


KING COUNTY AUDITOR'S OFFICE

JULY 9, 2019

ICE Access to County Data Shows Privacy Program Gaps

MEGAN KO
LAINA POON
BEN THOMPSON

Executive Summary

King County has made progress on its commitment to protect residents' privacy but has not put a robust privacy program in place. County policies discuss the need to safeguard information, but training and accountability is lacking. In this context, federal immigration agents maintained access to nonpublic information collected by law enforcement agencies, in violation of county code. We recommend that the County develop a privacy program, catalog personal information, and appropriately dispose of sensitive personal information. We also recommend training, regular monitoring, and other ways to ensure agencies comply with code-mandated protections of personal information for immigrant and nonimmigrant communities. In response to our findings, law enforcement agencies have started implementing added protections.

King County

ICE Access to County Data Shows Privacy Program Gaps

REPORT HIGHLIGHTS

What We Found

We found that U.S. Immigration and Customs Enforcement (ICE) agents had access to nonpublic information about people arrested and booked by county agencies, putting residents at increased risk of deportation. In violation of county code, the Department of Adult and Juvenile Detention (DAJD) and King County Sheriff's Office (KCSO) did not appropriately restrict access to nonpublic information to ensure that it was not used for civil immigration enforcement. We also found that in a one-month period, DAJD did not notify a significant portion of the people ICE asked DAJD to hold for civil immigration enforcement, reducing people's readiness to seek legal counsel. In some instances, DAJD also collected citizenship information, in violation of county code. In response to our findings, DAJD and KCSO have taken important first steps to implementing code-mandated protections.

King County made a commitment to protect residents' privacy but has not developed a robust program to carry it out. This increases the number of people at risk of someone inappropriately accessing or releasing their data. County policy discusses the need to safeguard data, but IT managers said that there is no accountability mechanism to ensure policy implementation. The County lacks a clear definition of personal information and a reliable inventory showing what personal information the County holds. Agencies have records retention schedules but do not follow them in ways that prioritizes people's privacy.

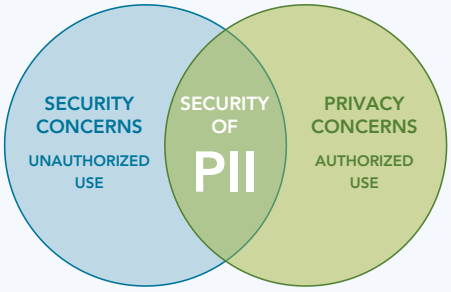
What We Recommend

We recommend that the County develop a privacy program, clearly define personal information, catalog the personal information it collects, and dispose of sensitive personal information in line with records retention schedules. We also recommend appropriate training, regular monitoring, and other methods to ensure that agencies comply with county legislation requiring the protection of personal information of immigrant and nonimmigrant communities.

Why This Audit Is Important

King County's Office of Risk Management reports that it is very likely for the County to experience a significant electronic security breach within the next five years. Unauthorized access to personal information could lead to serious harm to the County's reputation and finances and to the well-being of individuals and communities. County residents, including immigrants, law enforcement personnel, older people, youth, and people with disabilities, provide private information to county agencies to access essential services. King County Code establishes the County's commitment to protecting privacy for all residents and further clarifies the County's aim to protect citizenship information.

Protecting personal information is a matter of security and privacy



Note: PII means personally identifiable information.

Source: King County Auditor's Office, National Institute of Standards and Technology

ICE Access to County Data Shows Privacy Program Gaps

TABLE OF CONTENTS

ICE Regularly Accessed Law Enforcement Data

SECTION SUMMARY

Federal immigration agents had access to nonpublic information about people arrested and booked by county agencies, putting residents at increased risk of deportation. The King County Council passed an ordinance prohibiting agencies from providing personal information to federal immigration authorities for civil immigration enforcement in 2018. In violation of county code, the Department of Adult and Juvenile Detention (DAJD) and King County Sheriff's Office (KCSO) did not appropriately restrict information access to ensure that federal immigration agencies used nonpublic county data only for criminal cases. We found that U.S. Immigration and Customs Enforcement (ICE) regularly used nonpublic personal information, including addresses and photos, for everyone booked into county jails. We also found KCSO gave ICE unredacted case files in response to two dozen information requests. In a one-month period, DAJD did not notify a significant portion of the people ICE asked DAJD to hold for civil immigration enforcement, reducing people's readiness to seek legal counsel. Finally, DAJD collected citizenship information, encroaching on people's privacy and violating county policy. Appropriate training, regular monitoring, and minimal data collection and retention will allow the County to better protect residents' privacy. In response to our findings, DAJD and KCSO have taken important first steps toward implementing code-mandated protections.

ICE regularly accessed jail data

Federal agents regularly used jail data after county code prohibited their access, potentially leading to detention or removal of county residents. ICE accessed the data through a web service known as JILS LE, the law enforcement version of the Jail Inmate Lookup System (JILS).[1] JILS LE displays confidential information that is not available to the public, including photos, physical descriptions, addresses, and up to 50 aliases for each person booked into King County jails. Exhibit A lists all data fields in the JILS public and law enforcement versions. County code banned access to nonpublic facilities and databases by federal immigration agencies without criminal judicial warrants in early 2018.[2] With photos and addresses, federal agents can more easily identify and locate people, potentially leading to the detention or removal of county residents. Access logs show that 15 members of the ICE Detention and

[1] There are three versions of the Jail Inmate Lookup System: a public version and two nonpublic versions, one each for law enforcement and courts. Under RCW 70.48.100, data elements in a public jail register are a person's name, date and time of booking, reason for booking, and date and time of release.

[2] King County Code (KCC) 2.15.020 (B)(3) banned access to nonpublic databases without a criminal judicial warrant, while KCC 2.15.010 (I) prohibited employees from spending time or resources facilitating civil immigration enforcement, except where required by law.

Removal Unit logged in to JILS LE more than 1,000 times between March 2018 and April 2019.[3] During that period, DAJD recorded more than 40,000 bookings to the system.[4]

EXHIBIT A: ICE accessed nonpublic data in the Jail Inmate Lookup System (JILS) for Law Enforcement agencies

PUBLIC JILS DATA	NONPUBLIC JILS LE DATA
Bail amount	Address
Book of arrest number	Aliases
Charges	Arrest date
Court	Arresting/transport agency
Custody/facility	Birthdate
Date and time of booking	Booking photo
Date and time of release	Criminal justice identification numbers, e.g., FBI
Name	Eye color
Reason for release	Gender
	Height
	Race
	Weight

Note: Anyone can access public JILS data online without a user account. For JILS LE, the law enforcement version of the system, users need an account approved by DAJD.

