oversight of all contractors who assist in performing duties required to safeguard ISR Systems and the data it collects and stores.

Recommendation 9: Develop and implement a plan to conduct specialized training for personnel responsible for the security and maintenance of ISR Systems.

Recommendation 10: Develop and implement standard operating procedures for sustaining operations and ensuring ISR Systems comply with Federal and DHS information security policy.

OIG Analysis of Management Response to Recommendations

We obtained management comments to the draft report recommendations from the Acting Senior Component Accountable Official of CBP. We included a copy of those comments, in their entirety, in appendix B. Following is a summary of their management response to each recommendation and our analysis of their proposed corrective action plan.

Recommendation 3: Create a plan to establish programmatic and system ownership and ensure appropriate oversight of ISR Systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Response

Concur. CBP's Air and Marine Operations (AMO) has established programmatic and system ownership of ISR Systems, ensuring appropriate oversight. In May 2017, an AMO official was designated System Owner of ISR Systems and an AMOC contractor was designated the Information Systems Security Officer (ISSO) for ISR Systems.

DHS requires CBP and other components to use its Information Assurance Compliance System (IACS) to develop, maintain, and monitor Security Authorization Packages for all Sensitive but Unclassified Information Technology (IT) systems. DHS granted the ISR Systems ISSO access to IACS in November 2017.

We request that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation; however, we still require documentation demonstrating that:

- in November 2017, DHS approved AMO's development change request to include ISR Systems as part of CBP's IT inventory and issued a *Federal Information Security Modernization Act (FISMA)* ID; and
- CBP has added ISR Systems to its Investment Evaluation, Submission, and Tracking system for IT business case information and portfolio management.

We look forward to receiving these updates, and in the meantime, this recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.

Recommendation 4: Provide a plan, including timelines, for fulfilling supporting requirements and obtaining authorization to operate ISR Systems.

Management Response

Concur. AMO is developing a number of documents needed to obtain an authorization to operate (ATO) through the formal DHS/CBP IACS process. AMO has a Plan of Action & Milestones that includes timelines for obtaining authorization to operate ISR Systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We request that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation; however, we still require documentation demonstrating that AMO has a Plan of Action & Milestones that includes timelines for obtaining authorization to operate ISR Systems.

We look forward to receiving those updates. In the meantime, this recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.

Recommendation 5: Create and implement a process according to DHS policy for timely installing software patches on the VADER and Minotaur systems.

Management Response

Concur. AMO has created a process for timely, 90-day installation of software patches on the VADER and Minotaur system. To maintain DoD and CBP integrity and current efficiencies detailed in OIG's draft report, AMO has prepared a request to CBP OIT for approval to implement a timely software patch cycle of 90 days for Minotaur and VADER. AMO's request is supported by DHS 4300A, Policy ID 3.7.c. estimated for June 30, 2019.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation. We look forward to receiving updates regarding the new 90-day software installation cycle for Minotaur and VADER. This recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.

Recommendation 6: Create and implement a process to update all ISR System subsystems currently running on unsupported operating systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Response

Concur. AMO has created and implemented a process to update all ISR Systems subsystems currently running on unsupported operating system. The transition from Ocean Surveillance Initiative's (OSI) unsupported legacy software to the supported Minotaur system is programmed to occur no earlier than December 2018, by contract. Estimated completion date of January 30, 2019.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.

Recommendation 7: Create a plan for filling key IT positions and allocating sufficient budget and staff resources to perform duties required to safeguard ISR Systems and the data it collects and stores.

Management Response

Concur. AMO has filled its three key IT positions and has allocated sufficient budget and staff resources. ISR Systems currently have a System Owner, an ISSO, and Security Controls Assessor.

We request that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation; however, we still require documentation demonstrating that the position of Security Controls Assessor has been filled and that sufficient budget resources have been allocated to perform all the duties required under this recommendation.

We look forward to receiving those updates. In the meantime, this recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 8: Create a plan for providing oversight of all contractors who assist in performing duties required to safeguard ISR Systems and the data it collects and stores.

Management Response

Concur. AMO continues to have oversight of all contractors who assist in performing duties required to safeguard ISR Systems and the data collected and stored.

At the AMOC, contractors with administrative rights on ISR Systems have been functionally aligned under the AMOC Systems Division to ensure change control process and security practices are followed. Separation of duties between system administrators, engineers, and the ISSO are maintained in accordance with least privilege and separation of duties concepts, which is illustrated in AMO's functional organization charts.

We request that the OIG consider this recommendation resolved and closed as implemented.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation; however, we still require documentation of the organization charts, administration rights, and separation of duties.

We look forward to receiving those updates. In meantime, this recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.

