

Office of Health Affairs Has Not Implemented An Effective Privacy Management Program





DHS OIG HIGHLIGHTS

Office of Health Affairs Has Not Implemented An Effective Privacy Management Program

November 30, 2017

Why We Did This Audit

We evaluated the Office of Health Affairs' (OHA) privacy safeguards for protecting the personally identifiable information (PII) it collects and maintains. Our objective was to determine whether OHA ensures compliance with applicable Federal privacy laws, regulations, and policies.

What We Recommend

We are making 11 recommendations to OHA which, if implemented, should reduce privacy risks to the PII it collects and maintains.

For Further Information:

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

What We Found

OHA has not implemented an effective organizational framework for safeguarding PII in accordance with Federal requirements. OHA appointed a Privacy Officer, but this official lacks adequate authority and resources to carry out the various required privacy management responsibilities. This official also has not received OHA senior leadership support to issue the policies and procedures needed for effective organization-wide privacy management. Further, there was no central tracking to ensure that all employees completed annual privacy training and to accurately report this information to the Department and Congress as required. Given turnover in several key positions, senior leadership has not placed priority on addressing such issues and instilling a culture of privacy to ensure compliance with privacy protection laws, regulations, and policies.

These organizational shortfalls have resulted in a lack of transparency and security controls for protecting personally identifiable information OHA-wide. For example, OHA did not require DHS emergency medical first responders to properly notify patients of their privacy rights as required upon collecting their sensitive personal and medical information. Strong authentication protocols were not present to control access to a key OHA system and the sensitive data it processed. Further, OHA's public web portal was improperly categorized and potentially lacked the controls needed to effectively secure the information it contained against privacy risks. The portal also operated on a non-secure site. Until steps are taken to address these information and system control deficiencies, the sensitive PII that OHA collects and maintains will remain at risk.

OHA Response

Appendix B provides a copy of OHA's response to our report. OHA concurred with all 11 recommendations.



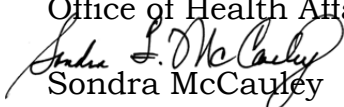
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

November 30, 2017

MEMORANDUM FOR: Larry Fluty
Assistant Secretary and Chief Medical Officer (Acting)
Office of Health Affairs

FROM: 
Sondra McCauley
Assistant Inspector General,
Information Technology Audits

SUBJECT: *Office of Health Affairs Has Not Implemented An
Effective Privacy Management Program*

Attached for your action is our final report, *Office of Health Affairs Has Not Implemented An Effective Privacy Management Program*. We incorporated the formal comments provided by your office.

The report contains eleven recommendations aimed at improving OHA's privacy management and reducing the risk to personally identifiable information it collects and maintains. Your office concurred with all eleven recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 and 3 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Further, based on the information provided in your response, we consider recommendations 2 and 4 through 11 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Please send your response or closure request to
OIGTAuditsFollowup@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 Richard Saunders, Director, Advance Technology Audits, at (202) 254-5440.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table of Contents

Background	1
Results of Audit	6
OHA Has Not Made Privacy Management a Priority	6
Lack of Priority on Privacy Management Poses Risks to Sensitive OHA Systems and Information	11
Recommendations.....	18

Appendixes

Appendix A: Objective, Scope, and Methodology	25
Appendix B: OHA Comments to the Draft Report	26
Appendix C: Office of IT Audits Major Contributors to This Report	30
Appendix D: Report Distribution.....	31

Abbreviations

BAR	BioWatch Actionable Result
EMS	emergency medical services
ePCR	Electronic Patient Care Reporting
GAO	Government Accountability Office
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCISO	Office of the Chief Information Security Officer
OHA	Office of Health Affairs
OIG	Office of Inspector General
PALMS	Performance and Learning Management System
PII	personally identifiable information
PIV	personal identity verification
PTA	Privacy Threshold Analysis



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

Established in 2007, the Office of Health Affairs (OHA) is the Department of Homeland Security's principal authority for all medical and health issues.¹ OHA's mission is to advise, promote, integrate, and enable a safe and secure workforce and nation.

OHA Responsibilities

Composed of about 100 staff members, OHA is among the Department's smallest organizations; however, it has wide-ranging responsibilities. In pursuit of national health security, OHA is responsible for leading DHS efforts to meet health security threats caused by terrorist attacks, natural disasters, and pandemic diseases. OHA coordinates and monitors emergency health response for nuclear, biological, chemical, and other agents and public health threats, such as anthrax, Ebola, and the plague. OHA provides medical countermeasures for the DHS workforce and those under DHS care and custody in the event of a biological incident, such as an area-wide aerosolized anthrax attack, and facilitates training such as "stop the bleed" to educate employees on how to respond in case of bodily harm. It also coordinates DHS health response efforts with the Centers for Disease Control and Prevention, and works with city, state, local, tribal, and other stakeholders regarding health security continuity of operations and best practices.

The Medical First Responder Coordination Branch within OHA supports the Department's emergency medical services (EMS) provided by first responders trained in emergency preparedness and immediate health countermeasures. The Department's EMS system comprises more than 3,500 pre-hospital and emergency medical services personnel. EMS personnel perform their medical duties along with law enforcement responsibilities in diverse, austere, and often dangerous environments, such as active shooter incidents. EMS personnel include emergency medical technicians at the basic, intermediate, and paramedic levels. OHA monitors the consistency and quality of services provided by EMS personnel. Figure 1 illustrates how DHS components are actively involved with the DHS EMS system.

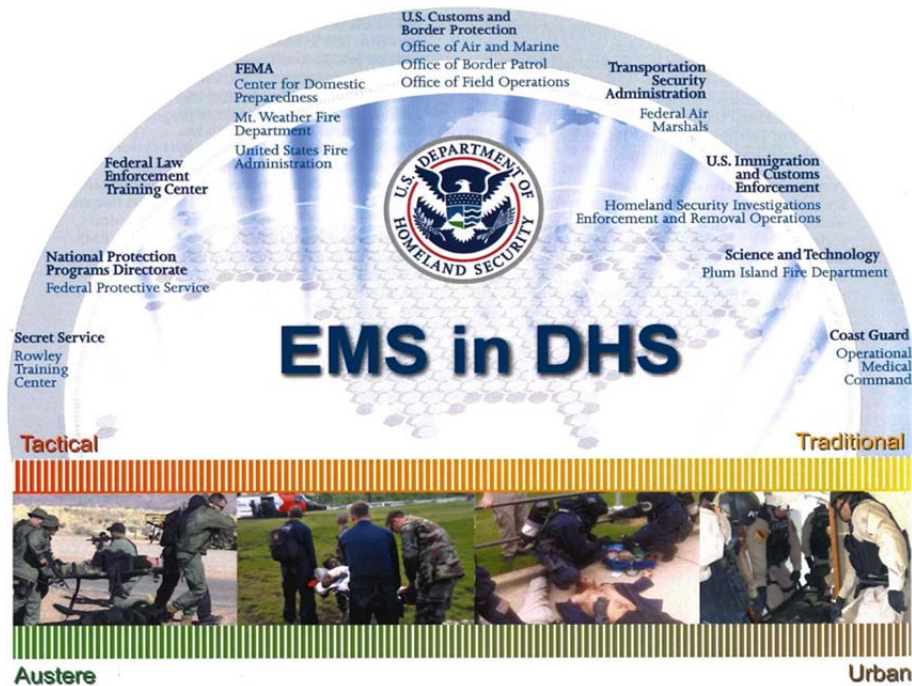
¹ The *Post-Katrina Emergency Management Reform Act* (PKEMRA) (P.L. 109-295), enacted on October 4, 2006, as title VI of the *2007 DHS Appropriations Act*, authorized the appointment of a Chief Medical Officer and established the Chief Medical Officer's responsibilities. This statutory authority is codified at 6 United States Code (USC) § 321e.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 1: DHS Components Included in the EMS Strategic Framework