Source: King County Auditor's Office

The Department of Juvenile and Adult Detention did not remove ICE accounts from JILS LE following code changes that restricted immigration authorities' access to nonpublic data. The County launched JILS in 2004. Before local legislation prohibited it, DAJD approved ICE access as a law enforcement agency that handles criminal cases. In 2018, county code banned access to nonpublic databases by federal immigration agencies without criminal judicial warrants. DAJD did not review access logs regularly or as a result of the code change. We requested access logs and, on April 9, 2019, notified DAJD and the Department of Information Technology (KCIT) that ICE was using the JILS LE. Five working days after we notified DAJD, it instructed KCIT to deactivate all ICE accounts.

We reviewed access logs again on May 1 and May 15, and found no evidence that ICE had used the system since deactivation. DAJD indicated that it plans to review user accounts monthly to ensure ICE does not access JILS LE going forward. In 2020, the County will replace JILS and other jail systems with a new jail management system (JMS). In setting up the JMS, KCIT and DAJD could require users to revalidate their

[3] Because the system does not log search history, we do not have evidence of who ICE searched.
[4] DAJD recorded 35,631 bookings in 2018 and targets 36,000 bookings in 2019. JILS records are updated in real time upon booking.

need and right to access the system, which could minimize the number of unauthorized users.

Recommendation 1

To comply with county code 2.15, the Department of Adult and Juvenile Detention should regularly monitor and manage access to nonpublic data systems to ensure that federal immigration authorities are not using them.

KCSO gave ICE case files upon request

The King County Sheriff's Office gave ICE unredacted case files in response to two dozen information requests, in violation of county code. KCSO received 25 information requests from ICE between January 2018 and May 2019, and in nearly all cases, provided ICE with requested documents. KCSO said that ICE provided either a person's name or case number for each request. However, KCSO did not determine whether ICE requests were for civil immigration enforcement before releasing county information. King County Code prohibits county agencies from providing personal information to federal immigration authorities for the purpose of civil immigration enforcement without a criminal judicial warrant or legal requirement to do so.[5] Other county law enforcement entities have taken steps to comply with this code. For instance, DAJD does not respond to requests for information from federal immigration authorities unless shown a criminal judicial warrant. In addition, the King County Regional Automated Fingerprint Identification System (AFIS) recently changed its standard operating procedures to prohibit sharing personally identifying fingerprint and other information with ICE unless the information pertains to a criminal matter. Without clear procedures, KCSO staff may be unaware of county policy directing them to handle ICE requests differently than those of other law enforcement agencies.

Recommendation 2

To comply with county code 2.15, the King County Sheriff's Office should develop, document, and implement a plan to ensure that it does not provide personal information to federal immigration authorities for civil immigration enforcement without a criminal warrant or legal requirement.

[5] KCC 2.15.020 (B)(4)

DAJD did not give copies of ICE detainers

DAJD did not give people copies of hold requests it received from ICE to hold them in custody, violating code and reducing people's readiness to seek legal counsel. After learning that ICE had access to DAJD data, we reviewed the most recent hold requests, also known as detainers, ICE sent to DAJD and contacted county personnel to determine if DAJD was following code requirements for notification.[6] King County Code (KCC) 2.15 requires DAJD: 1) to provide people with a copy of the ICE detainer, and 2) to inform people of the detainers placed on them as well as DAJD's intent to comply or not. We found that DAJD did not give people copies of the original detainers, which would have made it more difficult for them to work with legal counsel. We also found that DAJD did not inform people of detainers in 48 percent (21 of 44) of instances reviewed, potentially leaving these individuals unaware that they were being tracked by immigration enforcement agents. In all of the cases where DAJD did give notice, it stated that it did not intend to comply with the ICE detainer.

DAJD said it usually informs people within 24 hours of a receiving a detainer but that it can take up to a week. In 6 of 21 instances where DAJD did not inform people of the detainers, DAJD received the detainer more than a week before the person was released from the jail (see Exhibit B). Code does not specify a timeframe for when DAJD should notify people of the requests.

EXHIBIT B: DAJD had time to notify several people who were not informed of ICE hold requests

Available time to inform	Not informed
Less than 24 hours	7
24 hours to a week	8
More than a week	6
TOTAL	21

Note: Of 44 people in custody, DAJD informed 23 of ICE detainers and did not inform 21. This table shows a breakdown of those not informed by the time between DAJD's receipt of the detainer and either the person's release from custody or, in two cases, the time of our analysis.

Source: King County Auditor's Office

Recommendation 3

To comply with county code 2.15, the Department of Adult and Juvenile Detention should provide people in custody with copies of any Immigration and Customs Enforcement detainer hold, notification, or transfer requests placed on them while in custody.

[6] We reviewed 48 hold requests from March and April 2019, and 44 of the 48 requests referred to people who were in DAJD custody on the day ICE faxed the request to DAJD. DAJD estimates that it receives up to 300 ICE hold requests a year.

Recommendation 4

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.

DAJD collected citizenship data

DAJD collected data on citizenship and place of birth in its jail booking system without clear purpose or informed consent, violating code. Under certain circumstances,[7] DAJD policy directs intake officers to determine people's nationality at booking to carry out bilateral federal agreements to notify certain foreign consulates when their citizens are detained (see Appendix 1). DAJD personnel do not use the booking database to complete this task. Instead they ask verbally and, where applicable, notify consulates via fax. This means that information on place of birth and citizenship does not need to be recorded in the booking database, where, if accessed inappropriately, it could be used for other purposes. County code prohibits employees from maintaining or sharing information on national origin and mandates that county employees explicitly inform people of their right not to answer when asked about their citizenship status.[8] Booking personnel said that they do not tell people being booked into the jail that they have the option not to answer questions about citizenship information. Without informed consent, residents may feel coerced to respond. Because this information is put into a database, it may be subject to a data breach. Citizenship and place of birth are not required data fields in the booking database.

To protect people's privacy, national standards recommend, and KCC 2.14 directs, that organizations minimize their collection of personal information to what is strictly necessary to accomplish their mandated functions.[9] Currently, DAJD's booking system contains about 550,000 records of people's citizenship information, including roughly 40,000 foreign nationals and 40,000 blanks or data errors. Because data from existing records can auto populate new booking records, the system can update an individual's citizenship information without data entry by booking officers. DAJD and KCIT analysis showed that in the year ending April 2019, citizenship information was updated in the booking system for 53 percent of the county's 35,000 bookings. DAJD is working to replace its 40-year-old jail management system in 2020. This creates an opportunity for DAJD to purge unnecessary personal information by not migrating it to the new system, or to omit sensitive data fields from the new system completely to minimize the collection of personal information.

