




OFFICE OF THE INSPECTOR GENERAL

March 1, 2018

TO: Timothy L. Firestine
Chief Administrative Officer

FROM: Edward L. Blansitt III
Inspector General 

SUBJECT: Allegation of Improperly Handled Computer System Data Breach
OIG PIM #18-001

Based on a complaint that a data breach of a Montgomery County Department of Technology Services (DTS) computer system occurred in May of 2016 and that the breach was not properly reported, the OIG instituted this Preliminary Inquiry. During the inquiry, the OIG learned that both the Chief Information Officer (CIO) of the County and the Office of the County Attorney were aware of this matter in 2016 and had addressed it shortly after it was reported. The administrative response to this incident, recommended by the County Attorney and executed by DTS, was consistent with prior recommendations of the OIG and the applicable requirements in effect at that time.

The OIG took note of this allegation due to the potential serious nature and the exposure of the County if a breach actually took place. In the past several years computer (data) security has been addressed several times by both the OIG and the Montgomery County Office of Internal Audit. An external consultant had previously issued findings and recommendations that might have prevented this incident if fully implemented.¹

Computer data security was also addressed by the Montgomery County Office of Internal Audit in a May 2017 report titled "HIPAA Compliance - Phase 1 Risk Assessment."² While this report specifically looked at HIPAA compliance, recommendations were made addressing inadequate or outdated computer security policies and procedures.

The status of compliance with prior recommendations was not reviewed and is beyond the scope of this memo. However, considering the "near miss" of this and other incidents, we feel strongly that prompt implementation of appropriate recommendations should be given a high priority. When the DTS Enterprise Information Security Office (EISO) report is published on this incident, the results and the status of compliance with security recommendations should be presented by the CIO to the Chief Administrative Officer.

¹ Gartner Corporation report on IT Security Assessment.

² HIPAA is the Health Insurance Portability and Accountability Act.

PRELIMINARY INQUIRY DETAILS

Inquiry and Outcome:

In November of 2017, the OIG received a complaint that in May of 2016 a Montgomery County computer system was subjected to a data breach. The allegation was originally made to DTS in November 2016 and investigated by the EISO. The party that reported this vulnerability to DTS, a DTS contractor with system administrator rights but not assigned any computer security duties, accessed data records ostensibly to define and demonstrate the problem. In response to this report, certain other DTS personnel and/or contractors also accessed records of other employees to view and explore the vulnerability.

The complaint states that virtually any employee could access most of the data in the Enterprise Records Management System (ERMS) by using a latent security vulnerability in a commercial software package licensed by the County. This includes personnel records, retirement records, health records, and other Personally Identifiable information (PII) like tax records, social security numbers and dates of birth for any County employee.

The complainant advised that despite the vulnerability being reported in 2016, County employees were not, and have not been, notified that their personal information was accessible. Additionally, the complainant believes that the County failed to install a patch or identify the root cause of the breach, choosing instead to simply disable the access point.

Common use of the term “breach” is not the same as the legal definition of the term. The word “breach” can be used to mean that a person without authority has access to data. The legal definition of “breach” in this case is critical because it denotes a triggering event for certain required reporting and notifications of a data breach. Advice provided by the Office of the County Attorney, that legal definitions vary slightly depending on the local, state and federal laws and the one most applicable to this situation is contained in Maryland law,³ supports recent OIG analyses. This definition of “breach” requires, among other things, two events to occur before triggering certain reporting and notification actions: (1) an unauthorized acquisition of data and (2) the acquisition must compromise the security, confidentiality, or integrity of the personal information.

Information from the complaint and obtained from both the CIO and the County Attorney staff member assigned to this matter supports that a breach as the word is commonly used occurred; however, this event does not appear to meet the criteria of a legal data breach under Maryland law. The data access was made by a contractor exploring a vulnerability of a commercial off the shelf software package. Although this contractor may have abused system administrator access in exploring this vulnerability, there is no evidence at this time that data was “acquired” or that the security, confidentiality, or integrity of the personal

³ See Generally Md. Code State Government §10-1301 et seq.

information was compromised. This analysis by the OIG is consistent with the position taken by the Office of the County Attorney.

OIG staff conducted extensive interviews with the complainant and a witness to identify specific details of the allegation. While it could not be determined exactly when the vulnerability started, it was agreed by all that in early May of 2016 the vulnerability existed.⁴ A witness claimed that data files were exported by people in DTS while exploring the vulnerabilities but specifically denied that any information was accessed from outside DTS.⁵

The CIO was interviewed by the OIG and confirmed that in May of 2016 a latent vulnerability in a commercial off the shelf software product was explored or exploited by a contractor working for DTS. The CIO explained that the underlying vulnerability was immediately addressed with the vendor, and the issue was still under investigation by the EISO.

The CIO told the OIG that the initial EISO inquiry identified access of a single person's data by a DTS contractor; in conversation, the CIO indicated that there could be more people involved, but the EISO has not completed auditing the logs. The CIO provided assurances that the party whose information was accessed was notified per the advice of the County Attorney's Office.⁶ According to the member of the County Attorney's Office assigned to this matter, this notification was an exercise in an abundance of caution in trying to comply with the conflicting definitions of a data breach.

The CIO explained that the investigation was still open with EISO (from 2016 to present) due to the time it takes to examine each log entry to see who accessed various information, who they worked for, why they accessed the information and if they had both authorization and a reason to access the data. As a procedural explanation, he offered that many people in various County agencies and departments have legitimate access to these records on a recurring basis. Each access log entry needs to be explored to determine the validity of the purpose. The CIO said that, to his knowledge, this incident was the only improper access they had found so far.

