Journal of Bioterrorism & Biodefense

Harry Jackson, J Bioterror Biodef 2017, 8:1
DOI: 10.4172/2157-2526.1000153

Review OMICS International

Securing the BioWatch Web Portal

Harry Jackson*

Information Systems Security Manager, USA.

***Corresponding author:** Harry Jackson, 12823 Piney Point Place Herndon, VA 20171, USA, Tel: + 717 419 6053; E-mail: harryrjackson@gmail.com

Received date: December 27, 2016; **Accepted date:** January 20, 2017; **Published date:** January 27, 2017

Abstract

The Department of Homeland Security (DHS) BioWatch program is the only nationwide early detection system to provide warning, and situational awareness, to DHS decision makers, in the event of a bioterrorism attack. The BioWatch Web Portal is the means by which DHS collects, analyzes, and shares, bio-threat information amongst federal, state, and local jurisdictions. Integrity and confidentiality of the information collected by the portal is paramount to that decision makers make decisions on reliable, and accurate information. Just as important is the appropriate safeguarding of such information so that a malicious actor is denied sufficient detail as to the methods, materials, and false negative rates that would enable such an actor to spoof the system or circumvent detection.

An internal and external assessment analysis of the BioWatch Web Portal revealed that sufficient security controls to mitigate risk posed to the integrity and confidentiality of information processed by the BioWatch Web Portal was not in place. Furthermore, it was discovered that security countermeasures were not in place to detect a possible breach. In addition, it was discovered that the information processes information at the SECRET level security classification.

Keywords: Terrorist attacks; Bioterrorist; Public health

Securing the BioWatch Web Portal

In the wake of the September 11, 2001, terrorist attacks, to protect the United States against the threat of a bioterrorist attack that could cause mass casualties, critical infrastructure disruption, and economic disruption, the BioWatch program was established in April 2003 [1,2]. The BioWatch Program, managed by the Department of Homeland Security (DHS) Office of Health Affairs (OHA) provides early detection of a bioterrorism event. The program also facilitates the coordinated response nationwide among the federal, state, local, and tribal governments [3]. It is an interface for state and local public health and responder communities to respond jointly to an act of bioterrorism [4]. The mission of the BioWatch program is "to operate a nationwide, aerosol detection system providing early warning across all levels of government to support public health and emergency management communities to prepare for and respond to biological incidents" [5]. It is DHS's contribution to the national capability called for in Homeland Security Presidential Directive 10 (HSPD-10) for a national bioawareness capability [6]. The BioWatch program is a cornerstone of the DHS comprehensive strategy for countering terrorism and the nation's only system for providing early warning detection of an aerosolized biological attack. It provides this capability by positioning collection sensors in strategic locations around the United States that continuously monitor the air for biological threats 24 hours a day, 365 days a year. It is operated by a network of scientists, laboratories, emergency managers, and public health officials in over 30 jurisdictions in the United States [1,2]. The benefits of this program are estimated to reduce illness rate detections by as much as 36%, possibly saving tens of thousands of lives in the event of a biological aerosol attack, compared to the system's not being deployed [2].

Current BioWatch Web Portal ATO Package

The BioWatch Web Portal is a system of record that supports the BioWatch program, which connects the over 30 federal, state, local, and tribal jurisdictions where biological pathogen collectors are located. The BioWatch Web Portal is a government-owned, commercially operated system hosted in a commercial database center in McLean, Virginia, which is inaccessible to the federal government and hosted on a .org domain [7]. Despite not having a Security Assessment or a Security Control Assessment performed, the BioWatch Web Portal received its last Approval to Operate (ATO) in 2015 [8,9].

Within the Systems Security Plan, the impact levels to the confidentiality, integrity, and availability that form its security baseline configuration are low for all three areas. The portal is also designated a privacy information system and a non–Mission Essential System. Though designated a privacy information system, a Privacy Impact Assessment (PIA), as mentioned as a requirement in the system Privacy Threshold Assessment (PTA), was not completed as part of the BioWatch Web Portal's 2015 ATO [10]. Furthermore, the PTA submitted for the system as part of its 2015 ATO stated that the system does not process personally identifying information (PII), though it clearly does. The site is hosted on a .org domain and is accessible via single-factor authentication [11]. The Security Risk Assessment for the system with a Low-Low-Low Security Configuration Baseline lists the project risk for this system as "high" because only approximately half of the security controls required per the Risk Management Framework for a Low-Low-Low system have been implemented [12].