[7] Namely, where DAJD is the arresting agency, where people in custody request consular contact, or where DAJD staff become aware that an arresting agency did not complete consular notification.
[8] KCC 2.15.010 (E) and (G). KCC 2.15.020 (D)(3) further specifies that informed consent applies in cases of mandatory consular notification
[9] KCC 2.14.030 (B)

Recommendation 5

To comply with county code 2.15, the Department of Adult and Juvenile Detention should develop, document, and implement a plan to ensure that citizenship status and place of birth is not collected in its data systems.

Recommendation 6

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.

County did not prioritize immigrant privacy

King County has made slow progress training agencies on immigrant privacy protections, reducing County capacity to implement them effectively. County code directs agencies to review what data they collect and remove prompts for citizen or immigration status where possible.[10] This would help reduce the amount of sensitive personal information the County holds—and is therefore responsible for protecting. The County Council directed the County Executive to ensure employees receive training on how to implement code provisions that establish how agencies provide services to immigrant communities.[11] Thus far, the Office of Equity and Social Justice (OESJ), which is responsible for the training, has worked with Public Health - Seattle & King County to review all of its data collection forms and train managers and clinics in south King County. However, OESJ has made little progress with other agencies. OESJ stated that it puts relevant training on hold to prioritize the development of language assistance plans, also required by KCC 2.15. County Council mandated the County Executive submit these plans by September 30, 2018. Since code did not establish a timeline for training, OESJ made it a lower priority.

Recommendation 7

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.

[10] KCC 2.15.010 (B). This provision was first introduced in 2009 through Ordinance 16692, stating that agencies act "promptly" in their review. The 2018 ordinance removed the word "promptly."
[11] KCC 2.15.010 (K)

Need for a Privacy Program

SECTION SUMMARY

King County made a commitment to protect residents' privacy but has not developed a program to carry it out, leaving personal information at risk. County policy discusses the need to safeguard data but does not outline clear roles and responsibilities. The County lacks a clear definition of personal information and a reliable inventory showing what personal information the County holds. Agencies have records retention schedules but do not follow them in a way that prioritizes people's privacy. We recommend that the County develop a privacy program, clearly define personal information, catalog the personal information it collects, and dispose of sensitive personal information in line with records retention schedules.

Accountability gaps lead to privacy risks

Unclear responsibility for safeguarding personal information puts residents' privacy at risk. In the case of ICE access to DAJD's nonpublic data, both DAJD and KCIT were aware that JILS LE contained confidential criminal justice information. However, following the passage of county code prohibiting ICE access to nonpublic databases, neither DAJD nor KCIT initiated a review of user access. County code 2.14 states that the "data collector" is responsible for protecting personal information. Meanwhile, King County's Enterprise Risk Register lists all county agencies as accountable for managing the risk of an electronic security breach.

County policy states that the county's chief information security and privacy officer is responsible for guiding the county's privacy program, but a formal privacy program does not yet exist in King County.[12] Further, KCIT's Information Technology Plan 2016-2019 does not include a privacy program, indicating that establishing a formal privacy program has been a relatively low priority for the agency. KCIT has launched cybersecurity training including a module on privacy that directs employees to read various privacy and information security policies. However, most employees have not taken this training, so they may not be aware of the policies. KCIT managers stated that there is no mechanism for accountability to ensure that county entities implement the policies.

For example, one of the assigned policies, KCIT's 2010 Information Privacy Policy, assigns "Privacy Coordinators" responsibility for resolving privacy issues within county agencies and reporting concerns to KCIT. KCIT managers were unaware of the existence of agency Privacy Coordinators other than those who deal with protected health information, so this role is largely unfulfilled.

In addition, while the privacy policy requires that agencies retain personally identifiable information (PII) only as long as it is necessary to conduct county business and in accordance with the records retention schedules, public records officials indicated that

[12] Per 2010 KCIT Information Privacy Policy

although county agencies dedicate resources to records management, a significant amount of work remains in order to effectively manage records throughout their lifecycle, including at the end of their applicable retention period. The county's Public Records Committee (PRC) and Executive Senior Leadership Team are responsible for spearheading implementation of county records policy, which includes compliance with records retention schedules. The County Council created the PRC in 2006 in response to public concerns after the King County Recorder's Office posted social security numbers on county websites.[13] According to a senior PRC member, the PRC is a resource to support agency compliance with privacy policies to protect personal information, but it does not have the ability to enforce compliance with policy, nor does KCIT routinely collaborate with PRC on privacy initiatives.

As another example, KCIT's privacy policy calls on staff to limit how much personal information they collect. However, it does not mention what the process would be to stop collecting information if it is agency policy to do so. National best practice suggests that agencies conduct privacy impact assessments to look at what information they are collecting, why they are collecting it, and how it will be secured whenever they begin collecting, maintaining, or sharing personal information. KCIT managers were only aware of privacy impact assessments related to health information and did not think they were widely used across the county. The lack of a visible and functional privacy program to coordinate responses to such a high-level risk increases the county's vulnerability to data loss and liability.

EXHIBIT C: Privacy can be compromised in various ways

TYPE	BREACH	SPILL	LEAK
DESCRIPTION	Unauthorized access	Accidental release	Purposeful release

Source: King County Auditor's Office

Recommendation 8

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.

[13] The PRC is made up of a broad range of county departments and elected agencies.

Recommendation 9

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

County keeps personal information too long

Some county agencies retain personal information too long, increasing the number of people affected by potential data loss. County policies and national best practices require that records of personal information be securely disposed of once their retention periods have passed.[14] In addition to protecting privacy, purging records in accordance with relevant laws and schedules creates efficiencies by reducing the amount of information that needs to be reviewed, redacted, and released for public records requests. The County lacks comprehensive data on compliance with records retention schedules, and records management staff told us that most agencies are only partially compliant.[15] For example, DAJD has not purged its booking database in 40 years because the system does not allow for data removal, and DAJD views this data as important to understanding the jail population. Records management staff told us that few county databases have a purge function, suggesting that other agencies are keeping information longer than necessary due to technical constraints.

Recommendation 10

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.

Recommendation 11

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.

[14] The county policies are Management of King County Public Records, INF 15-4(AEP), and Information Privacy Policy, ITG-P-05-04-01.

[15] Records retention schedules list the records kept by an agency, how long an agency must retain these records, and whether an agency should archive or purge the records after the retention period ends.