Source: OHA, Medical First Responder Coordination Branch Chief

OHA Privacy Systems and their Data

Effective privacy information management is critical to accomplishing OHA's mission. OHA currently manages two major applications that collect or maintain privacy information: the Emergency Patient Care Reporting System and the BioWatch Web Portal. Table 1 provides an overview of each system, its data sources, and the type of information collected.

Table 1: Overview of OHA Systems that Store Privacy Information

System	OHA Data Source	Collected From Whom?	What Data May Be Collected?
Emergency Patient Care Reporting System	DHS medical providers collect personally identifiable information directly from the patient.	DHS and other Federal employees, as well members of the public who are treated by on-duty EMS health care providers.	Medically-relevant information may include name, date of birth, age, gender, location, address, medications, allergies, type and assessment of injury, chief complaint, vital signs, treatment, and medications administered.
BioWatch Web Portal	Federal, state, and local Stakeholders.	Stakeholders who sign up for BioWatch portal user accounts.	Names, work email addresses, and work phone numbers of stakeholders.

Source: Office of Inspector General (OIG)-compiled from OHA documentation



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Emergency Patient Care Reporting System

The Electronic Patient Care Reporting (ePCR) system is OHA's foremost system for supporting emergency first responder care. EMS providers collect personal and medical health information from patients on a standard hardcopy form.² EMS providers then input the patients' information and details of any care provided to them into the ePCR system, which OHA manages. At the time of our audit, OHA had a current Privacy Impact Assessment detailing the collection and maintenance of the personal and medical information captured in the ePCR system.

OHA uses sanitized reports from the ePCR system to monitor the quality and consistency of EMS care provided.³ If a patient requires transfer to an emergency room, DHS emergency personnel give a copy of the form, documenting the medical care they provided, to other EMS or hospital emergency room staff.

The BioWatch Web Portal

The BioWatch web portal is another means through which OHA collects personally identifiable information (PII). The BioWatch program was established in 2003 in the aftermath of the 2001 bioterrorism (i.e., anthrax) attacks in the Washington, DC; New York, NY; and West Palm Beach, FL, metropolitan areas.⁴ OHA acquired responsibility for the BioWatch program in 2007. The BioWatch Program helps public health and emergency management communities prepare for and respond to biological incidents. Its mission is to operate a nationwide, aerosol detection system to provide early warning across all levels of government. The system uses approximately 600 detectors and collection devices deployed to more than 30 U.S. cities.

BioWatch detectors sample the air for various aerosolized bio-threat agents. Exposed samples are collected daily and delivered to designated BioWatch laboratories for analysis. The detection of a biological agent by the BioWatch Program is referred to as a BioWatch Actionable Result (BAR).⁵ If harmful

² OHA is not a "covered entity" under the *Health Insurance Portability and Accountability Act*, P.L. 104-191. Specifically, EMS providers do not bill or charge for services rendered, nor do they electronically transmit PII collected and stored in ePCR. See 45 Code of Federal Regulations (CFR) § 160.103.

³ Quality management reports from ePCR do not include PII.

⁴ These anthrax attacks killed 5 people and sickened more than 20 others.

⁵ A BAR is defined as one or more polymerase chain reaction-verified positive results from a single BioWatch collector that meets the algorithm for one or more specific BioWatch agents. If polymerase chain reaction-verified positive results are obtained for two BioWatch agents on a single collector, this is considered one BAR.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

bacteria exist and a BAR is declared, the BioWatch program assists public health experts in determining the presence and geographic extent of the biological agent released. Once the situation is assessed, a response is agreed upon, and initial response actions are implemented, BioWatch officials transfer control to the local jurisdiction. According to OHA, since 2003, BioWatch has identified about 150 positive BAR incidents that have been environmental, not intentional human releases of harmful agents.

The BioWatch program partners with public health organizations, first responders, law enforcement personnel, and local officials at all levels. Federal partners include the Federal Bureau of Investigation, the Centers for Disease Control and Prevention, the Environmental Protection Agency, the Department of Health and Human Services, and the Department of Defense. State and local jurisdictions work with these Federal stakeholders to ensure overall resilience of the program's operations and coordinated response efforts. Each BioWatch jurisdiction has established a BioWatch Advisory Committee — a group of stakeholders and external partners — that convenes regularly to discuss and review operations and response plans. Coordination among these players is intended to result in communities that are better prepared for a biological attack *and* an all-hazards response.

Stakeholders use the BioWatch web portal as a communication tool. Each stakeholder may create an account to access and use the BioWatch portal. This process includes providing OHA with a work email address and other contact information to facilitate information sharing. The contact information is maintained on the BioWatch portal. According to one OHA official, 90 percent of the information posted to the portal is uploaded or posted by regional stakeholders. OHA officials explained that BAR results posted to the portal are considered Sensitive but unclassified and are marked “For Official Use Only.”

Privacy Management Requirements

The *Privacy Act of 1974*, 5 USC 552a, and the *E-Government Act of 2002* (P.L. 107-347), impose various requirements on agencies whenever they collect, use, maintain, or disseminate PII that contains the name of an individual or some number, symbol, or other identifier. The Department defines PII as “any information that permits the identity of an individual to be directly or indirectly inferred.”⁶ This includes any information that can be “linked or [is] linkable to an individual regardless of whether the individual is a U.S. Citizen, lawful permanent resident, visitor to the United States, or employee or contractor to the Department.” DHS defines Sensitive PII as a particular type of PII, “which if

⁶ DHS 4300A Sensitive Systems Handbook Version 12.0 (November 2015).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.”

The *Privacy Act* is based on Fair Information Practice Principles that provide the privacy policy framework for DHS. These principles include transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability and auditing. *DHS 4300A Sensitive Systems Handbook* Version 12.0 (November 2015) and its implementing instruction also establish security over information systems as required by the *Homeland Security Act of 2002* (P.L. 107-296), the *Federal Information Security Modernization Act of 2014* (P.L. 113-283), and other legal authorities.

Related Audits

In its February 2017 high-risk series, the Government Accountability Office (GAO) reported that Federal agencies had made progress —

- demonstrating top leadership commitment to protecting the privacy of PII,
- improving capacity for protecting information systems and PII,
- instituting corrective action plans to improve the protection of cyber assets and PII,
- implementing programs to monitor corrective actions related to cybersecurity and PII protections, and
- demonstrating progress in implementing the requirements for the security of Federal systems and networks.⁷

GAO also reported agencies had taken action to address 8 of 23 recommendations for improving their responses to PII breaches. Although GAO included DHS among the various Federal agencies that needed to improve their PII handling, GAO did not specifically mention any components within the Department in its high-risk reporting.