Recommendation 9: Develop and implement a plan to conduct specialized training for personnel responsible for the security and maintenance of ISR Systems.

Management Response

Concur. AMO has identified personnel with system security responsibilities, and will provide annual training that is a combination of existing Performance and Learning Management System requirements and tailored role- based training. Estimated Completion Date of January 30, 2019.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.

Recommendation 10: Develop and implement standard operating procedures for sustaining operations and ensuring ISR Systems comply with Federal and DHS information security policy.

Management Response

Concur. AMO is developing standard operating procedures for sustaining operations, including existing SOPs to be inherited and expanded to include ISR Systems. Estimated Completion Date of August 30, 2019.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until the component provides documentation to support that the planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. Our objective was to determine whether CBP is effectively safeguarding information, including images and video, collected on and transmitted from its UAS. Our work included examining the UAS IT systems security control environment.

We performed fieldwork at DHS headquarters and component organizations in Riverside, CA, and Corpus Christi, TX. We researched background information, including applicable laws, regulations, guidance, and prior audit reports related to the UAS Program. We also conducted interviews with representatives of CBP's Privacy and Diversity Office, as well as its Office of Information Technology to determine their respective roles in the operation and security of the UAS program.

From our interviews and site-visits, we were able to gather and analyze information on current policies and procedures related to the protection of sensitive and privacy data, as well as some of the security and programmatic challenges facing the UAS program. Specifically, while on site at the AMOC in Riverside, CA, November 2017, we conducted interviews with officials responsible for network security and system maintenance. AMOC officials also provided an overview of the UAS program and mission operations.

Personnel similarly discussed UAS mission operations during our site visit to the NASOC in Corpus Christi, TX, in November 2017. We also conducted interviews with officials responsible for NASOC leadership, piloting UAS and manned aircraft, GCS and VADER sensor operations, UAS engineering support, IT management, and evidence handling. We used no classified information to conduct this audit.

We conducted this performance audit between September 2017 and February 2018 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We appreciate CBP management's efforts to provide the information and access necessary for us to accomplish this audit. Appendix D contains major contributors to this report.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Management Comments to the Draft Report


1300 Pennsylvania Avenue NW
Washington, DC 20229



**U.S. Customs and
Border Protection**

September 5, 2018

MEMORANDUM FOR: Sondra F. McCauley
Acting Assistant Inspector General for Audits
Office of Inspector General

FROM: Henry A. Moak, Jr. 
Acting Senior Component Accountable Official
U.S. Customs and Border Protection

SUBJECT: Management Response to Draft Report: "CBP Has
Not Ensured Safeguards for Data Collected Using
Unmanned Aerial Systems" (Project No. 18-043-
ITA-CBP)

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

CBP's Intelligence, Surveillance, and Reconnaissance (ISR) Systems consist of interconnected software utilities and computer systems providing CBP with the network connectivity to share mission support data between CBP intelligence analysts, field operations, and operational decision makers. ISR Systems provide the network for sharing data between systems onboard unmanned aircraft systems (UAS), ground control stations (GCS), manned aircraft, operations centers, and the Office of Intelligence's (OI) Processing, Exploitation, and Dissemination (PED) Cell.

ISR Systems shares unclassified live surveillance and reconnaissance data - including radar tracks, still frame images, and full motion video - obtained from aircraft systems and sensors along the U.S. border that monitors for illegal events requiring CBP intervention. It is important to note that ISR Systems surveillance and reconnaissance data is not associated with any individual unless the data is linked to an investigation as a result of a law enforcement event. In the event that ISR Systems surveillance data is later linked to an individual subject in a CBP law enforcement or other investigation, data that is used for any prosecution case is linked outside the accreditation boundary of this system, and no other data is entered into this system. Further, individual biographic information is not used or input at any time, as ISR Systems only capture radar tracks,

1



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

still frame images, and full motion video. It should also be noted, data is stored in encrypted format and files not retrieved for evidentiary use are automatically deleted (recorded over) after five years.

As noted in the OIG report, CBP has begun steps to address the OIG's concerns. CBP is pleased to report that the Department of Homeland Security's (DHS) Privacy Office completed a Privacy Threshold Assessment (PTA) for ISR Systems in May 2018. The DHS Privacy Office determined that ISR Systems do not contain Personally Identifiable Information. Additionally, the DHS Privacy Office found that Privacy Impact Assessment (PIA) coverage is provided for ISR Systems by three other PIAs that address the privacy risks of ingesting global positioning system data; provide general notice regarding CBP's use of radar, sensors, and other surveillance technologies; and provide notice of CBP's deployment of surveillance technologies on UASs.