No clear definition of PII

King County lacks a clear and consistent way of determining what counts as sensitive personal information, making it difficult for agencies to use appropriate safeguards. County definitions of PII range from narrow to broad. For example, KCC 2.14 narrowly defines "personal identifying data" as just three things: social security number, date of birth, or mother's maiden name. The same section of code separately defines "personal data" as "any information concerning an individual that can be readily associated with a particular individual." KCIT's Information Privacy Policy mirrors the broader second definition but applies it to a term closer to the subject of the first definition, namely "personally identifiable information" (see Exhibit E). In 2018, the County Council revised county code 2.15 to add a definition of "personal information" that mentions various types of contact information including addresses. Addresses were one of the nonpublic pieces of information available in the nonpublic JILS LE system that ICE was able to access. The 2018 code revision focused on immigration enforcement as one unintended use of personal information the County holds.

A 2016 KCIT report to the County Council on personal information and privacy within King County recommended revising the county's definition of personally identifiable information to match national best practice. This is because the definition of "personal identifying data" that remains in county code is too narrow to protect people's privacy (see examples of personal information in Exhibit D). A common, countywide definition of sensitive personal information would help county agencies implement privacy policies more consistently.

EXHIBIT D: Selected examples of personally identifiable information as defined in national standards

NAMES	NUMBERS	CONTACTS	BIOMETRICS	OTHER
Alias	Bank card	Email address	Fingerprints	Gender
Full name	Birthdate	Home address	Photographs	Place of birth
Maiden name	State, federal IDs	Phone number	Retinal scan	Race
Mother's maiden name	Taxpayer identification		Voice signature	Religion

Source: King County Auditor's Office and National Institute of Standards and Technology

EXHIBIT E: County definitions of sensitive personal information range from narrow to broad

PHRASE	DEFINITION	POLICY
Personal data	Any information concerning an individual that can be readily associated with a particular individual	KCC 2.14 (1996)
Personal identifying data	Social security number, date of birth, or mother's maiden name	KCC 2.14 (1996)
Personally identifiable information	Any information concerning an individual which is contained in an organization record and, because of name, identifying number, image, mark, or description, can be readily associated with a particular individual, including information contained in printouts, forms, written analyses, or evaluations	KCIT Information Privacy Policy (2010)
Personally identifiable information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual	NIST* (2017)
Personal information	One or more of the following, when the information is linked with or is reasonably linkable, including via analytic technology, to the person's first name or first initial and last name: 1. Home address 2. Work address 3. Telephone number 4. Electronic mail address 5. Social media handle or other identifying social media information 6. Any other means of contacting a person 7. Social security number 8. Driver's license number or Washington identification card number 9. Bank account number or credit or debit card number 10. Information or data collected through the use or operation of an automated license plate recognition system 11. User name that, in combination with a password or security question and answer, would permit access to an online account	KCC 2.15 (2018)

*NIST refers to the National Institute of Standards and Technology

Source: King County Auditor's Office

Recommendation 12

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.

County unaware what personal information it has

The County does not know where it keeps sensitive personal information, stalling efforts to safeguard it efficiently and effectively. National best practice recommends that organizations identify all personal information they have using questionnaires, reviews of system documentation, interviews, and other methods. We found that KCIT has a countywide database with fields to classify software applications based on what kinds of personal information the applications contain.[16] However, KCIT staff indicated that it is not clear who is responsible for updating classification information. KCIT had only applied data classifications to about half of the 1,178 executive agency applications in its database (see Exhibit F).[17] While not all unreviewed applications necessarily contain PII, a review of application titles suggest that some may.

[16] The tags were for protected personal information, financial information, health information, and criminal justice information. Data classification categories are Confidential, Confidential with Special Handling, Sensitive, or Public and are related to the existence of protected personal information.

[17] The proportion was similar for non-executive agencies, but we did not include them because KCIT's authority is less direct for non-executive agencies than for executive agencies.

EXHIBIT F: KCIT has reviewed about half of county applications for personal information

Executive Agency	Total applications	% reviewed for PII
Public Health – Seattle & King County	114	93%
Department of Adult and Juvenile Detention	57	84%
Department of Community and Health Services	58	76%
Department of Natural Resources and Parks	144	76%
King County Metro Transit	259	61%
Department of Local Services	74	51%
Department of Executive Services	135	44%
King County Executive's Office	13	38%
Department of Public Defense	7	29%
Department of Information Technology	247	15%
Department of Judicial Administration	41	5%
TOTAL	**1,178**	**54%**

Source: King County Auditor's Office analysis of KCIT data

Even where KCIT has labeled applications as containing personal information, the data may not be reliable. KCIT security staff recently reviewed the database and found applications labeled as not having personal information that did have personal information, and vice versa. We interviewed KCIT personnel and found that agencies determine what labels KCIT applies. KCIT does not provide any guidance to agencies or its internal staff on what these labels mean and does not conduct regular reviews to verify that the labels they apply are correct. Without an integrated privacy program, KCIT does not currently use this information to apply privacy safeguards. In summary, the county's most ready-made personal data inventory is incomplete and not yet reliable for use in deploying privacy safeguards based on data security needs.

Recommendation 13

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.

Recommendation 14

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.

Appendix 1

List of Countries with Mandatory Consular Notification

Albania	Czech Republic	Malaysia	Singapore
Algeria	Dominica	Malta	Slovakia
Antigua & Barbuda	Fiji	Mauritius	Tajikistan
Armenia	Gambia	Moldova	Tanzania
Azerbaijan	Georgia	Nigeria	Tonga
Bahamas	Ghana	Philippines	Trinidad & Tobago
Barbados	Grenada	Poland	Tunisia
Belarus	Guyana	Romania	Turkmenistan
Belize	Hungary	Russia	Tuvalu
Brunei	Jamaica	Saint Kitts & Nevis	Ukraine
Bulgaria	Kazakhstan	Saint Lucia	United Kingdom
China, Macao, Hong Kong	Kiribati	Saint Vincent & Grenadines	Uzbekistan
Costa Rica	Kuwait	Seychelles	Zambia
Cyprus	Kyrgyzstan	Sierra Leone	Zimbabwe

Source: King County Auditor's Office, U.S. Department of State

Executive Response

King County

Dow Constantine
King County Executive
401 Fifth Avenue, Suite 800
Seattle, WA 98104-1818
206-263-9600 Fax 206-296-0194
TTY Relay: 711
www.kingcounty.gov

July 1, 2019

RECEIVED

JULY 1, 2019

KING COUNTY
AUDITOR'S OFFICE

Kymber Waltmunson
King County Auditor
Room 1033
COURTHOUSE

Dear Ms. Waltmunson:

Thank you for the opportunity to review and comment on the proposed final report "ICE Access to County Data Shows Privacy Program Gaps." I appreciate the work your office has done to ensure King County continues to make progress in extending the most rigorous privacy protections across all manner of electronic data.

