
From: Clerk of the Board
Sent: Monday, July 22, 2024 12:56 PM
To: Monica Nino; Enid Mendoza; Elizabeth Farrell
Cc: June McHuen
Subject: FW: Please take item C.151 Out of Consent Calendar and have discussion -- need more details of Thales Contract and what Mobile ID is -- There is potential privacy and civil rights issues related to mobileID so if and how it is implemented is important

The email below was received in the Clerk of the Board's office.

Stacey M. Boyd
Deputy Clerk
Clerk of the Board
1025 Escobar St., 1st Floor
Martinez, CA 94553
(925)655-2002 (Desk)
(925)655-2000 (Office)

From: Amada <>
Sent: Monday, July 22, 2024 12:16 PM
To: Supervisor John_Gioia <John_Gioia@bos.cccounty.us>; Supervisor Candace Andersen <SupervisorAndersen@bos.cccounty.us>; Supervisor_Burgis <Supervisor_Burgis@bos.cccounty.us>; Supervisor Carlson <supervisorcarlson@bos.cccounty.us>; Supervisor Federal Glover <DistrictFive@bos.cccounty.us>
Cc: Clerk of the Board <ClerkOfTheBoard@cob.cccounty.us>
Subject: Please take item C.151 Out of Consent Calendar and have discussion -- need more details of Thales Contract and what Mobile ID is -- There is potential privacy and civil rights issues related to mobileID so if and how it is implemented is important

Dear Contra Costa Board of Supervisors,

I respectfully ask you to take item C.151 out of the consent calendar for tomorrow July 23, 2024 Board of Supervisors meeting and delay a vote on this item to a future board meeting where it is an agenda item that is discussed prior to a vote. If you can not delay a vote, than I respectfully ask you to take out of the consent calendar and have a discussion where a lot more info is provided on what MobileID is -- has it already been implemented, what are the policies related to MobileID in Contra Costa County, is there any MOU with other departments (e.g. state, federal, local governments or business or other org groups), and what is the goals of mobile ID in Contra Costa County and are there any changes on the horizon as it relates to Mobile ID. I'm in particular concerned with the use of Mobile ID in item C.151 -- I think each of you need to learn more about Mobile ID as it relates to this contract and overall policies in Contra Costa County. I'd be curious as to any demographic information that has been tracked on the use of Mobile ID to date in Contra Costa County including where it was used (e.g. traffic stops, pedestrians, etc) and what the race/ethnicity of those tracked thru MobileID by the various types of stops. Another thing that is curious about this contract is that you are approving a contract that is as of Jan 1 2023, over 18 months ago! -- what is that about? What is really happening that didn't have this contract approved last year? Or is it being hidden to be approved thru consent calendar in the middle of the summer when there are a

huge number of consent items on the calendar... something seems off here... the optics don't look good. More details are needed on this as well.

Background - What is item C.151?:

Item C.151. is to "APPROVE and AUTHORIZE the Sheriff-Coroner, or designee, to execute a contract with Thales DIS USA, Inc., in an amount not to exceed \$652,374 for vendor maintenance and support for ID Unit systems for the period January 1, 2023 through June 30, 2025. (100% RAN Board)"

The details located here <https://contra-costa.legistar.com/LegislationDetail.aspx?ID=6790009&GUID=018AEE06-B09B-4A0F-8D59-6B509D3CDAF8&FullText=1>

"APPROVE and AUTHORIZE the Sheriff-Coroner, or designee, to execute a contract with Thales DIS USA, Inc., in an amount not to exceed \$652,374 for vendor maintenance and support for ID Unit systems for the Office of the Sheriff, such as LiveScan, Automated Fingerprint Identification System (AFIS) and Mobile ID, for the period January 1, 2023 through June 30, 2025.

