MACHINE TRANSCRIPT · CORAGGIO CONSULTING

# Fairfax County Board of Supervisors IT Committee, Tuesday, February 28, 2023

| | |
|---|---|
| Date | Tuesday, February 28, 2023 |
| Place | Fairfax County Board of Supervisors, Virginia |
| Length | 1h 38m (video) |

- Official meeting video (Fairfax County): https://video.fairfaxcounty.gov/player/clip/2766
- Official Board of Supervisors page (Fairfax County): https://www.fairfaxcounty.gov/boardofsupervisors/

> Machine transcript (speech-to-text) produced by Coraggio Consulting. Not an official county record. Names and numbers may be misspelled; check the video at the timestamp before quoting.

Speech-to-text: whisper.cpp, model large-v3-turbo. Produced 2026-11-04. Each paragraph starts with its time [HH:MM:SS] in the meeting video.

**[00:00:04]** Order, and now that I have my mic on, I'll call the committee meeting to order. Welcome, everybody. We have a couple of items on the agenda today. Hopefully, everyone has the slides. And the first one relating to mobile applications and data protection.

**[00:00:22]** I'll turn it over to Mr. Scott. Welcome. Good morning, members of the board and Chairman Alcorn and Chairman of the board, Mr. McKay. We want to talk to you a little bit this morning about mobile applications. I know there's been a lot in the news. Two months ago, there was something in the news about an application being used by a member of Fairfax County Government, and we want to address that and tell you what we're doing and how we're protecting our county when it comes to mobile applications.

**[00:00:52]** So this morning, I'm joined by two individuals who will do some speaking, and I'll let my staff here introduce themselves. Nate Wendland, Deputy to Greg in DIT. Charlie Gore, IT Security Program Director. Mike Dent.

**[00:01:11]** Michael Dent, Chief Information Security Officer. Okay, and so I'm going to hand it over to Nate and Charlie to take us through this presentation. Please stop us if you have questions. Let's make this very interactive, and we'll try to address any concerns you have around this topic.

[00:01:31] Go ahead, Nate. All right, thanks, Greg. So we're going to go through this presentation, and it's on the screen right now. So we're going to -- is that advancing? Kim, can you advance it to the next slide? All right.

[00:01:47] We're going to go into a few different things and areas in the mobile apps. We're going to start with the current state. We're going to break down the current state in the multiple areas, the device, the apps, and the data. It's very important we talk about each one of those layers as we walk through.

[00:02:04] So I'm going to start off and transition to Charlie to really lead off this slide on our current state. Good morning. As Nate mentioned, you know, we're going to be talking about mobile devices today, but I would like to start off just talking a little bit about our IT landscape as well as our cybersecurity attack surface overall, and then we'll lead into some of the ways that we protect the data and the systems across the county, regardless of the data type or the system type that we're using at this county.

[00:02:33] So, the county has over 200 physical locations supported by DIT in different manners, supporting over 60 different departments, all with unique missions, partners, and information technology tools to support their individual businesses. There are varying regulatory requirements governing data compliance in these departments.

[00:02:50] The county has EPHI governed by HIPAA. We have CJIS information, criminal justice information, credit card information governed by PCI DSS, as well as just general PII across the board, financial account records, personnel data, court, and law enforcement records.

[00:03:08] In support of these county departments, DIT maintains over 23,000 user accounts across the board. Some of those are unique accounts to individuals here at the county. Some are service and system accounts that support applications for different business divisions. Many of these unique users have a wide variance of technical expertise and familiarity with IT in general, as well as cybersecurity and the risk. If you think about some of the workforce overall, you know, we have a lot of flex throughout the year related to seasonal workers, volunteers supporting different missions, whether it's an election, whether it's working at a golf

[00:03:47] course, whether it's supporting the vaccinations. On our internal network, there are over 30,000 estimated network devices. This also fluctuates, you know, throughout the year, depending on the activities going on at the county these are on-premise systems cloud systems running different multiple operating systems different software versions we also have industrial control and operational technology so surveillance cameras we have HVAC systems we have fleets of vehicles that are internet connected supporting public transit supporting the ambulances and fire trucks and police cars out there all these are using different types of

[00:04:24] software different type of operating systems different types of hardware and And all of these systems have their own unique risks and threats that are applicable to those systems. We also have direct connections with other local jurisdictions for regional initiatives, connections to the Commonwealth of Virginia networks, connections with major cloud service providers, as well as many other vendors that support the county in some way, whether it's through a business or whether it's through an information technology service or product.