Finally, the CIO explained that, regarding computer security, the County adheres to industry best practices in National Institute of Standards and Technology standard 800-53, and this is documented by EISO. The CIO stated that the OIG would receive a copy of the final report by the EISO on this incident when the investigation is completed.

⁴ It is likely that this was a latent issue in the commercial software package and existed at the time of deployment in the County system, but this fact was not confirmed or dispelled.

⁵ This fact is significant in the relevant legal definition of a breach under Maryland law. "Breach of the security of a system" does not include the good faith acquisition of personal information by an employee or agent of a unit for the purposes of the unit, provided that the personal information is not used or subject to further unauthorized disclosure." Md. State Government Code Ann. § 10-1305 Et. Seq.

⁶ Relying on the definition from both Md. State Government Code Ann. § 10-1305 and Maryland Personal Information Protection Act, Md. Code Com. Law § 14-3501 et seq. (in effect in 2016, but significantly amended January 1, 2018)

Summary and Conclusion:

The OIG takes no issue with the CIO's assertion that the contractor appears to have exceeded system administrator access authority. In fact, this assertion demonstrates the need for updated procedural and policy controls on access to information.

The County narrowly missed a significant reportable computer security incident in this case, and the OIG will review the final EISO report when it is released. When that report is published, it is suggested that the CIO provide a report to the CAO along with a status report regarding compliance with recommended data security enhancements.⁷

Copies of this Preliminary Inquiry Memorandum (PIM) along with your response, if any, will be provided to the members of the County Council and the County Executive within 10 business days of the date of this PIM.

A Preliminary Inquiry Memorandum is appropriate in situations where we have, in reaction to a complaint, gathered and assessed sufficient information for us to draw limited conclusions related to the specific complaint. Since PIMs do not result from full inspections, investigations, or audits, it would not be appropriate for us to provide full findings and recommendations in PIMs. Instead, we may identify specific conditions, transactions, and events that management may want to continue to research from an investigative or policy standpoint.

⁷ DTS continues to investigate this matter, and the final EISO report is not available as of the publication of this PIM.

**Response to this Preliminary Inquiry Memorandum
From the Montgomery County Chief Administrative Officer:**

On March 9th, 2018 the office of the *Chief Administrative Officer* responded via Email:

“The Executive has a few points of clarification on the following sections of the Preliminary Inquiry Memorandum, OIG PIM-18-001, dated March 1, 2018 (“PIM”):

The PIM refers to a contractor on pages 2-3, stating:

Although this contractor may have abused system administrator access in exploring this vulnerability, there is no evidence at this time that data was “acquired” or that the security, confidentiality, or integrity of the personal information was compromised. This analysis by the OIG is consistent with the position taken by the Office of the County Attorney.

The PIM refers again to a contractor in the third full paragraph on page 3:

The CIO told the OIG that the initial EISO inquiry identified access of a single person’s data by a DTS contractor; in conversation, the CIO indicated that there could be more people involved, but the EISO has not completed auditing the logs. The CIO provided assurances that the party whose information was accessed was notified per the advice of the County Attorney’s Office.

This summary is accurate in some respects, but not in others. The complicated nature of the facts and the County’s steps under applicable law are set forth in more detail below.

As the report states, once DTS was notified of the security vulnerability in May 2016, immediate steps were taken to remedy the vulnerability. Once that was done, DTS took steps to review access logs that showed which users accessed records with sensitive information. This “access audit” is time consuming and ongoing.

During the “access audit,” one individual’s access immediately came to the fore as potentially not appropriate. This individual performed work for the County under a DTS contract. At one point in time, this individual did system administrator work for DTS. At the time of the unauthorized access, however, the individual was not working on DTS projects, but rather projects in other departments. In other words, non-DTS departments used a DTS contract to procure this individual’s services. (This is a routine practice under this particular DTS contract.) Therefore, referring to the individual as a “DTS contractor” does not fully paint the picture of the nature of the contractor’s work for the County at the time of the unauthorized access.

In any event, it became clear during the access audit that, given this individual's work assignments under the contract, the access to sensitive records of six employees was not appropriate. As a result, the County issued notices to the six affected employees under the Protection of Information by Government Agencies Act ("PIGA").

The *PIGA* requires notices to be issued to individuals whose "personal information" was breached if, "the unauthorized acquisition of personal information of the individual *has resulted in or is likely to result in the misuse of the information.*" See Md. Code Ann., St. Gov't § 10-1305(b)(1). The County did not have evidence of a misuse of the personal information accessed. (The law defines personal information to be a name plus certain identifying numbers such as a social security number. See Md. Code Ann., St. Gov't § 10-1301(c)). Out of an abundance of caution, however, and given the number of records accessed by the individual and the extended time period of inappropriate access, the County concluded that the unauthorized acquisition was likely to result in the misuse of the information. As a result, the six affected individuals were notified of the breach.

In addition to sending notices to the affected employees, the County took steps to remove the individual from any County projects under the contract: the individual's inappropriate access to confidential information unrelated to the individual's assigned tasks under the contract, at a minimum, breached the terms of the contract.

We hope this provides a clearer explanation of the circumstances surrounding the County's actions in connection with the identified unauthorized access identified to date in connection with the May 2016 security incident. As the PIM points out, this investigation is ongoing by the Executive."