We concur with the audit recommendations and appreciate the acknowledgement of our efforts to safeguard immigrant legal rights at a time when they are under constant assault by the Trump administration. For example, the Department of Adult and Juvenile Detention (DAJD) has not honored U.S. Immigration and Customs Enforcement (ICE) detainers without a judicial warrant since County code prohibited such practice in 2013. In addition, DAJD has not allowed ICE to access inmates, also consistent with County code.

Five days after receiving notice from the Auditor's Office that ICE was using the Jail Inmate Lookup System-Law Enforcement database to access confidential information of inmates including photograph, physical description and aliases, DAJD instructed King County Information Technology to deactivate all ICE accounts. It should be noted that we know of no circumstance where federal agents used this data to detain or remove county residents.

Effective June 4, in response to your report, DAJD stopped requesting information about the citizenship, immigration status or place of birth of anyone being booked into our facilities. DAJD is also now providing copies of each detainer received to the involved inmate in a timely manner. These changes are now incorporated into a DAJD policy which governs all DAJD related immigration issues. (Copy attached).

We concur with recommendations for a more robust privacy program throughout county government, and increased focus on training and regular monitoring to ensure all agencies comply with policies and legislation.

At King County, we value the communities that we serve and recognize the importance of personal information. We are committed to building trust through transparency and protection of privacy information, while at the same time meeting our legal commitments and business needs.

King County Department of Information Technology is currently updating the privacy program to better support our commitment to privacy and the communities we serve. Starting in July 2019, KCIT has a policy revamp effort that will update all security and privacy policies. King County's new privacy program will include updated details on the collection, use, disclosure, sharing, security, retention, and individual's choices related to their personal information that we receive through King County business and services; whether in person, online or by mail. Our privacy policy will be easy to read and understand. Demonstrating good data stewardship and practices is important to us and work is already well underway. This work is being led by the King County Chief Information Security & Privacy Officer. The programs to implement and enforce these policies are expected to launch early 2020. It should be noted that separately elected officials follow their own privacy policies and programs and are not accountable to KCIT.

Thank you again for your important work on behalf of King County. If you have any questions regarding our audit response, please contact Casey Sixkiller, Chief Operating Officer, Office of the Executive at 206-263-5700.

Sincerely,

Dow Constantine
King County Executive

Enclosure

cc: Rachel Smith, Deputy County Executive, King County Executive Office (KCEO)
Casey Sixkiller, Chief Operating Officer, KCEO
John Diaz, Interim Director, Department of Adult and Juvenile Detention
Tanya Hannah, Director, Department of Information Technology

King County	Department of Adult and Juvenile Detention All Divisions General Policy Manual	
	Chapter 5 Intake, Transfer and Release	
5.02.017 **ICE Detainers and Administrative Warrants, Gathering Immigration Related Information and Consular Notification/Access, and Access to Inmates and Records by Federal Immigration Authorities**	Approved By:	Interim Director John Diaz
	Effective Date:	6/28/19
	Reviewed By:	PRC Committee
	Review Date:	June 27, 2019
Distribution:	Document Code No.	

Statement of Purpose

The purpose of this policy is to describe actions necessary to comply with county code and state law related to inmate immigration status and access by federal immigration authorities to inmates and information absent an appropriate criminal warrant. The county has taken actions to limit the collection of data regarding citizenship and place of birth, and to limit involvement in civil immigration matters. Additionally, the policy is intended to clarify issues of consular notification.

Policy

Detainers and Administrative Warrants: DAJD will only honor Immigration Detainers or Administrative Warrants that are accompanied by a criminal warrant issued by a U.S. District Court Judge or magistrate.

Gathering Immigration Related Information and Consular Notification: DAJD will not inquire about, or request from any person information about the citizenship or immigration status or place of birth of any person booked into DAJD facilities. However, if DAJD becomes aware that an inmate is a Foreign National it will ensure that consular notification is pursued in accordance with applicable law.

Access to Inmates by Federal Immigration Authorities: DAJD will not permit ICE, CBP or USCIS officers, agents or representatives access to inmates without a judicial criminal warrant.

Limited Access to Records and Information by Federal Immigration Authorities: DAJD will not release inmate records to ICE, CBP, or USCIS officers, agents or employees beyond what is available to the public under state law without an accompanying criminal warrant issued by a U.S. District Court Judge or magistrate. DAJD will not provide ICE, CBP, or USCIS officers, agents or employees access to non-public databases or interfaces under the control of DAJD, such as JILS LE. DAJD employees may not provide any information, except as noted below, to ICE, CBP, or USCIS officers, agents or employees without an accompanying criminal warrant issued by a U.S. District Court Judge or magistrate. The fact that some inmate records may be available to the public does not mean that DAJD staff may discuss the information contained in those records with ICE, CBP, or USCIS officers, agents or employees. Staff may refer federal immigration authorities to DAJD public-facing websites.

Exception to Limited Access to Information by Federal Immigration Authorities: Under federal law, 8 U.S.C. Section 1373, local governments may not prohibit their employees from discussing a person's "immigration status" with federal officials. While it would be unusual for a DAJD employee to have definitive information about the actual immigration status of inmates, discussions about an inmate's "immigration status" are not prohibited by this policy.

References

K.C.C.	Chapter 2.15
Federal	8 U.S.C. 1373 Vienna Convention on Consular Relations, Article 36
RCW	70.48.100 43.43.705 ESSSB 5497
Department Forms	Consular Notification Form (F-620) Notice of Request for Hold (F-808)
Department Policy	1.01.012, Release of Information 5.02.004 Booking Procedures 5.01.001 Intake Procedures 5.02.003 Booking of Foreign Nationals

Definitions

Administrative Warrant: A noncriminal immigration warrant of arrest, order to detain or release alien, notice of custody determination, notice to appear, removal order, warrant of removal or any other document, issued by the USDHS sub-agencies ICE,

CBP, or USCIS that can form the basis for a person's arrest or detention for civil immigration enforcement purposes.

CBP: The United States Customs and Border Protection agency of the United States Department of Homeland Security.

Criminal Justice Agency: Agencies whose principle function is to apprehend, prosecute, adjudicate, or rehabilitate "criminal offenders."

DHS: The United States Department of Homeland Security.

Immigration Detainer: A request from ICE for DAJD to provide notice of release or maintain custody of a person based upon an alleged violation of civil immigration law.

ICE: The United States Immigration and Customs Enforcement agency of the United States Department of Homeland Security.

USCIS: The United States Citizenship and Immigration Services agency of the United States Department of Homeland Security.