BACKGROUND: The Office of the Sheriff utilizes numerous Thales DIS USA, Inc. hardware, software and services to meet the biometric needs of the County. The RAN Board annually reviews and forecasts all budgetary and strategic decisions and these costs have already been approved. The systems include:

- LiveScan: Terminals that allow Law Enforcement agencies to fingerprint applicants, detainees, arrestees, registrants and deceased individuals for electronic submission to the Automated Fingerprint Identification System (AFIS).
- AFIS: Facilitates the statewide telecommunications network dedicated to the transmission of fingerprint data throughout the state for use of identification by law enforcement agencies.
- Mobile ID: A connection that allows law enforcement agencies to share information through a mobile device with the ability to rapidly search through DOJ's statewide criminal record repository for wanted persons and other persons of special interest. This system helps reduce terrorist and criminal activities by improving and expanding biometric services to Contra Costa.

The department is requesting approval of this retroactive contract due to the delay from uncertainty of how the contractor wanted to proceed with the renewals. Despite the delay in payment, Thales DIS USA, Inc. continues to provide services in good faith and the department wishes to continue working with this vendor through the requested contract term end date."

**

Please note -- I'm concerned on how Mobile ID has been or will be implemented in Contra Costa County. I would like you as well as the community to have more details before you vote on whether to give a contract to Thales DIS USA, Inc.

Please read more here:

<https://www.aclu.org/wp-content/uploads/publications/20210913-digitallicense.pdf>

Excerpts from this ACLU report on what digital driver's licenses could mean for privacy, equity and freedom report:

- "By making it more convenient to show ID and thus easier to ask for it, mDLs will inevitably make demands for ID more frequent in American life. They may also lead to the routine use of automated or "robot" ID checks carried out not by humans but by machines. Depending on how a

digital ID is designed, it could also allow centralized tracking of all ID checks, and raise other privacy issues."

- "Potential Threats to Privacy:

1. **POLICE ACCESS TO PEOPLE'S PHONES:** The most immediate and obvious danger of transferring our driver's licenses from physical plastic cards to our phones would arise if we were required to hand our phones over to a police officer. That would be a total nonstarter for any mDL system given how much personal information our phones hold.Despite a crystal-clear Supreme Court requirement that police obtain a warrant for smartphone searches, questionable "consent-based" police searches of people's cell phones happen thousands of times a day. A police officer's request—"mind if I look at your phone?"—may make a search "voluntary" in the eyes of the law, but few searches based on such police requests are truly voluntary. That is especially true for members of poor and marginalized communities. And while people may think an officer is just planning to flip quickly through their phone, many are surprised when an officer then walks away with it. When your phone is taken from you—especially if it's taken out of your sight—you have no idea what is being done with it. An officer may have indeed just looked through it, but they may also have used forensic tools—which have become widespread within law enforcement—to copy the phone's entire contents. If your cellphone is taken, police could even install spyware or make other changes to it."
2. **CENTRALIZED ID TRACKING:** Another significant question about a digital identity system is whether it would make centralized tracking possible. When someone visually inspects your plastic driver's license, no record of that inspection is automatically generated, retained, or shared with the DMV. But with a shift from plastic to digital identities, such tracking becomes possible. No system of electronic identity that permits that kind of tracking should be supported..... For mDLs, such tracking would mean the DMV would learn that "police officer X checked driver's license holder Z's ID on this date at this time." Having information on police traffic stops flowing to the DMV may not seem like an enormous invasion of privacy, but remember that driver's licenses have become all-purpose identity documents in American life. This means that tomorrow, information could be gathered by DMVs about every bar, club, casino, office lobby, bank, pharmacy, doctor's office, and airport that you visit; every convenience store beer purchase, equipment rental, or hotel check-in; any applications for social services; and any other circumstance in which you may be asked to show an ID.... In addition, if the police in your town have a memorandum of understanding (MOU) with your state's DMV—and almost all of them do—that could give the police access to whatever the DMV can see. Where a DMV chooses to outsource its verification functions, that data might also flow to private contractors—companies that would have a constant incentive to make money off our personal information. DMVs themselves have long sold access to personal information as a revenue source."

- "Potential Harmful Consequences of Digital Driver's Licenses "There are potential longer-term consequences and evolutionary paths that digital identities might take that would hurt privacy and other civil liberties interests in significant ways.

Thank you for looking into more, please do not approve this line item under the consent calendar. More discussion and details are needed.

A concerned parent living and working in Contra Costa County for the past 10+ years.