[00:04:57] Okay. So as the first slide states here, you know, we mentioned 5,000-plus mobile devices. This is just one major platform that's in use here at the county. You know, there are different types, flavors of

mobile devices all across the county. We've got Apple devices. We've got Microsoft Windows mobile devices.

[00:05:14] We have Android devices. All of these, again, come with their own unique risks and components that need to be managed and have a supporting management platform behind that to be able to mitigate the risks associated with those platforms and manage the data that those systems are processing.

[00:05:33] So one of the security and privacy principles we use to approach this wide attack surface is based off the concept of zero trust. Zero trust is an approach where we require all users and devices, whether they're inside or outside our organization's network, whether it's a smartphone, a PC, a tablet, or another type of device, to be authenticated, authorized, and continuously validated, so the security posture validated on those devices, before they are granted or can retain access to the applications and data that the county supports.

[00:06:06] The Zero Trust Framework is an evolution of the idea of least privilege, which is a term that's been in the cybersecurity community for years, as well as, I think, defense and intel, limiting access to systems and data based on a need to know and a need to have only. So not only is it a security concept, but what comes along with some of the technologies that have come out is a suite of capabilities that can better help support remote access and mobility security to allow more flexibility to the workforce overall.

[00:06:35] So we approach this concept of zero trust for all devices to include mobile devices and smartphones and tablets for a combination of technical and procedural processes, which are outlined in Procedural Memorandum 705. That's the county's IT security policy. PM 705 establishes a minimum baseline for the county for cybersecurity program, administrative, and technical controls to implement it across all county departments and apply it to all device platforms, so not limited just to certain types of PCs or whether it's a smartphone, a tablet, a PC, a surveillance camera.

[00:07:11] All the controls that are in the security policy are relevant to those platforms. Several of the critical areas of our cybersecurity strategy include implementing data loss prevention techniques, centrally managing systems, these mobile devices with the platforms that are capable of doing that.

[00:07:31] For example, a mobile device management platform that can manage iOS device, Apple devices, or Android devices and things like that, as well as the Active Directory infrastructure that supports Windows, computers, and servers. Other things that we do are related to continuous monitoring of all system and user activity across the board that may be indicative of a potential data breach or some sort of cybersecurity event.

[00:07:57] We use various platforms for monitoring device and user activity. We also do continuous attack surface testing, which is taking a look at our external perimeter to see potential exposed vulnerabilities on systems that citizens may be used or that the county may be using to access internal resources.

[00:08:15] We do something called penetration testing, which is simulation of a hacking event to see what type of data could be exposed, what systems could be compromised. And we're continuously doing vulnerability and risk management activities across the board.

[00:08:30] And again, this is on all platforms, mobile devices, Windows computers, all the systems that are on our enterprise overall. Charles, before you go on to the next slide, so the 5,000-plus mobile devices, these are all county-owned. County-owned, that's correct.

[00:08:46] That's correct. We're not talking about devices people would bring that are their personal. Yes, these are all county-owned, county-managed devices. All right, thank you. So lastly, before we go to the next slide, I did want to talk a little bit more about data loss prevention. Data loss prevention is a set of tools and processes used to ensure that sensitive data not lost, misused, or accessed by unauthorized users.

[00:09:09] We use various tools in our enterprise to discover, detect, and monitor for the possible exfiltration of regulated data types, specifically HIPAA, PCI DSS, and PII, such as social security numbers and date of birth, and the things Virginia Code typically identifies as PII.

[00:09:25] And these data loss prevention techniques are both at the device level and application level. The first of which we're going to discuss is the overall device security controls on our county-owned managed devices. Next slide, Kim. So there are many different components of a data loss prevention program. One of the first steps is to secure the device itself. Just like your standard county Windows computers, DIT centrally manages smartphones and tablets using a mobile device management platform and applies security controls centrally to all those devices consistently. The platform allows us to

[00:10:02] plot controls in various different ways, but probably the most visible ways that you see these controls in place would be enabling multi-factor authentication, requiring a PIN code for that device, initiating a screen lock on that device after a period of inactivity on that device. So if it's lost or stolen, no one's going to be able to get into that device if that inactivity threshold is met. We can wipe a device remotely. A device will be wiped after a certain amount of incorrect password attempts.