We evaluated OHA privacy safeguards for protecting the PII it collects and maintains. The objective of our audit was to determine whether OHA ensures compliance with applicable Federal privacy laws, regulations, and policies.

⁷ GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others* (GAO-17-317, February 2017).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Results of Audit

OHA has not implemented an effective organizational framework for safeguarding PII in accordance with Federal requirements. OHA has appointed a Privacy Officer, but this official lacks adequate authority and resources to carry out the various required privacy management responsibilities. This official also has not received OHA senior leadership support to issue the policies and procedures needed for effective organization-wide privacy management. Further, there was no central tracking to ensure that all employees completed annual privacy training and to accurately report this information to DHS and Congress as required. Given the turnover in several key positions, senior leadership has not placed priority on addressing such issues and instilling a culture of privacy to ensure compliance with applicable privacy protection laws, regulations, and policies.

These organizational shortfalls have resulted in a lack of transparency and security controls for protecting privacy information OHA-wide. For example, OHA did not require DHS emergency medical first responders to notify patients of their privacy rights upon collecting their sensitive personal and medical information. Strong authentication protocols were not present to control access to a key OHA system and the sensitive data it processed. Further, OHA's public web portal was improperly categorized and potentially lacked the controls needed to effectively secure the information it contained against privacy risks. OHA also hosted the portal on an untrusted internet site that was not secured behind DHS' firewall. Until steps are taken to address these information and system control deficiencies, the sensitive PII that OHA collects and maintains will remain at risk.

OHA Has Not Made Privacy Management a Priority

OHA has not ensured an effective governance structure for safeguarding privacy information. Specifically,

- OHA's Privacy Officer lacks adequate authority and resources to carry out required privacy management responsibilities;
- OHA senior leadership has not approved and disseminated the policies and procedures needed for effective organization-wide privacy management; and
- OHA did not centrally track and accurately report its employees' completion of annual privacy awareness training as required.

Given the turnover in several key positions, OHA senior leadership has not placed priority on addressing such matters to institute a culture of privacy and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

thereby ensure compliance with applicable privacy protection laws, regulations, and policies.

Privacy Officer Lacks Authority OHA-wide

Despite Federal and DHS requirements, OHA did not appoint its Privacy Officer with the authority to develop, implement, and maintain an organization-wide privacy program. OHA designated this GS-15 level official in June 2013. However, senior leadership at the time did not formally introduce this official or notify OHA staff of the Privacy Officer's appointment, authority, or responsibilities. Failing to do so, senior managers missed the opportunity to stress the importance that OHA program offices should coordinate with the Privacy Office in collecting, maintaining, sharing, and disposing of the PII that they routinely collect through automated and manual means in carrying out their respective mission responsibilities.

Privacy Policies and Procedures Not Approved

The OHA Privacy Officer developed internal OHA standard operating procedures for privacy in November 2016, but they remained in draft. This official also developed additional operating policies on privacy incident handling in May 2016 and on *Freedom of Information Act* issues in September 2016.⁸ Yet, as of June 2017, OHA senior leadership had not approved, disseminated, or implemented any of them.

In the absence of standard privacy guidance, OHA program offices were managing their privacy data as they deemed appropriate in a decentralized manner. According to the Privacy Officer, program office staff generally consulted when they encountered a problem, such as a potential privacy incident or a privacy clause missing in a contract. Program offices consulted with this official for component approval of privacy threshold analyses that are used to assess whether the system is privacy sensitive. Upon component approval, OHA forwards the document to the DHS Privacy Office for final approval and implementation. Nevertheless, the OHA program offices did not necessarily include the Privacy Officer in all privacy-related matters.

Privacy Office Lacks the Resources to Be Effective

OHA has not allocated adequate resources for the Privacy Officer to implement and maintain an organization-wide culture of privacy. Currently, this official reported having no budget but indicated that, at a minimum, funds were

⁸ Department-wide privacy policy and guidance is available on the DHS Privacy Office website.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

needed to obtain training and privacy certification for the Privacy Officer position. This official also worked alone with no staff. The Privacy Officer indicated needing at least one additional staff member to help carry out the various privacy management responsibilities. These responsibilities included coordinating with OHA program and system managers to complete privacy compliance documentation, assisting with and reviewing privacy threshold analyses, privacy impact assessments, and systems of records notices for accuracy and completeness. This official ensured that *Freedom of Information Act* requests were adequately addressed and privacy information was redacted as appropriate. The Privacy Officer maintained records of all OHA documents and systems containing PII. Among other requirements, this official also was responsible for making mandatory annual privacy awareness training available to all employees.⁹

OHA Has No Assurance Its Employees Took Annual Privacy Training

Within OHA, there was a lack of central tracking to ensure that all employees took mandatory annual privacy awareness training and that this information was accurately reported for accountability purposes. The OHA Privacy Office and the OHA Training Coordinator had shared responsibility in this regard. Nevertheless, between the two offices, there was no central tracking to ensure that the training was taken and its completion fully documented.

National Institute of Standards and Technology (NIST) and DHS policy require that organizations develop and implement a comprehensive training awareness strategy to ensure all personnel understand their privacy protection responsibilities. DHS employees and contractors are required to take such privacy and security awareness training annually. DHS requires that each component Privacy Officer subsequently report the number of component employees that have completed the mandatory training to the DHS Privacy Office for inclusion in its quarterly report to Congress.¹⁰

Additionally, according to the OHA *Professional Development Procedural Guide*, the OHA Training Coordinator is required to perform the following:

⁹ See DHS Privacy Policy Instruction 047-01-005 for a complete list of Component Privacy Officer responsibilities.

¹⁰ As required by Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, P.L. 110-53. See 42 USC 2000ee-1(f).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Ensure compliance with applicable laws, regulations, and policies with regard to mandatory training, job-related training, tuition assistance, certifications, licenses, and advanced professional development.¹¹
- Maintain mandatory training completion data for all OHA Federal employees and contractors. Provide monthly status reports to OHA's Chief of Staff and Division Directors.
- Maintain training records and approval of expenditures for all OHA Federal employees and contractors.

The procedural guide states that employees who do not complete mandatory training may be subject to appropriate corrective action. After taking the training, OHA requires that each employee forward a copy of the completion certificate or other proof of attendance to the OHA Training Coordinator.

The OHA Privacy Office and the Training Coordinator should work in tandem to ensure office-wide fulfillment of the annual privacy awareness training requirement. However, we found this was not happening. The OHA Training Coordinator did not centrally track or maintain mandatory training completion data (e.g., privacy training completion certificates) as the *Professional Development Procedures Guide* requires. Rather, the OHA Training Coordinator reported to the Chief of Staff on privacy training completion using reports generated through DHS's online training system, the Performance and Learning Management System (PALMS). The Training Coordinator recognized and admitted to us that PALMS was not reliable for capturing training completion data.