The draft report contains ten recommendations, with which CBP concurs. Attached is our detailed response to the recommendations. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: Management Response to Recommendations Contained in (Project No. 18-043-ITA-CBP)

The Office of Inspector General (OIG) recommended that the CBP Privacy Office:

Recommendation 1: Provide documentation showing completion of a privacy threshold assessment with a determination regarding privacy requirements for ISR Systems.

Response: Concur. On May 14, 2018, the DHS Privacy Office approved a Privacy Threshold Assessment (PTA) conducted by the CBP Privacy Office for the CBP Intelligence, Surveillance, and Reconnaissance (ISR) Systems. The DHS Privacy Office determined that the CBP ISR Systems do not contain Personally Identifiable Information.

Supporting documentation was previously provided to OIG under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

The Office of Inspector General (OIG) recommended that the CBP's Chief Information Officer:

2



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 2: Develop a process for ensuring all information systems are included in the CBP Office of Information Technology inventory, along with notification to the CBP Privacy and Diversity Office when a system is added.

Response: Concur. CBP's Office of Information and Technology (OIT) will develop a process for ensuring all information systems are included in the official CBP OIT Federal Information Security Management Act (FISMA) system inventory.

CBP's Cyber Security Directorate (CSD) Security Operations Center (SOC) Vulnerability Assessment Team (VAT) will create a bi-weekly dashboard showing detected, unauthorized systems. The dashboard will highlight decentralized servers and systems without the Tanium agent. CSD will reach out to CBP Privacy and Diversity Office (PDO) to discuss its role and inclusion in the updated FISMA Inventory Standard Operating Procedure (SOP) and will update the FISMA Inventory SOP.

CBP's Chief Information Officer will issue a memo regarding security compliance and communication failures when an unauthorized system is detected on the CBP network, and determine the course of action for the issuance of a memo to CBP community. Estimated Completion Date (ECD): December 31, 2019.

The Office of Inspector General (OIG) recommended that CBP's Air and Marine Operations Executive Assistant Commissioner:

Recommendation 3: Create a plan to establish programmatic and system ownership and ensure appropriate oversight of ISR Systems.

Response: Concur. CBP's Air and Marine Operations (AMO) has established programmatic and system ownership of ISR Systems, ensuring appropriate oversight. As the OIG learned during its site visit to the Air and Marine Operations Center (AMOC) in November 2017, AMO officials were already in the process of assuming programmatic ownership of ISR Systems. In May 2017, an AMO official was designated System Owner of ISR Systems and an AMOC contractor was designated the Information Systems Security Officer (ISSO) for ISR Systems.

In November 2017, DHS approved AMO's development change request to include ISR Systems CBP's inventory, and issued a FISMA ID. DHS Office of Chief Information Officer notified CBP's OIT of this approval on November 7, 2017.

Further, DHS requires CBP and other components to use its Information Assurance Compliance System (IACS) to develop, maintain, and monitor Security Authorization Packages (SAP) for all Sensitive but Unclassified (SBU) Information Technology (IT) systems. DHS granted the ISR Systems ISSO access to IACS in November 2017.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Finally, CBP has added ISR Systems to its Investment Evaluation, Submission, and Tracking (INVEST) system for IT business case information and portfolio management.

Supporting documentation was previously provided under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

Recommendation 4: Provide a plan, including timelines, for fulfilling supporting requirements and obtaining authorization to operate ISR Systems.

Response: Concur. AMO is developing a number of documents needed to obtain an authorization to operate (ATO) through the formal DHS/CBP IACS process. AMO has a Plan of Action & Milestone (POA&M) that includes the completed PTA for ISR Systems and its System Privacy Plan. The POA&M includes timelines for obtaining authorization for operating ISR Systems.

Supporting documentation was previously provided under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

Recommendation 5: Create and implement a process according to DHS policy for timely installing software patches on the VADER and Minotaur systems.

Response: Concur. AMO has created a process for timely, 90-day installation of software patches on the VADER and Minotaur system. Both Minotaur and Vehicle and Dismount Exploitation Radar (VADER) originated from and continue to be supported by the Department of Defense (DoD). CBP has, and continues to maintain identical patching cycles to coincide with DoD's 90-day software patch cycle. Current CBP contracts with Johns Hopkins University Applied Physics Laboratory (for Minotaur) and Northrop Grumman Corporation (for VADER) have Navy and Army sponsors that fund the bulk share of the software development for both programs. Changing the cycle time from 90 days to 30 days would force the two vendors to provide disparate code for DoD and CBP customers (additionally, such a change would be cost prohibitive).

To maintain DoD and CBP integrity and current efficiencies detailed in OIG's draft report, AMO has prepared a request to CBP OIT for approval to implement a timely software patch cycle of 90 days for Minotaur and VADER.