The current Systems Security Plan does not list any subsystems or minor applications for the portal. The only system interconnection with the BioWatch Web Portal is via the Internet. System users must have a minimum clearance level of Confidential, and foreign nationals are not permitted to access the application. There are no cross-domain

solutions associated with the system. Figure 1 illustrates the data center architecture [11].

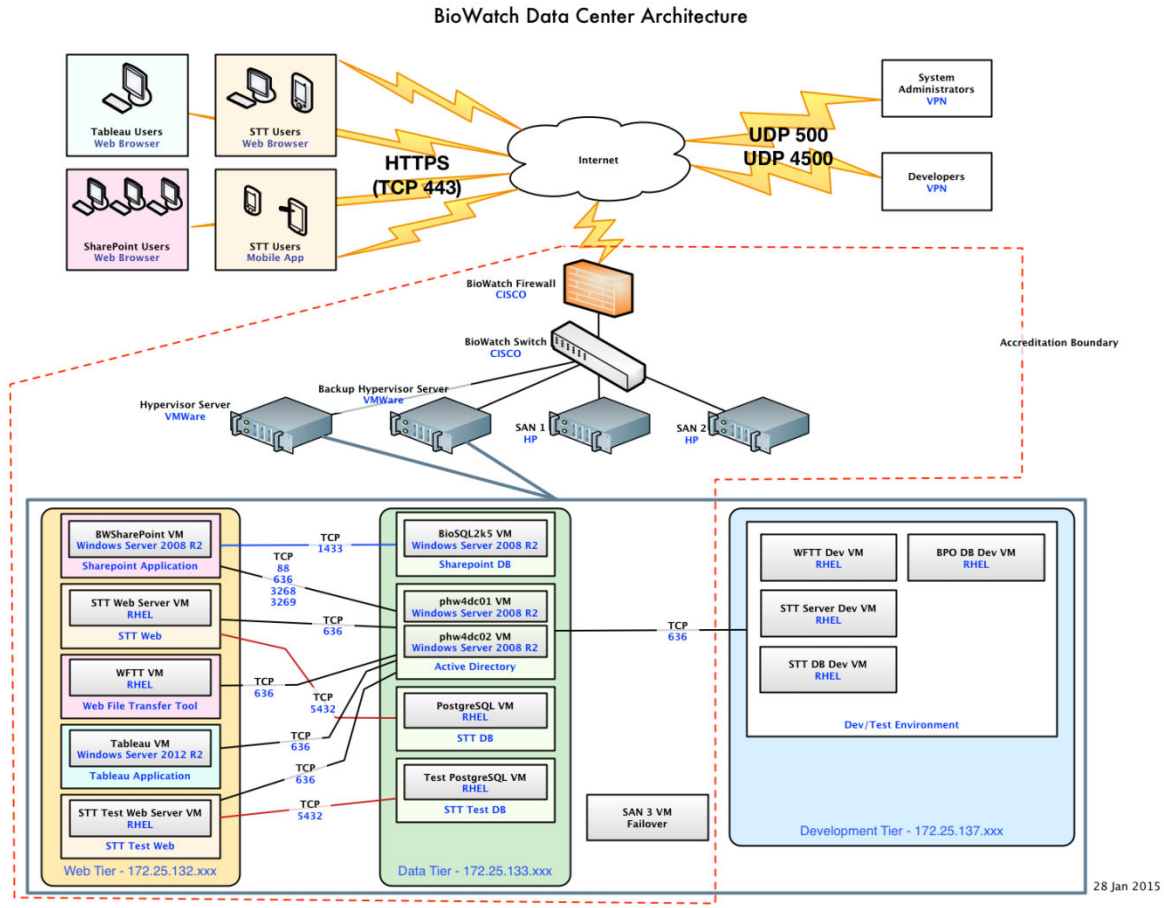

Figure 1: BioWatch data center architecture. This figure illustrates the system's boundaries and that the BioWatch Web Portal lacks a trusted Internet connection.

ATO Issues

The system is a designated privacy information system that resides in an uncontrolled space that the federal government cannot monitor and that lacks a trusted Internet connection with two-factor authentication. OMB A-130 requires that government agencies use only a .mil, .gov, or fed.us domain unless the "agency head explicitly determines another domain is necessary for the proper performance of an agency function" [13]. The BioWatch program does not have such explicit authorization from the Secretary of the Department of Homeland Security. The stated justification as to why the site was hosted on a .org domain is because state and local partners were reluctant to use a .gov system because they did not want the federal government to see their data [14].

It is the nation's only system for providing early warning detection of an aerosolized biological attack, implying that it could be a National Security System. For this reason a review of the first step of the Risk Management Framework, categorization of the controls, should reoccur.