For example, the Training Coordinator explained that sometimes PALMS locked up at the end of a training session, and when this occurred, the training completion certificate might not be available or the employee's training history in PALMS might not reflect all completed training. We asked whether OHA enforced the requirement that staff delinquent in completing required training take action to do so. This OHA official responded that they could not generate a PALMS report to identify staff delinquent in training, and as a result, OHA did not enforce mandatory training. Further, the official implied that certain staff had not taken required training in the past 3 years. We recently reported that

¹¹ OHA *Professional Development Procedural Guide* delegates these responsibilities to the Office of Human Capital. However, according to OHA's Human Capital Director, the Training Coordinator is responsible for performing these functions.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

despite spending \$24.2 million, PALMS did not achieve intended benefits or address the Department's training needs.¹²

The OHA Privacy Officer also did not review OHA employees' privacy training completion certificates, but instead relied on each supervisor's quarterly accounting to affirm that their staff had completed mandatory privacy training. The Privacy Officer used this imprecise information to report on OHA employee privacy training completion to the DHS Privacy Office for inclusion in its quarterly report to Congress.

Until we alerted them in July 2017, OHA senior leaders were unaware of this lapse in accountability for accurately ensuring annual privacy training completion. They agreed that, given the relatively small size of the OHA organization, this was a deficiency they could readily correct. Until they address this issue, however, OHA will remain unable to ensure that all OHA employees are trained as required and adequately recognize the importance of privacy management, and that reporting in this regard to DHS and Congress is accurate.

Lack of Senior Leadership Priority on Ensuring Effective Privacy Management

OHA officials we interviewed attributed the lack of priority for ensuring an effective organization-wide privacy program in part to turnover in key positions. According to OHA's Privacy Officer, prior to June 2013, one OHA employee had privacy management as one of many additional responsibilities and, as such, it did not receive much attention. The OHA Acting Assistant Secretary in place when a Privacy Officer was first appointed in June 2013 was in the process of leaving the agency and did not prioritize the creation of the new Privacy Office. The Privacy Officer indicated that such turnover in key positions resulted in delays getting privacy policy and procedures approved and disseminated. Two senior OHA officials — the Chief of Staff and the Acting Assistant Secretary for OHA — that we recently interviewed indicated they had only been with OHA for less than a year and a half. Neither official could explain why OHA had not emphasized the importance of building privacy into OHA operations.

Nonetheless, the Chief of Staff said OHA has begun to recognize the importance of effective privacy management. To illustrate, the Privacy Officer told us the Chief of Staff recently emphasized that program offices route contracts to her office to ensure they contain required privacy clauses. Further, the Acting Assistant Secretary indicated a willingness to issue a letter outlining the

¹² *PALMS Does Not Address Department Needs*, DHS OIG-17-91, June 30, 2017.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Privacy Officer's authority and responsibilities. This official also was open to conducting town hall meetings with all program staff to stress the importance of working collaboratively with the Privacy Office on issues related to their respective programs and systems. As of July 2017, such actions had not been initiated.

A Culture of Privacy Is Needed at OHA

Without a strong top-down organizational approach to instilling a culture of privacy, OHA cannot ensure compliance with Federal laws and regulations for protecting privacy information. Without authority and resources to implement an organization-wide privacy program, the Privacy Officer cannot ensure OHA program offices consistently and appropriately collect, use, maintain, share, and dispose of privacy information in carrying out their respective mission responsibilities. Moreover, OHA cannot demonstrate organizational commitment to minimizing privacy risk.

Lack of Priority on Privacy Management Poses Risks to Sensitive OHA Systems and Information

Without an effective governance structure, OHA lacked transparency and security controls for protecting privacy information organization-wide. For example,

- OHA did not require DHS emergency medical first responders to notify individuals of their privacy rights upon collecting their sensitive personal and medical information;
- strong authentication protocols were not present to control access to the ePCR system and the sensitive data it processed; and
- remote access controls were missing to limit ePCR system access to authorized users only.

Further, the BioWatch web portal did not have the proper risk category and potentially lacked the controls needed to effectively manage privacy risk. OHA also did not host the portal on a trusted site behind DHS' firewall. Until steps are taken to address these information and systems control deficiencies, the sensitive PII that OHA collects and maintains will remain at risk.

ePCR System Control Weaknesses

We found that a number of controls were missing related to collecting patient data and safeguarding records of patient care in the ePCR system. Given such deficiencies, patients lacked assurance that their medical information collected



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

by first responders would be properly maintained. Also, OHA could not ensure that the system used to store patient data had the proper safeguards in place to prevent unauthorized access and misuse of the information.

Patients Did Not Receive Privacy Act Statements as Required

Recipients of emergency care did not receive privacy statements as required. The *Privacy Act* requires that organizations provide notice to each individual from whom they collect privacy information on how they intend to use and maintain that information.¹³ When providing medical care, EMS providers may collect and record PII and medical information, such as name, date of birth, duty station, and past medical history on a standard hardcopy form. Per the *Privacy Act*, EMS personnel are required to give the patient a Privacy Act Statement at the time of care, either on the form used to collect the PII or on a separate form that explains the following:

- the authority (whether by statute or executive order) authorizing the solicitation of the information and whether the disclosure of such information is mandatory or voluntary;
- the principal purpose for collecting the information;
- how the information will be used; and
- the effects, if any, of not providing all or any part of the requested information.

Despite these requirements, OHA did not require DHS first responders to provide recipients of medical care a copy of the Privacy Act Statement. An OHA official we interviewed told us that while first responders typically provided patients with copies of the standard form documenting their personal information and the care received, when requested, they did not include the Privacy Act Statement. According to this official, the law enforcement mission and the quality of care provided is the first priority of EMS personnel. This official said that first responders generally administer emergency care under extreme and unusual circumstances; it was not clear how emergency personnel were to transport this paperwork and hand it out to patients during medical response. A card or privacy notice flyer containing this information also had not been created.

Further, according to DHS *Emergency Medical Services System Strategic Framework*, the primary focus of EMS providers is to protect and serve the DHS workforce. They also provide services to the general public in the case of natural disaster or terrorist attack. Nonetheless, the OHA Medical First

¹³ See 5 U.S.C. §552a (e)(3).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Responder Coordination Branch Chief indicated that most of the emergency care they give is to undocumented aliens who may be in the process of being apprehended. These undocumented aliens may not want to reveal their actual names and identities and also may not be able to read or speak English, rendering efforts to comply with the *Privacy Act* notification requirement a futile activity.

Despite these difficulties in providing Privacy Act Statements to recipients of emergency care, the requirement is mandated in Federal law. Given the lack of compliance, individuals may be unaware that their personal and medical information is maintained in a government information system, is used for specific purposes, and may remain accessible for future purposes.

ePCR System Authentication Protocols Were Not in Place

OHA did not have strong authentication controls in place for its ePCR system. Homeland Security Presidential Directive 12 sets policy for and instructs the Department of Commerce, in conjunction with other agencies, to implement a common identification standard for Federal employees and contractors. This standard is in the form of the personal identity verification (PIV) card, a common means of authenticating access to agency facilities, networks, and information systems. In excepted instances, systems may be waived from this requirement if being decommissioned. DHS also requires alternate authentication such as strong passwords on its information systems. In addition, the *DHS 4300A Sensitive Systems Handbook* requires that all new information systems are PIV-enabled before they are put into production.

