COUNTY OF MILWAUKEE
Inter-Office Communication

Date: May 27, 2016

To: Scott Manske, Milwaukee County Comptroller
Chris Abele, Milwaukee County Executive
Supervisor Theodore Lipscomb, Sr., Milwaukee County Board Chairman

From: Jerome J. Heer, Director of Audits

Subject: Audit of Cybersecurity (File No. 15-495)

The Cybersecurity audit as requested in File No. 15-495 has been completed. The work was conducted by Experis Finance, Risk Advisory Services ("Experis") under a contract with our office.

The audit objectives were:

- to review threats and risks to data, applications, networks and operating platforms
- to evaluate security plans and policies for addressing identified threats, vulnerabilities and risks.

Experis interviewed key County staff and reviewed County reports, procedures, audits, and policies. In doing so, the Experis team focused on conducting an information security program assessment that evaluated the lifecycle of information security management, including the people, processes and controls used to identify, evaluate, treat, mitigate, eliminate or accept information risks. Their Information Security Program Assessment Methodology, illustrated the following graphic, ensured a consistent result that was tailored to the County's specific business needs and information security management.

Summary of Experis Information Security Program Assessment Methodology

Information Security Program Discovery	Program Scope and Priorities	Information Security Program Assessment	Report Development
Task 1	*Task 2*	*Task 3*	*Task 4*
• Validate business areas and services to be included • Determine key internal and external program drivers • Identify security program structure, including processes and stakeholders (internal/external) • Determine applicable security standards and composite controls matrix to use • Identify critical security program elements to include in review • Identify key documents and stakeholders to include in assessment • Initiate a Document Request List (DRL) for information gathering	• Review discovered business and cyber security program documentation • Interview key security program stakeholders for current and strategic security needs • Identify recent, in-process and planned security initiatives affecting the scope of review • Determine scope and key priorities of the security program • Agree on a sampling plan to use for the assessment • Agree on the level of control, process and system inspection to be included in the assessment • Finalize the scope and timetable for execution	• Review key controls and processes against security drivers and requirements • Determine alignment of existing controls and processes with critical risks and threats • Identify any key risks and threats not addressed by current security controls • Determine high-level current state of security program elements against identified security requirements and agreed standards • Identify critical program risks, gaps and strategic opportunities and improvement areas that should be addressed • Determine a roadmap of prioritized actions to close critical gaps	• Agree on program review report format and content • Review and validate the draft capability ratings, risks, gaps and program opportunities with key stakeholders • Draft initial report of program capabilities, gaps, opportunities and recommended actions/ improvements for review • Hold a review meeting with stakeholders to discuss and agree on final content • Create and circulate report and collect feedback • Revise and deliver the final information security program assessment report

Source: Experis Information Security Program Assessment Methodology

The engagement was conducted in 2 steps:

Step 1: Tasks 1 and 2 above were initially completed and high level results were presented to help plan subsequent tasks. The County was asked to approve continuation to Step 2, below, prior to proceeding.

Step 2: After approval to proceed was given, Tasks 3 and 4 were completed as specified above.

We used this two-step approach to ensure that preliminary work warranted the expenditure of resources for the complete project. It became clear early in Step 1 that the full assessment was warranted. It was also clear early in Step 1 that the Department of Administrative Services Information Management Services Division (IMSD) was willing to commit to, and engage in, the robust evaluation aspects of Step 2.

Overall Observation and Recommendations

The observations, findings, and recommendations resulting from the review contain sensitive information and are disclosed in a separate, confidential report. We are happy to make the Experis team available to Executive and Legislative officials to discuss the reports privately or in closed session.

We appreciated the cooperation of IMSD throughout the review process. The Division has demonstrated a commitment to address issues noted in the report and has indeed already taken steps to ensure a more secure technology environment for Milwaukee County. Our office will continue to work with IMSD to address items in need of corrective action. We have also committed to addressing recommendations made by Experis to strengthen our audit efforts regarding cybersecurity.

Jerome J. Heer

JJH/cah

cc: Teig Whaley-Smith, Director, Department of Administrative Services
Laurie Panella, Chief Information Officer, DAS-IMSD
Steven Kreklow, Director of Performance Strategy & Budget, DAS
Steve Cady, Research & Policy Director, Office of the Comptroller
Kelly Bablitch, Chief of Staff, County Board Staff
Janelle Jensen, Chief Committee Coordinator, County Board Staff