The fact that the system is a designated privacy system that is hosted on a dynamic web page requires that moderate confidentiality security controls be applied to the system [15]. An interview with senior officials at OHA on November 18, 2016, revealed that the integrity controls were also categorized inappropriately. The OHA chief of staff stated that the integrity of the data in the system is "critical" to the function of the system and reiterated its importance to national security, relaying the message that the system should have high confidentiality controls. Consensus in the room was that if the system were taken offline for a period of a month, they could continue normal business operations, indicating that a low availability system categorization was appropriate. Therefore, the system security baseline for its ATO should be Moderate-High-Low and not Low-Low-Low.

Root Causes of the ATO Issues

Every two years at the start of a new Congress, the U.S. Government Accountability Office (U.S. GAO) publishes a "High Risk List" to bring to the attention of lawmakers those program areas and agencies that are high risk because of their vulnerabilities to fraud, waste, abuse, and

mismanagement and in need of transformation [16,17]. Despite efforts to improve the acquisition management of the program, the acquisition management of the BioWatch program has been on the GAO's High-Risk List since 2005 [4].

External Assessment

From 14 December 2016, through 11 January 2017, the DHS Vulnerability Assessment Team (VAT) conducted an external assessment of the BioWatch Web Portal. The DHS VAT conducted a scan of the BioWatch Web Portal domain at www.biowatchportal.org and discovered five other different IP addresses in the same subnet (Two of which are a test and development IP address on the same subnet as the production IP). The DHS VAT team used only one source IP address during the three week scanning period and there were no reports of any scanning activities or notifications reported for the component to any stakeholders. The source IP during the scan was not blocked, giving the conclusion that the BioWatch Web Portal does not contain any protective monitoring [18].

Risk Management Team Issues

An inappropriate relationship currently exists because the contrast program manager also serves as the Information Systems security officer (ISSO) for the system [10]. This presents a conflict of interest and is a contributing factor to the deficiencies in the ATO package. Such deficiencies include the failure to adhere to agency and federal laws, regulations, and policies regarding the ATO system; the miscategorization of the security baseline to justify opting for the cheapest compliance solution, which is not commensurate to the true impact to the confidentiality, integrity, and availability of the system, to drive down costs; and the deliberate omission of information in the ATO security artifacts, which resulted in substantial changes to the system configuration, requiring another ATO [7].

Furthermore, the acting ISSO of the system was not designated in writing as the ISSO of the system. The last ISSO letter for the system, as required by the DHS Security Authorization Process Guide, indicated two other individuals designated as ISSOs as recently as September 2016 [19]. The individual currently performing the ISSO function has been doing so since 2012 [20].

In addition, the ISSO for the system had not completed any type of ISSO training and allowed for the creation of privileged accounts for users that were not on contract with DHS, thus, not having been processed through the DHS Office of Security to ensure they had the appropriate clearance levels. Lastly, there is no user training for new users of the system and no acceptable use agreement for users to sign, nor have user access forms been routed to the Information Systems security manager (ISSM) for approval.

Program Office Application

The Systems Security Plan does not mention subsystems nor minor applications within the BioWatch Web Portal [11]. During a meeting on November 15, 2016, it was revealed to the ISSM by the BioWatch Web Portal Chief Architect that the BioWatch program had implemented a Program Office Application as a subsystem in the BioWatch Web Portal and had been operating the system for some years. The application itself aggregated data the BioWatch sensors collected, as well as sensitive PII. Upon review from the DHS Privacy Office, it was determined by the OHA privacy representative that the implementation of the application constituted a privacy incident. The DHS Office of Security's preliminary analysis of the data indicated that the aggregated data violated the BioWatch Security Classification Guide. This resulted in a classified spillage at the secret level because the application collects information that shows deficiencies in the system that, if disclosed to an adversary, would provide the actor with information sufficient to release a biological pathogen in the continental United States that could evade detection [20]. In its current state, the Program Office Application records information technology security infractions, privacy infractions, and security infractions for the ISSO, program manager, and system owner of the BioWatch Web Portal.

Possible Reason for Policy Infractions

The U.S. GAO, since 2012, has reported to Congress that the BioWatch program faced challenges in its ability to reliably detect attacks. In September 2012, the U.S. GAO found that the program approved an acquisition, Gen-3, in 2009 without fully developing knowledge that the acquisition would ensure sound investment decision making and the pursuit of optimal solutions. DHS concurred with the U.S. GAO's assessment, and in 2014, the Gen-3 acquisition was canceled [16].