Despite these requirements, OHA did not use strong passwords or PIV authentication to authorize user access to its ePCR system. OHA's Medical First Responder Coordination Branch Chief stated they did not implement strong passwords or PIV-enable the ePCR system since it would be decommissioned and replaced with a new system by the end of fiscal year 2017. In the interim, they were using weak passwords, non-compliant with Department policy, because they had not updated their password security requirements.

Until the ePCR system is decommissioned and replaced, OHA can strengthen its privacy protections for PII by enforcing strong passwords on all systems that are not PIV-enabled. Without the use of strong authentication controls, OHA is at an increased risk of internal or external users gaining unauthorized access and abusing or misusing personal and medical information.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Access Control Needed to Limit ePCR System Access

OHA did not limit ePCR system access as required. According to the ePCR system security plan, no personal mobile devices should be used for access, and only DHS-owned devices would be able to connect to the system.¹⁴ However, we were able to access the ePCR system using a non-authorized personal computing device and an OHA-supplied login and password.¹⁵ We did not examine the system's contents using this device because this was prohibited. OHA staff had already shown us that the ePCR system contained personal and medical information that EMS providers had collected, as well as treatment and medications they had provided to patients.¹⁶

When alerted, one OHA official acknowledged being aware of this vulnerability. When asked why the risk had not been mitigated, the official indicated that the DHS Office of the Chief Information Officer (OCIO), not OHA, was responsible for maintaining system security. However, we determined that the *Federal Information Security Modernization Act* places responsibility for data protection on the system owner, not the entity administering the system on which the data is stored.¹⁷ As the system owner, OHA should have taken action to remediate the ePCR system access control vulnerability in coordination with OCIO.

Lacking this access control, OHA could not prohibit employees from using unauthorized mobile computing devices to connect to the ePCR, which contained sensitive PII and medical information. This vulnerability placed such information at risk, since unauthorized mobile devices may not meet DHS security standards and may contain malware, Trojan horses, or computer viruses. Moreover, if employees were to use a public network or domain to connect to the ePCR system via these unauthorized devices, their login credentials could be stolen by individuals not affiliated with OHA.¹⁸ Unauthorized individuals could then use the credentials to access and potentially misuse the sensitive and privacy information contained in the ePCR system.

¹⁴ NIST 800-53, *Security and Privacy Controls for Federal Information Systems*, version 4, dated April 2013.

¹⁵ The personal computing device we used was an Apple iPad.

¹⁶ EMS providers collect the minimal information necessary to document the patient and care provided.

¹⁷ P.L. 107-347, codified as 44 USC § 3541, et seq., as amended by P.L. 113-283. See 44 USC § 3554

¹⁸ For example, a public WiFi connection may offer no protection to the user.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

BioWatch System Control Weaknesses

OHA's BioWatch portal, used to help prepare for and respond to biological incidents, was not categorized appropriately and therefore may not include all of the controls needed to safeguard against privacy risks. OHA also hosted the portal on an untrusted website that was not secured behind DHS' firewall. Steps are needed to address these deficiencies and better protect the PII that OHA collects and maintains on the system.

Improperly Categorized BioWatch Portal Potentially Lacked Controls for Protection against Privacy Risk

The BioWatch portal did not have the appropriate risk category needed to ensure effective controls for protecting the PII contained in the system. DHS 4300A states that any information system containing PII must be categorized, at a minimum, as having moderate risk for ensuring the confidentiality of that information. Security controls for protecting the PII stored on the system from unauthorized access and disclosure must be commensurate with that moderate risk rating.¹⁹

Despite this requirement, OHA categorized its BioWatch web portal as having low security risk for confidentiality, even though it contained work email addresses and other contact information. DHS Privacy and Security guides do not specifically include or exclude work contact information as PII, leaving them ambiguous and left to interpretation. However, according to the DHS Privacy Office, such information constitutes PII requiring that, at a minimum, the system storing it be categorized at moderate risk for potential loss of confidentiality. With a moderate risk rating, additional security controls are required beyond those for systems categorized at the low risk level.

An official from the DHS Privacy Office went on to say that DHS defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department." As such, using this definition, a work email address, which contains an individual's name, is PII. The DHS Privacy Office does not recognize

¹⁹ NIST 800-53, *Security and Privacy Controls for Federal Information Systems*, version 4, dated April 2013.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

the “rolodex exemption” that some agencies opt to use to categorize systems containing work contact information as low risk.²⁰

When we advised OHA of this vulnerability, the agency Chief Information Officer told us that he did not consider work emails and other work contact information PII, or believe that systems storing this information should be managed as privacy sensitive. The Chief Information Officer also stated that OHA had updated the BioWatch Privacy Threshold Analysis (PTA) in July 2016 and requested that the system be re-categorized as a non-PII system. In response, the DHS Privacy Office approved the BioWatch PTA, but also commented that the system was privacy-sensitive and should be categorized as moderate for confidentiality. Rather than approving the BioWatch PTA for the normal 3-year period, DHS Privacy gave the PTA an expiration date of 1 year, allowing OHA time to bring the portal into compliance with the moderate risk control requirements.

OHA did not take action in response to the DHS Privacy Office’s comments on the PTA. The current OHA Chief Information Officer, new to the agency since January 2017, had not thoroughly reviewed the PTA and was unaware that the BioWatch system was considered a privacy system. Nonetheless, this official advised that, to address a potential privacy incident, the agency was coordinating with the DHS OCIO to conduct a full vulnerability assessment that would ultimately determine the appropriate risk category for the BioWatch portal.

By failing to appropriately categorize BioWatch system risk commensurate with the information stored in the system, OHA could not ensure that adequate security controls were instituted to safeguard the privacy sensitive system. Inadequate security controls increased the risk of unauthorized access, which could result in identify theft, destruction, or misuse of PII.

BioWatch Portal Not Secure

The BioWatch portal was not hosted on a trusted website. Secure hosting was needed to safeguard sensitive BAR results, work emails, and other contact information that the portal contained. DHS 4300A requires that any direct

²⁰ Office of Management and Budget M-07-16, Footnote 6, establishes the flexibility for an organization to determine the sensitivity of its PII in context using a best judgment standard. The example provided in M-07-16, Footnote 6 addresses an office rolodex and recognizes the low sensitivity of business contact information used in the limited context of contacting an individual through the normal course of a business interaction. The “rolodex exception” is a scoping decision that, when applicable, helps organizations avoid unnecessary expenditures of resources based on a risk determination for this limited subset of PII.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

connection between the internet or extranets and DHS One Net, DHS networks, or DHS mission systems occur through DHS Trusted Internet Connection Policy Enforcement Points.²¹

Despite this requirement, OHA has hosted its BioWatch portal on a non-governmental “.org” site located outside of the DHS firewall since 2007. Years ago, OHA officials explored the idea of moving the BioWatch portal inside the DHS firewall. However, OHA opted to leave the portal where it was given stakeholders’ concerns about their response plans and other proprietary documents being stored in a system on the DHS server where other government officials could access it at any time without their knowledge or consent. According to one official’s understanding, these response plans were not widely shared and were closely held by each jurisdiction, and stakeholders did not want broad government access and control of them. As a result, the BioWatch portal does not currently have a DHS trusted internet connection.

