Follow-up on ICE Access to County Data Shows Privacy Program Gaps

King County Information Technology (KCIT) hired a privacy program manager to begin working on our audit recommendations in May 2020. The department has taken steps to set up a privacy program including updating security policies and developing training. KCIT anticipates that work to develop and implement the program will continue into 2022. KCIT and the Public Records Committee (PRC) set up a Privacy Workgroup to facilitate ongoing collaboration on recommendations related to records and data containing personally identifiable information (PII). The department is poised to make more progress when vendors complete contracted work assessing the County's privacy maturity level and developing a plan to roll out a privacy program.

The Department of Adult and Juvenile Detention (DAJD) completed implementing its recommendations to protect citizenship and place of birth information for people in custody. DAJD created processes to ensure compliance with county code by updating its policies to prevent the possibility of collecting personal information that could be used inappropriately.

The Office of Equity and Social Justice (OESJ) completed its recommendation to create and implement a countywide training plan educating agencies on King County Code 2.15. OESJ had made significant progress developing a training program for county agencies on protecting data on citizenship and immigration status in 2019, but staff turnover and redeployment to the public health department to manage the COVID-19 pandemic delayed completion. As of March 2021, OESJ began training county staff.

Of the 14 audit recommendations:

	8 DONE		4 PROGRESS		2 OPEN
Fully implemented Auditor will no longer monitor.		**Partially implemented** Auditor will continue to monitor.		**Remain unresolved** Auditor will continue to monitor.	

Please see below for details on the implementation status of these recommendations.

Recommendation 1	On November 26, 2019	DONE ✓

Recommendation 2	On November 26, 2019	DONE ✓

Recommendation 3	On November 26, 2019	DONE ✓

Recommendation 4 — DONE ✓

To comply with county code 2.15, the Department of Adult and Juvenile Detention should establish and monitor a performance measure to ensure its personnel inform people in custody in a timely manner when it receives Immigration and Customs Enforcement hold, notification, or transfer requests for them.

STATUS UPDATE: As of November 2019, DAJD had set a target of notifying people in custody of an U.S. Immigration and Customs Enforcement (ICE) hold, notification, or transfer request within two days of DAJD's receipt. Of the 168 ICE requests DAJD received in 2020, there were only three instances where a person remained in custody more than two days after an ICE request was received and they were not given a copy of it. In the vast majority of cases, the person got a copy of the ICE request the same day it was received. DAJD tracks timeliness data and command staff review it weekly. When there are instances that exceed DAJD's target timeframes, staff receive additional training to correct the problem.

IMPACT: DAJD has shown compliance with county code 2.15.020 D. 2., which requires the agency to provide people in custody with a copy of any ICE hold, notification, or transfer request "upon receipt." Promptly providing people the information that they are being tracked by immigration enforcement agents enables them to work more effectively with legal counsel.

Recommendation 5	On November 26, 2019	DONE ✓

Recommendation 6 — DONE ✓

To comply with county code 2.15, the Department of Adult and Juvenile Detention should inform people of their right not to answer questions about citizenship status or place of birth and the reasons for these questions.

STATUS UPDATE: DAJD changed its foreign national policy in December 2019 to prohibit staff inquiries as to peoples' citizenship status or place of birth during the jail intake process. As of February 2021, the department updated its Inmate Information Handbook to emphasize that people in custody are not required to answer questions about citizenship status or place of birth. DAJD offers handbooks at intake and they are also available upon request at any time. Because

staff no longer ask questions about citizenship or place of birth, DAJD did not include reasons for these questions in its revised handbook.

IMPACT: DAJD has demonstrated compliance with county code 2.15.010 E., which prohibits county employees from inquiring about citizenship or immigration status or place of birth of any person. Changing procedure to prohibit employees from asking questions about citizenship or place of birth and informing people of their right not to answer such questions is a two-pronged approach. These actions ensure that information on citizenship and place of birth will not be obtained or recorded in the booking database where, if accessed inappropriately, it could be used for other purposes.

Recommendation 7 — DONE ✓

The Office of Equity and Social Justice should develop, document, and implement a training plan to assist agencies in implementing county code 2.15 in a timely manner.

STATUS UPDATE: Despite staff turnover and redeployment to respond to the COVID-19 pandemic, OESJ finished developing training materials and a plan to train all agencies in implementing county code 2.15. The two main parts are 1) ensuring that King County's data and resources are not used to assist in federal deportation efforts, and 2) ensuring that county agencies provide free interpretation and translation services to limited-English-proficient persons. All materials went through an additional review and approval process by OESJ's Prosecuting Attorney's Office liaison. OESJ staff began implementing their plan to train all county employees in March 2021.

IMPACT: Training employees to implement the provisions of county code 2.15 will promote trust and fairness for immigrant communities within King County by giving county agencies the tools to protect sensitive personal information and ensure equal language access to county services.

Recommendation 8 — PROGRESS ⋯

The Department of Information Technology should develop, document, and execute a countywide privacy program to implement county policy that clarifies roles and responsibilities and resource needs.

STATUS UPDATE: KCIT has taken steps to develop and document a privacy program. The department drafted a request for proposals (RFP) for a privacy maturity assessment, privacy program implementation plan, and a communication plan to facilitate adoption of the new countywide privacy program. KCIT plans to release the RFP in the first or second quarter of 2021 and predicts it will be seven months until required reports and plans are complete.

In preparation for the new privacy program, KCIT refreshed its security policies. As of February 2021, KCIT's Technology Management Board and the Business Management Council have approved 12 new or updated security policies. One example is the data security policy, which ensures controls are in place to prevent inappropriate access to data and protect the confidentiality, integrity, and availability of King County's data assets. KCIT is developing a training

plan for the new and updated policies that will help employees understand their roles and responsibilities.