In 2015 the U.S. GAO found that the BioWatch program lacked reliable information about the system's current capabilities to detect a biological attack, in part, because the program has not developed technical performance requirements for the system [16]. The lack of performance requirements inhibits the ability of the program to interpret test results and draw conclusions about the system's ability to detect attacks. DHS again concurred with the U.S. GAO's assessment and agreed not to pursue upgrades to the system until it establishes technical performance requirements to meet clearly defined operational objectives in which the assessment of the system against these performance requirements can occur [16].

It is likely for this reason that the Program Office Application (of important note in the Contingency Plan is the listing of the Portal Web Capabilities, which mentions the capability to aggregate key content) was developed and implemented in the BioWatch Web Portal. The aggregation of the data by the program office application clearly results in the ability to show plum trends and the operational status of collections that can aid in the development of objective and threshold Key Performance Parameters that a new system would have to achieve.

Conclusion

The BioWatch Web Portal, since its inception, has undergone unrestrained system growth to meet customers' needs. The security baseline of the system was miscategorized. The system also underwent substantial changes to its configuration, with addition of the four undocumented subsystems. Due to these factors alone, the system should undergo an immediate ATO process. A complete update to the Systems Security Plan should occur that complies with the National Institute of Standards and Technology Special Publication 800-16.

Furthermore, revisions to the Risk Management Framework team composition should occur. The individual acting in the ISSO capacity should be reassigned to other duties as well as the federal project manager and system owner for the deliberate miscategorization of controls and the negligent spillage of PII and classified information on a network that does not use a proven solution or adhere to common criteria standards.

In addition, for changes made to the system, an Integrated Product Team should be established comprising representation from the DHS Offices of Privacy, Chief Information Office, Office of Security, General Counsel, and the Customer Representative to ensure compliance and appropriateness of changes. New users to the system should be required to sign an acceptable use document, informing them of inappropriate actions and consent to monitoring; receive user training on the system; and have forms collected and tracked by the ISSO for compliance. In addition, privileged users must also receive training and be vetted by the ISSM of the system.

The BioWatch program is the nationwide early biological pathogen detection system designed to reduce the loss of life in the event of an act of bioterrorism. The sensitivity and criticality of the information the system processes and the potential impact to the degradation of the confidentiality, integrity, or availability merit more than a Low-Low-Low security configuration baseline and should certainly, at a minimum, have a trusted Internet connection and require two-factor authentication. Therefore, the system should be migrated off the .org domain to a proven solution that facilitates collaboration among federal, state, local, and tribal governments, such as the Homeland Security Information Network [3]. Because the BioWatch program requires the aggregation of information from its BioWatch collectors that rise to the level of secret classification, the program should acquire an appropriate cross-domain solution to facilitate the transfer of information from its collectors on an unclassified network to a secret network, such as the Homeland Security Data Network, for aggregation and analysis.

References

1. Office of Health Affairs (2016) BioWatch.
2. Office of Health Affairs (2016) BioWatch Infographic.
3. Department of Homeland Security (2016) Health Threats Resilience Division.
4. U.S. Government Printing Office (2014) BioWatch: Lessons Learned and the Path Forward.
5. Office of Health Affairs (2016) The BioWatch Program.
6. Currie C (2016) BIOSURVEILLANCE: Ongoing Challenges for DHS Biosurveillance Efforts.
7. Longa C, Derby P, Albert K (2016) BioWatch Web Portal: Contingency Plan.
8. Department of Homeland Security (2016) C&A Detail Report.
9. Department of Homeland Security (2016) Homeland Security Information Network.
10. Department of Homeland Security (2015) BioWatch Privacy Threshold Analysis.
11. Longa C, Derby P, Albert K (2015) BioWatch Web Portal: Systems Security Plan.
12. Department of Homeland Security (2016) BioWatch Web Portal: Risk Report.
13. Johnson C (2014) Memorandum for the Heads of Executive Departments and Agencies. Office of Management and Budget.
14. Fernandez C (2016) BioWatch Web Portal Information Security Program Request for Waiver #48.
15. Riley D (2016) BioWatch Confidentiality Levels.
16. U.S. Government Accountability Office (U.S. GAO) (2016) BIOSURVEILLANCE: Ongoing Challenges and Future Considerations for DHS Biosurveillance Efforts.
17. U.S. Government Accountability Office (U.S. GAO) (2016) High Risk List.
18. Department of Homeland Security (2017) Summary Report for the Department of Homeland Security External Assessment of BioWatch Portal Program. District of Columbia: Departement of Homeland Security.
19. Varner G (2016) ISSO Letter.
20. Department of Homeland Security (2012) BioWatch Program Security Classification Guide.