In November 2016, OIG received a Hotline complaint that the portal was operating with classified information and PII on it, and that this information had been potentially leaked to unauthorized individuals. In response to this complaint, the DHS Office of the Chief Information Security Officer (OCISO) conducted a vulnerability assessment in December 2016 which identified both critical and high risk vulnerabilities. Subsequently, OHA requested a more in-depth security posture assessment of the BioWatch system which OCISO conducted from March to April 2017. Table 2 highlights critical and high-risk impact vulnerabilities identified from the security posture assessment.

Table 2: DHS OCISO BioWatch Security Posture Assessment

Risk Level	Character or Consequence of Vulnerability
Critical	Potentially could allow a local or unauthenticated remote attacker to: <ul style="list-style-type: none">• impact system integrity• cause denial of service conditions• gain elevated privileges
High	Potentially could allow an unauthenticated remote attacker to: <ul style="list-style-type: none">• impact system integrity• execute arbitrary code• disclose sensitive information

Source: OIG analysis of BioWatch vulnerabilities from DHS OCISO’s security posture assessment

Based on the security posture assessment results, DHS OCISO determined that a number of corrective actions were needed to mitigate the risk of

²¹ A “Trusted Internet Connection” is a single point of connection to the internet, protected by firewalls, scanners, and other means.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

unauthorized portal access. Further, DHS OCISO found no classified information on the portal and reported being satisfied with a system security risk assessment of medium-medium-medium for its security configuration baseline. To address some of the identified vulnerabilities, OHA was actively coordinating with DHS OCIO to move BioWatch inside the DHS firewall as of July 2017. However, until this and other corrective actions are accomplished, PII on the BioWatch portal will remain at risk of unauthorized access and disclosure.

Recommendations

We recommend that the Acting Assistant Secretary of Office of Health Affairs:

Recommendation 1: Assign the OHA Privacy Official position the appropriate authority, roles, and responsibilities needed to successfully implement an organization-wide privacy program.

Recommendation 2: Inform OHA staff in writing of the Privacy Official's statutory responsibilities and the need for all staff to comply with privacy requirements and any requests from the Privacy Officer.

Recommendation 3: Allocate the financial and staff resources needed for the OHA Privacy Office to effectively carry out its authority, roles, and responsibilities.

Recommendation 4: Develop a system to centrally track annual employee completion of mandatory DHS Privacy Awareness training for accurate reporting to DHS and Congress.

Recommendation 5: Enforce the requirement that all OHA staff take mandatory Privacy Awareness training annually so that staff know how to properly handle and protect PII used in OHA programs and information systems.

Recommendation 6: Implement a process requiring that emergency medical services responders provide Privacy Act notifications when collecting personally identifiable information from individuals.

Recommendation 7: Enforce strong passwords on the ePCR system to improve authentication of authorized users accessing the system, until the system is decommissioned as planned.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 8: Validate that the new ePCR system is PIV-enabled in compliance with HSPD-12 requirements.

Recommendation 9: Implement a solution to prevent the use of unauthorized personal mobile devices to connect to the ePCR system.

Recommendation 10: Establish a plan of action and milestones to bring the BioWatch system to a moderate rating for confidentiality, including the security controls required to safeguard privacy sensitive systems.

Recommendation 11: Move the BioWatch system to a trusted domain to comply with system security requirements and thereby safeguard sensitive and personally identifiable information.

Management Comments and OIG Analysis

In the formal written comments on a draft of this report, the Acting Assistant Secretary for Health Affairs and Chief Medical Officer concurred with all of our recommendations. Following is a summary of OHA management's response to each recommendation and our analysis. We included a copy of the comments in their entirety in appendix B. We also obtained technical comments on the draft report that we addressed and incorporated in the final report, as appropriate.

Recommendation 1: Assign the OHA Privacy Official position the appropriate authority, roles, and responsibilities needed to successfully implement an organization-wide privacy program.

OHA Response to Recommendation 1: OHA leadership concurred with this recommendation, acknowledging that someone within the organization should be identified and have the appropriate authority, roles, and responsibilities to successfully implement an organization-wide privacy program. They stated that OHA is not required to have a Component Privacy Officer; therefore, in June 2014, OHA leadership designated an employee to serve as the organization's privacy point of contact. According to OHA and DHS Privacy Instruction 047-01-001, *Privacy Policy and Compliance*, this individual essentially has the same duties as a Component Privacy Officer. As such, OHA requested that OIG consider this recommendation resolved and closed.

OIG Analysis: OHA's response falls short of fulfilling the intent of this recommendation. While we agree that the Privacy Official's roles and responsibilities should not change based on position title, OHA has not provided evidence of empowering this official with the authority to implement



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

an organization-wide privacy program. We will consider this recommendation resolved once OHA provides a plan of action, including an anticipated completion date, for empowering the Privacy Official with the requisite authority. We may close this recommendation upon receipt of evidence that OHA has followed through in ascribing the Privacy Official full authority for implementing OHA's organization-wide privacy program.

Recommendation 2: Inform OHA staff in writing of the Privacy Official's statutory responsibilities and the need for all staff to comply with privacy requirements and any requests from the Privacy Officer.

OHA Response to Recommendation 2: OHA leadership concurred with this recommendation and agreed to inform staff in writing of the privacy point of contact's responsibilities and the need for staff to comply with Department policies and related guidance. OHA expects this notice will be completed by November 30, 2017.

OIG Analysis: OHA's intended actions should fulfill the intent of recommendation 2. We consider this recommendation open and resolved. We can close this recommendation once OHA provides evidence of informing staff in writing of the Privacy Official's statutory responsibilities and stressing the importance of complying with privacy requirements. OHA expects this process will be completed by November 30, 2017.

Recommendation 3: Allocate the financial and staff resources needed for the OHA Privacy Office to effectively carry out its authority, roles, and responsibilities.

OHA Comments to Recommendation 3: OHA leadership concurred with this recommendation, believing that the resources needed to fulfill the privacy point of contact's roles and responsibilities have already been sufficiently addressed through standard OHA resourcing activities. Specifically, they indicated that they assigned a senior GS-15 non-supervisory program analyst as the privacy point of contact, with access to personnel within OHA Divisions who can assist in successfully implementing an OHA-wide privacy program. As such, OHA requested that recommendation 3 be considered resolved and closed.

OIG Analysis: OHA's actions have not fulfilled the intent of recommendation 3. Specifically, OHA has not provided a solid basis for concluding that sufficient privacy management resources and staffing already exist. We can resolve this recommendation once OHA provides a plan of action and an expected completion date for evaluating OHA programs, privacy responsibilities, and resources. OHA may otherwise assist in closing this recommendation by



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

providing the methodology it used to conclude that sufficient privacy management resources and staffing exist.