KCIT also initiated a change in how the Office of Risk Management (ORM) characterizes risk to show privacy as a distinct impact area. By including privacy as a distinct impact area in its risk register, ORM will be able to assess privacy impacts countywide. This information will help KCIT to ensure county agencies appropriately safeguard sensitive data.

WHAT REMAINS: KCIT anticipates that its vendor will deliver the countywide privacy maturity assessment, privacy program implementation plan, and communication plan by early 2022. At that point, KCIT will need to finalize documentation of the privacy program and begin implementation. Full implementation requires involvement and collaboration from all branches of King County government, including those managed by separately elected officials.

Recommendation 9 — DONE ✓

The Department of Information Technology should collaborate with the Public Records Committee to develop and communicate tools for agencies to conduct privacy impact assessments.

STATUS UPDATE: KCIT and the PRC collaborated closely through a joint Privacy Working Group to develop a countywide privacy impact assessment tool that became effective in December 2020. KCIT and PRC determined that most county agencies do not have personnel with the necessary subject matter expertise to conduct privacy impact assessments. They designed the process to refer agency project staff to KCIT, where an information security risk and compliance analyst reviews the assessment request. The analyst then works with the KCIT privacy program manager to perform the assessment. Since December 2020, KCIT staff have engaged in discussions with two project groups to determine if they needed a privacy impact assessment. As a result of those conversations, they have two assessments scheduled in March.

KCIT also modified the phases for county IT projects to require project staff to identify PII much earlier in the project life cycle. This allows for early review and mitigation of potential privacy issues.

IMPACT: At the time of our audit, KCIT managers were only aware of county agencies conducting privacy impact assessments on health-related information and did not think they were widely used across the County. In addition, KCIT did not routinely collaborate with the PRC on privacy issues. As a result of the audit, KCIT and the PRC greatly enhanced their collaboration on privacy policy and governance. Together, they designed a privacy impact assessment in-line with national best practices and a method to conduct the assessments early in county project life cycles. Routine privacy impact assessments enhance KCIT's ability to identify and mitigate risks associated with unknown or unintended problematic data actions across the County.

Recommendation 10 — PROGRESS ⋯

To comply with county policy, the Department of Information Technology should collaborate with the Public Records Committee and Executive Senior Leadership Team to establish and

monitor performance measures to ensure that county agencies purge sensitive personal information in line with relevant records retention schedules.

STATUS UPDATE: KCIT stated that it is actively working with the PRC to determine an integrated approach to handling data expiration and purging. KCIT anticipates this will be completed by the fourth quarter of 2021. KCIT's Privacy Working Group, which includes the county information records manager, is working with the privacy program manager to establish performance measures related to this recommendation.

WHAT REMAINS: KCIT and PRC need to finish developing performance measures ensuring that county agencies purge sensitive personal information in-line with county policy. They need to work with the Executive Senior Leadership Team to finalize the measures and develop and implement a monitoring process.

Recommendation 11 — OPEN ⊗

The Department of Information Technology should develop, document, and implement a plan to ensure that all county information systems are capable of purging data in accordance with county policy and best practice.

STATUS UPDATE: KCIT stated that it is developing a standard for purging data that will allow data owners to achieve compliance with departmental retention policies. KCIT anticipates this will be completed by the fourth quarter of 2021.

Recommendation 12 — OPEN ⊗

The Department of Information Technology should work with the County Council and other stakeholders to establish, communicate, and use a common definition of personally identifiable information.

STATUS UPDATE: KCIT indicated that it has held initial internal discussions on this issue. Due to near-term challenges of the COVID-19 pandemic and overall KCIT workload, KCIT plans further action on this issue in the fourth quarter of 2021.

Recommendation 13 — PROGRESS ⊙

The Department of Information Technology should develop, document, and execute a plan to build and maintain an accurate and up-to-date inventory of personal information the County collects.

STATUS UPDATE: In August 2020, KCIT hired a data services person to conduct "data discovery," a process to catalogue various attributes of data held by county agencies. In March 2021, KCIT purchased a tool that the data services person will use to classify datasets as part of data discovery. Data discovery will allow the County to conduct a thorough inventory of PII enterprise wide, including identifying sensitive PII.

WHAT REMAINS: To complete this recommendation, KCIT needs to use the tool to build and maintain an accurate and up-to-date inventory of personal information the County collects.

Recommendation 14   PROGRESS ⬤

The Department of Information Technology should develop and disseminate tools for agencies to identify personally identifiable information collected in department databases that requires additional safeguards.

STATUS UPDATE: In February 2021, KCIT instituted a suite of new and updated information security policies (mentioned in Recommendation 1, above). Some of them directly assist agencies with identifying PII and appropriately safeguarding it.

First, the new KCIT Information Classification Policy helps agencies identify the sensitivity of information in county databases. It details a process to establish and control the level of potential risk and adverse impacts to technology assets using a classification system defined in the policy (see table below).

Category 1	Category 2	Category 3	Category 4
Public information	Sensitive information	Confidential information	Confidential information requiring special handling

Second, the new KCIT Data Security Policy directs agencies to complete information security risk and privacy impact assessments for category 3 or 4 data assets and then implement controls at the appropriate level.

KCIT is working on developing a training program to communicate the policies to relevant employees.

WHAT REMAINS: To ensure consistent data privacy across the county, KCIT needs to disseminate its security policies and other tools to relevant employees in all branches of King County government.

Luc Poon conducted this review. If you have any questions or would like more information, please contact the King County Auditor's Office at KCAO@KingCounty.gov or 206-477-1033.