[00:10:38] We've used Mobile Device Managed as well for some things like certificate-based authentication, which is basically giving that device a key that's unique to that device to be able to talk to another system, so it helps us prove the integrity and the trust of that device. We can push software and different versions of software up to the devices that are managed by the county.

[00:10:59] That includes, you know, mandatory security updates where those devices might have a risk, whether it's something related to a SMS phishing message or something like that that could compromise the device. We're also implementing policies on these devices that restrict the different applications running on those devices to be able to share or have excessive permissions over that device, like does an app really need your location at all times?

[00:11:25] Does an app need access to your camera? All the different capabilities across these iOS devices, we can control those policies. Through this mobile device management platform and last we also have a mobile device security product that takes a look at That runs on each device that takes a look for potentially malicious apps, you know based on Signatures associated with known malicious apps that are out in the community next slide So before I hand this back to Nate to talk a little bit more about application management I wanted to touch very quick on data loss prevention techniques at the application level as I mentioned

[00:12:03] And we use various tools to discover and protect different data types across these devices. The most common way that we've implemented application data loss prevention techniques is in the Microsoft Office Suite. So you have Microsoft Outlook, you have OneDrive, SharePoint, Teams, which are also the most common apps on county devices because they're our main enterprise platforms.

[00:12:25] But we've applied application-level policies. These application-level policies can also apply to a non-county managed device. So if someone downloads the Outlook app or the Teams app and they access it on a personal device, the application-level policies will apply there.

[00:12:41] And so another way that this is most visible is through things like MFA. You have to use MFA to be able to access that enterprise resource. We also have policies that force encryption of data that is being sent outbound to partners or other mail domains outside of our network if sensitive data is detected.

[00:13:03] And lastly, we can prevent -- within those apps, we have controls that can prevent data from being copied, downloaded, transmitted, or shared to other applications, including screenshots and things like that of data that might be considered regulated, right? So, I'm going to talk about the next layer when we actually discuss apps.

[00:13:26] The next two layers are really apps and data. We talked about the device layer as one of those things that we are protecting. As we get into the app layer, we really get into the aspect of sort of managing and controlling our own app store, call it a corporate app store.

[00:13:42] We actually allow or we don't allow apps to be either be downloaded or installed on devices. Typically we use these three phrases, blacklisting, whitelisting, and graylisting. Blacklisting is what it really does is it prevents an app to be used or blocks an app from being used on a device.

[00:14:04] It prevents access to it, install of it, or even use of it on any county-managed devices. Whitelisting is allowing that device. There's a business justification around that app to use it. As Charlie mentioned earlier, things like, obviously, Microsoft Teams, the Microsoft Suite, those are like whitelisted apps that we have to allow people to use.

[00:14:27] And then we have also graylisting. And people may not have heard graylisting before, But what it is, it's in the process of becoming either blacklisting or whitelisted on an app. It's sometimes under, we would call under a review process where either DIT or somebody is, any individual agency is reviewing that app to be able to use it for business justification.

[00:14:50] So those are really the three major categories that we have during that process. I'll talk a little bit more about the process later of what we're looking to implement. But holistically, what it allows us to do is manage those apps on those devices.

[00:15:06] As we see this over time, there's around 2,500 apps that are deployed to the Apple App Store every day. There's over 3,000 per day on the Android. For us to be able to keep up with the quantity of those apps on a consistent basis and know where they're at, we have to continually monitor those, manage those, and have to have a process in place to say, this can be used this cannot be used.

[00:15:31] We have also referenced and looked at things from NIST, DOD, DHS. They've looked through these processes as well, how they've actually managed this and how they're looking to manage these over time. We also are very aware that apps are used on a consistent basis for business use.

[00:15:49] And they will be over time as we advance applications. We make them more accessible in the field. make them more available not only to possibly residents but also to to the business units and what they do and how they access data so apps are going to be something that's going to be consistent just how do we manage that how do we control that for that entire process we also have a way of blocking apps as

well through the mobile device management we can actually block them if they become compromise or something does happen we're able to sort of very quickly and

[00:16:26] efficiently go through and block those apps through devices that we manage as we've heard multiple times over the years things do happen on you know with apps or with platforms so our ability to react quickly is sort of essential to that entire process so we'll move on now to the third stage and the third layer which is really data. As we talked about, we get more granular on what is accessible and what is controlled on each one of these layers. On the data management or the content management layer,

[00:17:05] we really are talking a lot about what can be reviewed, what can be edited, and what can be shared on that individual layer. As Charlie mentioned, we have thousands and thousands of ways to access data it's not just through mobile apps you can be on a mobile device and access data through a web interface not just through the app so we have to look at controlling the data and how that data is accessible not just through apps but through any interface that we have that's why data management content management is so critical and we have to have those securities

[00:17:44] and policies in place to allow for that process to prevent that data loss or that download or unauthorized use of that data.