Recommendation 4: Develop a system to centrally track annual employee completion of mandatory DHS Privacy Awareness training for accurate reporting to DHS and Congress.

OHA Comments to Recommendation 4: OHA concurred with recommendation 4. OHA, in coordination with DHS Office of the Chief Human Capital Officer, plans to investigate whether PALMS can centrally track annual employee completion of mandatory Privacy Awareness training. If PALMS lacks this capability, OHA plans to identify an alternative solution. OHA expects to complete this corrective action by December 30, 2017.

OIG Analysis: OHA's proposed actions should fulfill the intent of this recommendation. This recommendation is open and resolved. We may close this recommendation upon receipt of documented evidence that OHA is centrally tracking employee completion of DHS Privacy Awareness training.

Recommendation 5: Enforce the requirement that all OHA staff take mandatory Privacy Awareness training annually so that staff know how to properly handle and protect PII used in OHA programs and information systems.

OHA Comments to Recommendation 5: The OHA Training Coordinator plans to provide periodic reports to OHA Division Directors and first-level supervisors regarding staff completion of annual mandatory training. OHA also plans to revise its current training policy to include language for holding Division Directors and first-level supervisors accountable for ensuring employee training completion. OHA anticipates the policy revisions and periodic reports will be implemented by December 30, 2017.

OIG Analysis: OHA's proposed actions should fulfill the intent of recommendation 5. This recommendation is open and resolved. We may close this recommendation upon receipt of the updated policy, examples of the periodic reports, and evidence of OHA ensuring that delinquent employees followed through in taking the mandatory Privacy Awareness training as required.

Recommendation 6: Implement a process requiring that emergency medical services responders provide Privacy Act notifications when collecting personally identifiable information from individuals.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OHA Comments to Recommendation 6: OHA leadership concurred with this recommendation and agreed that recipients of emergency care need to receive the Privacy Act Statements. Although OHA does not provide emergency medical services directly to patients, the OHA Medical First Responder Coordination Branch agreed to stress to DHS Components that provide such care the importance of complying with the Privacy Act notification requirement. In addition, the new version of the Department's electronic patient care reporting system will generate a Privacy Act Statement on all documents given to patients during future medical service encounters. OHA expects to implement this recommendation by December 30, 2017.

OIG Analysis: OHA's proposed actions should fulfill the intent of recommendation 6. As such, this recommendation is open and resolved. We may close this recommendation upon receiving documented evidence that the planned actions have been implemented.

Recommendation 7: Enforce strong passwords on the ePCR system to improve authentication of authorized users accessing the system, until the system is decommissioned as planned.

OHA Comments to Recommendation 7: OHA leadership concurred with this recommendation and informed us that ePCR 1.0 was decommissioned in July 2017. According to OHA, DHS components are currently using paper records and, as such, passwords are no longer needed. OHA asked us to consider this recommendation resolved and closed.

OIG Analysis: OHA's actions fulfill the requirement of this recommendation. This recommendation is open and resolved. We may close this recommendation once OHA provides documentation confirming that ePCR 1.0 has been decommissioned.

Recommendation 8: Validate that the new ePCR system is PIV-enabled in compliance with HSPD-12 requirements.

OHA Comments to Recommendation 8: OHA leadership concurred with recommendation 8. According to OHA, staff of the Medical First Responder Coordination Branch meet at least weekly with DHS OCIO representatives to ensure ePCR 2.0 is PIV-enabled and compliant with HSPD-12 requirements. OHA expects ePCR 2.0 to be operational by April 30, 2018.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis: OHA's planned action is responsive to recommendation 8. We consider this recommendation open and resolved. We will close this recommendation after receiving evidence that ePCR 2.0 is PIV-enabled.

Recommendation 9: Implement a solution to prevent the use of unauthorized personal mobile devices to connect to the ePCR system.

OHA Comments to Recommendation 9: OHA leadership concurred with the recommendation. According to OHA, staff of the Medical First Responder Coordination Branch are coordinating with DHS OCIO representatives and the ePCR vendor to identify and implement a solution that will prevent unauthorized personal mobile devices from being connected to the new ePCR system. OHA estimates this will be completed by April 30, 2018.

OIG Analysis: OHA's planned action is responsive to the recommendation. This recommendation is open and resolved. We will close this recommendation upon receipt of evidence or test results confirming that personal mobile devices cannot be connected to ePCR.

Recommendation 10: Establish a plan of action and milestones to bring the BioWatch system to a moderate rating for confidentiality, including the security controls required to safeguard privacy sensitive systems.

OHA Comments to Recommendation 10: OHA leadership concurred with this recommendation. According to OHA, BioWatch program staff established a plan of action and milestones to bring the system to a moderate rating for confidentiality, including the security controls required to safeguard privacy sensitive systems. Specifically, OHA has a contract in place to move the BioWatch portal to the DHS Data Center; installation of security management tools is ongoing. OHA expects to complete the planned actions by March 30, 2018.

OIG Analysis: OHA's planned action should fulfill the intent of the recommendation. We consider this recommendation open and resolved. We will close this recommendation after receiving the formal plan of action and milestones outlining OHA's planned actions to bring the BioWatch portal to a moderate rating for confidentiality, including the security controls required to safeguard privacy sensitive systems.

Recommendation 11: Move the BioWatch system to a trusted domain to comply with system security requirements and thereby safeguard sensitive and personally identifiable information.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OHA Comments to Recommendation 11: OHA leadership concurred with this recommendation. According to OHA, BioWatch program staff are moving the BioWatch web portal from the Level III commercial data center site to a DHS data center to comply with system security requirements. OHA expects to complete the move by March 30, 2018.

OIG Analysis: OHA's planned action is responsive to the recommendation. Recommendation 11 is open and resolved. We may close this recommendation once OHA provides evidence that the BioWatch portal has been moved to a DHS data center.



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*. We evaluated OHA's privacy safeguards for protecting the PII it collects and maintains. Our objective was to determine whether OHA ensures compliance with applicable Federal privacy laws, regulations, and policies.

As background for this audit, we obtained and reviewed relevant laws, directives, policy, guidelines, and privacy controls. We reviewed prior reports, testimony, and OIG Hotline complaints related to OHA programs and privacy. We interviewed OHA senior leaders, the Privacy Officer, the training officer, security officers, program managers, and the BioWatch contracting officer representative and contracting officials. We also met with representatives of the DHS Privacy Office and DHS OCIO. We obtained and evaluated OHA privacy documents for promoting agency transparency, such as OHA's privacy inventory, PTAs, system of record notices, and privacy impact assessments. We also reviewed *Freedom of Information Act* requests and OHA responses. We examined OHA contracts for privacy clauses. We examined internal controls for managing OHA information systems and also looked at information system risk assessments and system security plans to determine compliance with privacy system security requirements. We did not look at classified information as part of this audit.

We conducted this performance audit between January and July 2017 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.