AMO's request is supported by DHS 4300A, Policy ID 3.7.c. "Information security patches are installed in accordance with CM (Configuration Management) plans and within the timeframe or direction stated in the Information Security Vulnerability Management (ISVM) message published by DHS ESOC (Enterprise Security Operations Center)." ECD: June 30, 2019.

Recommendation 6: Create and implement a process to update all ISR System subsystems currently running on unsupported operating systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response: Concur. AMO has created and implemented a process to update all ISR Systems subsystems currently running on unsupported operating system. ISR Systems are continuously scanned for compliance and determination of end-of-support, and system hardware and software inventory is used to plan system lifecycles to maintain compliance. The transition from Ocean Surveillance Initiative's (OSI) unsupported legacy software to the supported Minotaur system is programmed to occur no earlier than December 2018, by contract. Should ISR Systems receive an ATO before the contracted date in December 2018, AMO will prioritize the removal of OSI from service and accept an operational capability gap until the scheduled transition is complete. ECD: January 30, 2019.

Recommendation 7: Create a plan for filling key IT positions and allocating sufficient budget and staff resources to perform duties required to safeguard ISR Systems and the data it collects and stores.

Response: Concur. AMO has filled its three key IT positions and has allocated sufficient budget and staff resources. ISR Systems currently have a System Owner, an ISSO, and Security Controls Assessor (SCA). As for budget resources, AMO presents an annual funding request "to fortify AMOC capabilities [to] more efficiently process increased data from Intelligence, Surveillance, and Reconnaissance (ISR) activities" through CBP's budget process.

Supporting documentation was previously provided under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

Recommendation 8: Create a plan for providing oversight of all contractors who assist in performing duties required to safeguard ISR Systems and the data it collects and stores.

Response: Concur. AMO continues to have oversight of all contractors who assist in performing duties required to safeguard ISR Systems and the data collected and stored. At the AMOC, contractors with administrative rights on ISR Systems have been functionally aligned under the AMOC Systems Division to ensure change control process and security practices are followed. Separation of duties between system administrators, engineers, and the ISSO are maintained in accordance with least privilege and separation of duties concepts, which is illustrated in AMO's functional organization charts. Additionally, AMO has lines of reporting for maintenance and other contractors at the National Air Security Operations Center.

Supporting documentation was previously provided under separate cover. We request that the OIG consider this recommendation resolved and closed as implemented.

Recommendation 9: Develop and implement a plan to conduct specialized training for personnel responsible for the security and maintenance of ISR Systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response: Concur. AMO has identified personnel with system security responsibilities, and will provide annual training that is a combination of existing Performance and Learning Management System (PALMS) requirements and tailored role-based training. ECD: January 30, 2019.

Recommendation 10: Develop and implement standard operating procedures for sustaining operations and ensuring ISR Systems comply with Federal and DHS information security policy.

Response: Concur. AMO is developing standard operating procedures for sustaining operations, including existing SOPs to be inherited and expanded to include ISR Systems. ECD: August 30, 2019.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
List of Unauthorized Removable Media Devices
Used to Access ISR Systems

Type of Device	Product Names
Flash Drives	<ul style="list-style-type: none">• Kingston DataTraveler 2.0 USB Flash Drive• Kingston DT Ultimate G3 USB Flash Drive• Lexar USB Flash Drive Flash Drive• LOK-IT Secure USB Flash Drive• Patriot Memory USB Flash Drive• SanDisk Cruzer USB Flash Drive• SanDisk Enterprise Federal Information Processing Standards USB Flash• SanDisk Ultra USB Flash Drive• Toshiba TransMemory USB Flash Drive
Removable Hard Drives	<ul style="list-style-type: none">• Buslink USB 3.0 External Hard Drive• Defender H100 USB External Hard Drive• Maxtor OneTouch III USB External Hard Drive• Samsung SSD 850 Pro USB Hard Drive• Samsung SSD 850 EVO USB Hard Drive• OCZ-VERT EX USB Hard Drive• Seagate BUP Slim USB External Hard Drive• Seagate FreeAgent GoFlex USB External Hard Drive• WD Elements External Hard Drive• WD My Passport External Hard Drive
Mobile Phones	<ul style="list-style-type: none">• Apple iPhone• LG Phone• Samsung Phone

Source: DHS OIG-generated based on testing of ISR Systems and comparison of results against AMO's list of authorized removable media devices



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D
Office of IT Audits Major Contributors to This Report

Richard Saunders, Director
Jaquone Miller, Audit Manager
Hoa Do, Senior Auditor
Brian Smythe, Program Analyst
Daniel McGrath, Program Analyst
Leah Garrison, Auditor
Thomas Rohrback, Chief, Information Assurance and Testing
Jason Dominguez, IT Specialist, Information Assurance and Testing
Beverly Burke, Referencer



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
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
Chief Privacy Officer

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