General Guidelines

A. Immigration Detainers and Administrative Warrants

1. DAJD will only honor Immigration Detainers and Administrative Warrants that are accompanied by a criminal warrant issued by a U.S. District Court Judge or magistrate.
2. Upon receiving an Immigration Detainer or Administrative Warrant DAJD staff shall provide a copy of the Immigration Detainer or Administrative Warrant to the subject inmate and inform the inmate whether DAJD intends to comply with the Immigration Detainer or Administrative Warrant (Form F-808).

B. Gathering Immigration Related Information and Consular Notification

1. DAJD will not inquire about, or request from any person information about the citizenship or immigration status or place of birth of any person booked into DAJD facilities.
2. However, if DAJD becomes aware that an inmate is a Foreign National it will ensure that the county pursues consular notification pursuant to the Vienna Convention and/or U.S. bilateral treaties. An examples of when this could occur is when the inmate volunteers that he or she is a foreign national and requests consular notification.

C. Access to Inmates by Federal Immigration Authorities:

1. DAJD will not permit ICE, CBP or USCIS officers, agents or representatives access to an inmate without a criminal warrant issued by a U.S. District Court Judge or magistrate.

D. Access to Records and Information by Federal Immigration Authorities:

1. The Department will not release inmate records, beyond what is available to the public under RCW 70.48.100(1) to ICE, CBP, or USCIS officers, agents or employees. The fact that some inmate records may be available to the public does not mean that DAJD staff may discuss the information contained in those records with ICE, CBP, or USCIS officers, agents or employees.
2. DAJD employees may not provide any information, including a person's next court date or release date, to ICE, CBP, or USCIS officers, agents or representatives, except that nothing in this policy prohibits DAJD employees from sending to, receiving from, requesting from, or exchanging with any federal, state or local governmental agency information regarding the immigration status of a person or from maintaining such information. Staff may direct federal immigration authorities to DAJD public-facing websites.
3. The Department will not provide ICE, CBP, or USCIS officers, agents or employees access to non-public databases or interfaces under the control of DAJD, such as JILS LE.

Procedure

A. Consular Notification

1. If an inmate seeks consular notification or DAJD becomes aware, without making an inquiry, that an inmate is a Foreign National, Officers shall follow DAJD Policy, 5.02.003 Booking of Foreign Nationals.

B. Access to Records and Information by Federal Immigration Authorities:

1. The Department will monitor databases and interfaces under DAJD control such as JILS LE, to ensure ICE, CBP, or USCIS officers, agents or employees have not been provided access.

Recommendation 1

To comply with county code 2.15, the Department of Adult and Juvenile Detention should regularly monitor and manage access to nonpublic data systems to ensure that federal immigration authorities are not using them.

Agency Response	
Concurrence	**Concur**
Implementation date	4/16/19
Responsible agency	DAJD
Comment	DAJD removed ICE access to JILS LE on 4/16/19; same date DAJD implemented monthly QA to determine if ICE had gained access. DAJD implemented new immigration policy/prodedure on 6/28 providing additional guidance to staff. DAJD and KCIT also developing access management protocols design for new Jail Management System in order to better manage external agency access, provide auditing and QA ongoing. DAJD is in the process of replacing a cumbersome 40 year old mainframe system for inmate data that makes managing information challenging.

*Recommendation 2 was sent to the King County Sheriff.

Recommendation 3

To comply with county code 2.15, the Department of Adult and Juvenile Detention should provide people in custody with copies of any Immigration and Customs Enforcement detainer hold, notification, or transfer requests placed on them while in custody.

Agency Response	
Concurrence	**Concur**
Implementation date	5/3/19
Responsible agency	**DAJD**
Comment	DAJD began providing detainer and notice form (F-808) to inmates in custody who are the subject of ICE detainer. DAJD implemented new immigration policy/procedure on 6/28 providing additional guidance to staff.

Recommendation 4

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.

Agency Response

Concurrence	**Concur**
Implementation date	9/6/19
Responsible agency	**DAJD**
Comment	County Code 2.15 does not indicate timing to provide notice of detainers. DAJD is providing notice expeditiously and is evaluating methods, measures and means to lean the timeframe further.

Recommendation 5

To comply with county code 2.15, the Department of Adult and Juvenile Detention should develop, document, and implement a plan to ensure that citizenship status and place of birth is not collected in its data systems.

Agency Response

Concurrence	**Concur**
Implementation date	6/3/19
Responsible agency	**DAJD**
Comment	DAJD staff instructed on 6/3 to discontinue collecting citizenship and place of birth information; KCIT also began working on computer application system changes to remove both fields. DAJD implemented new immigration policy/prodedure on 6/28 providing additional guidance to staff.

Recommendation 6

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.

Agency Response

Concurrence	**Concur**
Implementation date	6/3/19
Responsible agency	**DAJD**
Comment	DAJD staff instructed on 6/3 to discontinue asking questions about citizenship or place of birth. DAJD will amend the inmate handbook to inform inmates that they have the right not to answer questions about citizenship status or place of birth.

Recommendation 7

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.

Agency Response

Concurrence	**Concur**
Implementation date	11/1/19
Responsible agency	**OESJ**
Comment	The Office of Equity & Social Justice will build on work already done with departments to develop, document and deliver training, and also update training content as needed given the newest tactics of the federal government.

Recommendation 8

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.

Agency Response

Concurrence	**Concur**
Implementation date	06/29/2020
Responsible agency	**KCIT**
Comment	King County's current privacy policy is from 2010 and lacks an active operational program to support it. KCIT is addressing an updated privacy program, in concert with an updated security program, for countywide implementation. King County's new privacy program will include updated details on the collection, use, disclosure, sharing, security, retention, and individuals' choices related to their personal information that King County receives through business and services; whether in person, online or by mail. The scope of compliance and enforcement efforts will be related to King County enterprise systems and services only.

Recommendation 9

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

Agency Response

Concurrence	**Concur**
Implementation date	06/29/2020
Responsible agency	**KCIT**
Comment	A Privacy Impact Assessment (PIA) form/ template has been drafted and procedures need to be developed to integrate into all technology project lifecycles and to guide employees on how to conduct an assessment to identify privacy risks and to implement appropriate controls to reduce the risk of privacy violations. Industry best practices will be used to set the standard and stakeholders will be educated on the importance of conducting a PIA. Collaboration, coordination, and communication efforts will continue to be addressed through the rest of 2019, with full implementaton to be tied to the launch of the new privacy program in 2020.

Recommendation 10

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.