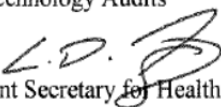


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
OHA Comments to the Draft Report

November 1, 2017

MEMORANDUM FOR: Sondra McCauley
Assistant Inspector General
Information Technology Audits

FROM: Larry D. Fluty 
Acting Assistant Secretary for Health Affairs and
Chief Medical Officer

SUBJECT: Management Response to OIG Draft Report: "Office of Health
Affairs Has Not Implemented An Effective Privacy Management
Program" (Project No. 017-18-ITA-OHA)

Thank you for the opportunity to review and comment on this draft report. The Office of Health Affairs (OHA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

OHA leadership is committed to ensuring compliance with privacy-related regulations and policies and has taken steps to stress the importance of privacy throughout the office. OHA staff works collaboratively with the DHS Privacy Office on issues related to OHA programs and systems, and is currently reviewing the Privacy Point of Contact (PPOC) authority and responsibilities. Additionally, OHA continues to actively build upon improvements made prior to, during, and after OIG's audit.

The draft report contained eleven recommendations, all of which OHA concurs. Attached find our detailed response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were separately provided. Please feel free to contact us if you have any questions. We look forward to working with you in the future.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Attachment: Management Response to Recommendations Contained in 017-18-ITA-OHA

The OIG recommended that the Acting Assistant Secretary of Office of Health Affairs:

Recommendation 1: Assign the OHA Privacy Official position the appropriate authority, roles, and responsibilities needed to successfully implement an organization-wide privacy program.

Response: Concur. OHA agrees that someone needs to be identified and have the appropriate authority, roles, and responsibilities needed to successfully implement an organization-wide privacy program. It is important to note, however, that according to DHS Privacy Instruction No. 047-01-005, "Component Privacy Officer," OHA is not required to have a Component Privacy Officer. Instead, since June 2014, and in accordance with DHS Privacy Instruction 047-01-001, "Privacy Policy and Compliance," OHA has had an employee designated to serve as the OHA Privacy Point of Contact (PPOC). This person essentially has the same duties and responsibilities that a Component Privacy Officer would have under Instruction 047-01-005, including those, for example, related to responding to a data breach incident pursuant to DHS Privacy Policy Directive 047-01-008, "DHS Privacy Incident Handling Guidance." We request that the OIG consider this recommendation resolved and closed.

Recommendation 2: Inform OHA staff in writing of the Privacy Official's statutory responsibilities and the need for all staff to comply with privacy requirements and any requests from the Privacy Officer.

Response: Concur. Although OHA has introduced the OHA PPOC to OHA staff on numerous occasions, OHA will inform staff in writing of the PPOC's responsibilities and the need for staff to comply with Department privacy policies and related guidance. Estimated Completion Date (ECD): November 30, 2017.

Recommendation 3: Allocate the financial and staff resources needed for the OHA Privacy Office to effectively carry out its authority, roles, and responsibilities.

Response: Concur. OHA senior leadership believes that the resources needed to fulfill PPOC roles and responsibilities have already been sufficiently addressed through standard OHA resourcing activities. A senior GS-15 non-supervisory program analyst has been assigned as the PPOC and has access to personnel within the OHA Divisions to assist with successfully implementing an OHA-wide privacy program, as appropriate. We request that OIG consider this recommendation resolved and closed.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 4: Develop a system to centrally track annual employee completion of mandatory DHS Privacy Awareness training and thereby ensure more accurate reporting to DHS and Congress.

Response: Concur. OHA Training Coordinator, in coordination with DHS Office of the Chief Human Capital Officer staff, will investigate the potential use of the DHS Performance and Learning Management System (PALMS) to centrally track annual employee completion of mandatory DHS Privacy Awareness training. If for some reason PALMS cannot be used for this purpose, alternative options will be identified. ECD: December 30, 2017.

Recommendation 5: Enforce the requirement that all OHA staff take mandatory Privacy Awareness training annually to ensure staff know how to properly handle and protect PII used in OHA programs and information systems.

Response: Concur. OHA Training Coordinator will provide OHA Division Directors and first-level supervisors with periodic reports identifying staff who have/have not completed annual mandatory training. OHA Human Capital staff is also in the process of revising the current training policy to include enforcement language applicable to Division Directors and first-level supervisors. OHA employees and contractors will complete annual training by required due date(s). ECD: December 30, 2017.

Recommendation 6: Implement a process to ensure that emergency medical services responders provide Privacy Act notification as required when collecting personally identifiable information from individuals.

Response: Concur. We agree that recipients of emergency care need to be provided mandated Privacy Act statements. However, it must be noted that OHA staff does not provide emergency medical services (EMS) directly to patients, but rather Component EMS responders provide these services. OHA Medical First Responder Coordination Branch staff will stress to EMS leaders of the DHS Components the importance of complying with providing Privacy Act requirements as regards privacy statement notifications. In addition, the new version of the Department's electronic patient care reporting system (ePCR) will include a Privacy Act Statement, as required by 5 U.S.C. § 552a(e)(3), on all documents generated and to patients during medical service encounters. ECD: December 30, 2017.

Recommendation 7: Enforce strong passwords on the ePCR system to improve authentication of authorized users accessing the system, until the system is decommissioned as planned.

Response: Concur. OHA decommissioned EPCR 1.0 in July 2017, DHS Components are now using paper records, and passwords are no longer needed. We request that OIG consider this recommendation resolved and closed.

Recommendation 8: Ensure that the new ePCR system is PIV-enabled in compliance with HSPD-12 requirements.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response: Concur. OHA Medical First Responder Coordination Branch staff will continue to work with DHS OCIO, during a weekly teleconference and through other interactions, to ensure ePCR 2.0 will be PIV-enabled and in compliance with HSPD-12 requirements. ECD: April 30, 2018.

Recommendation 9: Implement a solution to prevent the use of unauthorized personal mobile devices to connect to the ePCR system.

Response: Concur. OHA Medical First Responder Coordination Branch staff is coordinating with DHS Office of the Chief Information Officer (OCIO) and the ePCR vendor to identify and implement a solution that will prevent unauthorized personal mobile devices from being connected to the new ePCR system. ECD: April 30, 2018.

Recommendation 10: Establish a plan of action and milestones to bring the BioWatch system to a moderate rating for confidentiality, including the security controls required to safeguard privacy sensitive systems.

Response: Concur. OHA BioWatch program office staff have established a plan of action and milestones that addresses the rating for confidentiality, including the security controls required to safeguard privacy sensitive systems. In cooperation with DHS OCIO, a contract for moving the portal to the DHS Data Center is in place and the installation of security management tools is ongoing. ECD: March 30, 2018

Recommendation 11: Move the BioWatch program office web portal system to a trusted domain to comply with system security requirements and thereby safeguard sensitive and personally identifiable information.

Response: Concur. OHA BioWatch program office staff are moving the Biowatch program office web portal system from the Level III commercial data center site to a DHS Data Center to comply with system security requirements. ECD: March 30, 2018.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix C

Office of IT Audits Major Contributors to This Report

Richard Saunders, Director
Beverly Burke, Audit Manager
Robert Durst, Senior Analyst
Brian Smythe, Program Analyst
Anna Hamlin, Independent Referencer



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D
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
DHS Privacy Office

Office of Health Affairs

Acting Assistant Secretary
Chief of Staff
Audit Liaison

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