Agency Response

Concurrence	**Concur**
Implementation date	6/29/2020
Responsible agency	**KCIT**
Comment	As noted above, KCIT recognizes the importance of trust and protection of personal information and are committed to establishing program performance measures within the new privacy program. We want to be able to provide evidence of our compliance with policies, procedures, legislative and regulatory requirements, as well as to our commitment to good data stewardship practices. Metrics and monitoring of the privacy program should consider benchmarking, data collection, and implementation. This will support identifying measures to ensure agencies purge sensitive personal information methods with required schedules. Planning and coordination will start in 2019.

Recommendation 11

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.

Agency Response

Concurrence	**Partially concur**
Implementation date	06/29/2020
Responsible agency	**KCIT**
Comment	In alignment with Recommendation 10's comment, KCIT is in agreement. Technical evaluation will start July 2019 with supporting documentation and implementation targeted 2020. This work will be important in the effort to support Recommendation 10. At a minimum, all system administrators/ owners should identify which systems have the technical capablity to purge data. Gaps may be identified that require system replacement/ upgrade or other technical considerations that require additional resources or funding. All enterprise systems will have a plan to comply.

Recommendation 12

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.

Agency Response

Concurrence	**Concur**
Implementation date	06/29/2020
Responsible agency	KCIT
Comment	The policy update effort is to kick-off July 2019. Starting in August KCIT will partner with Council designees and stakeholders to identify a common definition of personally identified information, that aligns with industry best practices and federal privacy statutes, that is best for King County. Once the definition is identified, it will be established and communicated as part of the new policies' rollout, and the new privacy program launch in 2020. KCIT will use technology where appropriate to enforce policy.

Recommendation 13

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.

Agency Response

Concurrence	**Concur**
Implementation date	06/29/2020
Responsible agency	KCIT
Comment	KCIT agrees with the recommendation, as this is already on the KCIT Implementation Roadmap, and evaluation and identification of the location to host and manage this data inventory has begun. An initial location has been identified but may not be the best or most feasible long term solution. That will be better understood after further analysis and understanding of the manual and automated means planned to identify and update the data inventory.

Recommendation 14

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.

Agency Response

Concurrence	**Concur**
Implementation date	2021
Responsible agency	KCIT
Comment	Potential tools are currently being considered and evaluated. Depending on cost and budget availablity, full implementation may not be available for dissemination across all relevant database instances or made directly available to agencies. Regardless of the budgetry concerns, this is a priority effort to help identify and validate data collection and sources, as well as the ability to maintain an accurate inventory. Further planning and analysis is required to set a firm date.

Sheriff Response

King County

Dow Constantine
King County Executive
401 Fifth Avenue, Suite 800
Seattle, WA 98104-1818
206-263-9600 Fax 206-296-0194
TTY Relay: 711
www.kingcounty.gov

July 1, 2019

RECEIVED

JULY 1, 2019

KING COUNTY
AUDITOR'S OFFICE

Kymber Waltmunson
King County Auditor
Room 1033
COURTHOUSE

Dear Ms. Waltmunson:

Thank you for the opportunity to review and comment on the proposed final report "ICE Access to County Data Shows Privacy Program Gaps." I appreciate the work your office has done to ensure King County continues to make progress in extending the most rigorous privacy protections across all manner of electronic data.

We concur with the audit recommendations and appreciate the acknowledgement of our efforts to safeguard immigrant legal rights at a time when they are under constant assault by the Trump administration. For example, the Department of Adult and Juvenile Detention (DAJD) has not honored U.S. Immigration and Customs Enforcement (ICE) detainers without a judicial warrant since County code prohibited such practice in 2013. In addition, DAJD has not allowed ICE to access inmates, also consistent with County code.

Five days after receiving notice from the Auditor's Office that ICE was using the Jail Inmate Lookup System-Law Enforcement database to access confidential information of inmates including photograph, physical description and aliases, DAJD instructed King County Information Technology to deactivate all ICE accounts. It should be noted that we know of no circumstance where federal agents used this data to detain or remove county residents.

Effective June 4, in response to your report, DAJD stopped requesting information about the citizenship, immigration status or place of birth of anyone being booked into our facilities. DAJD is also now providing copies of each detainer received to the involved inmate in a timely manner. These changes are now incorporated into a DAJD policy which governs all DAJD related immigration issues. (Copy attached).

We concur with recommendations for a more robust privacy program throughout county government, and increased focus on training and regular monitoring to ensure all agencies comply with policies and legislation.

Recommendation 2

To comply with county code 2.15, the King County Sheriff's Office should develop, document, and implement a plan to ensure that it does not provide personal information to federal immigration authorities for civil immigration enforcement without a criminal warrant or legal requirement.

Agency Response

Concurrence	**Concur**
Implementation date	09/01/2019
Responsible agency	**KCSO**
Comment	We are currently revising our policy to ensure no personal information is released to federal immigration authorities for civil immigration enforcement without a criminal warrant or legal requirement. Until our policy is updated in our General Orders Manual (GOM) we have instituted an internal process where our legal team reviews any docments requested by federal immigration authorities prior to dissemination.

*Recommendations 1, 3-14 were sent to the County Executive.

Statement of Compliance, Scope, Objective & Methodology

Statement of Compliance with Government Auditing Standards

We conducted this performance audit in accordance with 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope of Work on Internal Controls

We assessed internal controls relevant to the audit objectives listed below. This included interviews and reviews of access logs related to nonpublic data access, review of information technology (IT) training logs, checking for compliance with records retention schedules, reviewing the county's application portfolio for the use of flags for various kinds of personally identifiable and/or sensitive information.

Scope

This performance audit evaluated the extent to which King County collects and protects personally identifiable information (PII) of county residents. We used the definition of PII provided in the National Institute for Standards and Technology (NIST) Guide to Protecting the Confidentiality of Personally Identifiable Information:

> Any information about an individual maintained by an agency, including 1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, and 2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[18]

This audit does not review compliance with the Public Records Act. Privacy concerns and compliance issues discussed in this report refer to county policy violations, not violations or personal information breaches under of state law. This audit looks at information held in county data systems; it does not review county data held by third parties.

Objectives

1. To what extent does the County adhere to best practices for collecting and protecting personally identifiable information?
2. To what extent are county agencies in compliance with KCC 2.15 regarding the protection of personally identifying citizenship information?

Methodology

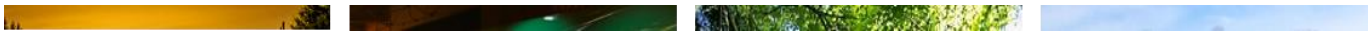
To understand the extent to which the County collects and protects PII, we reviewed county policies with the search terms privacy, PII, personal information, identity theft, immigrant status, and common public disclosure exemptions. We also interviewed county staff at the Department of Information Technology,

[18] SP 800-122 p 2-1

Department of Adult and Juvenile Detention (DAJD), Department of Community and Human Services, Department of Executive Services, King County District Court, King County Superior Court, King County Sheriff's Office, Office of Equity and Social Justice, Office of Risk Management and its Public Records Office, Public Health - Seattle & King County, Public Records Committee, and Records and Licensing Services. We compared our interview findings with county policies, NIST guidelines for protecting PII, and information from our interview with the City of Seattle's chief privacy officer.

Because the County does not currently have a comprehensive way of documenting its PII holdings, we reviewed data from Innotas, a management system for county-owned applications, to understand the extent to which county applications do or may contain PII. This determination was based on fields specifying data sensitivity as well as general descriptions of the applications' purposes. For select applications, we requested IT staff to provide us with data field lists and information on data management. We also conducted a review of the county's open data to look for data sets that included PII.

To check for unauthorized access to nonpublic data systems by federal immigration authorities, we reviewed access logs and data fields for select criminal justice applications. To determine compliance with county requirements to inform people when the DAJD receives a hold request from U.S. Immigrations and Customs Enforcement (ICE), we reviewed paper records of hold requests and notices from March and April 2019, the most recent months for which data was available. We chose the most recent months since that would have given DAJD the longest period of time to implement county policy that went into effect in March 2018. A small sample was also necessary because analyzing the paper forms involved time consuming data entry from two sources. As a result, we cannot project the findings to all hold requests on file with DAJD. We cataloged the date of the hold request and the person's date and time of booking into and release from the jail to determine if the person was in custody at the time DAJD received the request, whether DAJD informed the person of the request, and how much time DAJD would have had to inform the person given the time the request was faxed and the time the person was released from the jail.



List of Recommendations & Implementation Schedule

Recommendation 1

To comply with county code 2.15, the Department of Adult and Juvenile Detention should regularly monitor and manage access to nonpublic data systems to ensure that federal immigration authorities are not using them.

IMPLEMENTATION DATE: 4/16/2019

ESTIMATE OF IMPACT: By regularly monitoring and managing access to nonpublic data systems, the Department of Adult and Juvenile Detention can detect and stop unauthorized access.

Recommendation 2

To comply with county code 2.15, the King County Sheriff's Office should develop, document, and implement a plan to ensure that it does not provide personal information to federal immigration authorities for civil immigration enforcement without a criminal warrant or legal requirement.

IMPLEMENTATION DATE: 9/1/2019

ESTIMATE OF IMPACT: Verifying whether there is a criminal warrant or legal requirement can reduce the likelihood that the County uses resources to facilitate civil enforcement, while collaborating on criminal cases that endanger public safety.

Recommendation 3

To comply with county code 2.15, the Department of Adult and Juvenile Detention should provide people in custody with copies of any Immigration and Customs Enforcement detainer hold, notification, or transfer requests placed on them while in custody.

IMPLEMENTATION DATE: 5/3/2019

ESTIMATE OF IMPACT: Providing copies of these documents allows targeted individuals to have necessary information to pursue legal aid.

Recommendation 4

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.

IMPLEMENTATION DATE: 9/6/19
Implementation date provided by DAJD on 7/8/2019, subsequent to receipt of executive response.

ESTIMATE OF IMPACT: By tracking how long it takes to inform people of these requests, the County can ensure that it makes a reasonable effort to notify people with crucial information.

Recommendation 5

To comply with county code 2.15, the Department of Adult and Juvenile Detention should develop, document, and implement a plan to ensure that citizenship status and place of birth is not collected in its data systems.

IMPLEMENTATION DATE: 6/3/2019

ESTIMATE OF IMPACT: By reducing the amount of personal information it collects and stores in its data systems, the County can lower the negative potential harm caused by a data breach.

Recommendation 6

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.

IMPLEMENTATION DATE: 6/3/2019

ESTIMATE OF IMPACT: Providing informed consent reduces the likelihood that people will feel coerced to respond and may reduce the amount of sensitive information the County collects and stores.

Recommendation 7

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.

IMPLEMENTATION DATE: 11/1/2019

ESTIMATE OF IMPACT: A training plan will help ensure that all relevant agencies are prepared to carry out code revisions that directly affect county residents.

Recommendation 8

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.

IMPLEMENTATION DATE: 6/29/2020

ESTIMATE OF IMPACT: A unified program will provide the tools and accountability frameworks to develop concrete, consistent ways of protecting people's privacy.

Recommendation 9

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

IMPLEMENTATION DATE: 6/29/2020

ESTIMATE OF IMPACT: Collaboration will use existing expertise across county agencies to ensure that privacy protection tools are relevant and accessible.

Recommendation 10

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.

IMPLEMENTATION DATE: 6/29/2020

ESTIMATE OF IMPACT: By purging information at the end of its life cycle, the County can lower the negative potential harm caused by a data breach and reduce the cost of data storage.

Recommendation 11

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.

IMPLEMENTATION DATE: 6/29/2020

ESTIMATE OF IMPACT: The county can only benefit from purging information at the end of its life cycle if it has data systems that are able to do this without compromising data necessary for county operations.

Recommendation 12

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.

IMPLEMENTATION DATE: 6/29/2020

ESTIMATE OF IMPACT: A common definition will create a shared understanding of what information may need to be protected to ensure people's privacy.

Recommendation 13

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.

IMPLEMENTATION DATE: 6/29/2020

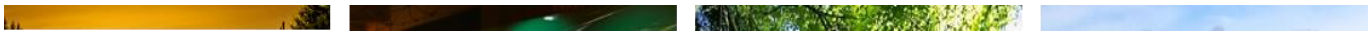
ESTIMATE OF IMPACT: Only by first identifying what personal information it collects, can the County properly protect people's privacy.

Recommendation 14

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.

IMPLEMENTATION DATE: 2021

ESTIMATE OF IMPACT: With relevant tools, county agencies can more efficiently and effectively identify sensitive information and take a risk-based approach to protecting privacy.



KING COUNTY AUDITOR'S OFFICE

Advancing Performance & Accountability

KYMBER WALTMUNSON, KING COUNTY AUDITOR

MISSION

Promote improved performance, accountability, and transparency in King County government through objective and independent audits and studies.

VALUES

INDEPENDENCE - CREDIBILITY - IMPACT

ABOUT US

The King County Auditor's Office was created by charter in 1969 as an independent agency within the legislative branch of county government. The office conducts oversight of county government through independent audits, capital projects oversight, and other studies. The results of this work are presented to the Metropolitan King County Council and are communicated to the King County Executive and the public. The King County Auditor's Office performs its work in accordance with Government Auditing Standards.

AUDIT

This audit product conforms to the GAGAS standards for independence, objectivity, and quality.