[00:17:59] There's also ways that we can do automated content management where we can either restrict or pull back data. There's ways to be able to update that data, which we do consistently when someone updates a document on their mobile device, it automatically synchronizes that to, you know, a Windows device or someplace else or through a web interface.

[00:18:19] So, all of those things to centralize that data management and that content management is essential. Having multiple areas to have that data creates the possibilities of data loss, so centralizing that is essential for us to control and manage that data.

[00:18:36] So there'll be times when we talk to agencies that are external with Fairfax County wanting to access specific data. That's why we try to make sure we manage that data externally and keep it within our controlled environment, because as that data, if we allow that data to get out, we can't control the data beyond our threshold of capabilities of what we can manage.

[00:19:02] And just to add a point to what Nate's talking about is that, you know, we're doing a lot more with our cloud vendors and stuff like that. And so what we do as an architecture review board as part of our IT committee is to really look into that and understand how that data is being really replicated and protected in the cloud. And we've actually turned down applications from the business unit because the data was not going to be as protective as we wanted, you know, to make sure that we protect our own data. So that's another phase that we go through as we look at these applications. Mr. Scott, if I could just jump in there. But it doesn't mean we never

[00:19:39] include any data in the cloud. No, no, no. Right. We make sure that security. Right. We make sure that that main component around that data and how that data is secure is what we really care about. Thank you. It's actually a good transition to zero trust data access. So as Charlie mentioned, we do talk about zero trust, but this is also a portion of that is zero trust data access. This is something, as you mentioned as well, that this has been, this is not new. This is making it and putting a posture for how our data is accessed and who accesses it. And also understanding that

[00:20:17] we just don't inherently trust that someone will do the right thing with our data and just trust them that they are going to control it and manage it the proper way. So that zero trust access all the way through MFA multi-factor authentication and other things to gain access to that data is part of that essential key as we move forward.

[00:20:39] I mean, all these security controls come back to, you know, ensuring privacy and being part of the overall data life cycle. So the focus here on device management and the applications that are being used overall is tied also back to our ability to adequately inventory and know where our data sources are whether they're you know it's a public record or whether it's it's a centralized repository that has the security controls that are necessary for auditing and and different things and retaining

[00:21:12] data long term so so ultimately the security controls are tied back to uh maintaining control over the data and the sources that that data and a man in a way that would be compliant with overall data government's capabilities all right moving on to the next slide which is the future state. So as we mentioned, there are consistently things that we have to look at on this frontier to make sure that we are protected as a county. Obviously, there will be future apps that will

[00:21:47] need to be allowed for business requests or for things that either an agency or a process needs for that app. Mobile devices will continually increase over time. That is something that we have to anticipate for, but creating a process for us to allow that and for us to then evaluate those apps and evaluate and make sure we categorize and track those apps that we have allowed is essential for us to maintain that security posture so that that way we know that we are

[00:22:23] protected, our data is protected, our device is protected, and the apps are protected, so that that way as we move forwards, we're not putting ourselves in a compromised situation. We also want to look at reporting and dashboards for agencies so they are aware of what apps are out there that their agencies are using. Tracking what apps are in each individual area or each individual agency is also essential for them because as they transition from certain business processes, they may want to say, listen, we don't need that app anymore.

[00:22:59] Let's go ahead and we're going to consolidate or maybe migrate to another platform, as well as making sure that they are fully aware of notifications that we get in DIT of concerns around apps. As we mentioned earlier, we're reaching out and watching what is happening with NIST, DHS and DOD. This is something that if you've seen a lot of papers and other things in the past year, especially after the pandemic and after the mobile workforce expanded over time, these are a lot of research papers that they've been doing as well of how do we make sure that the data is accessible

[00:23:39] and we have that mobile workforce, but at the same time it is secure. So those are things that we're watching as they submit and publish papers. And as they do different things, we're watching their posture to see if that's something that we should adjust to ours as we move forward.

[00:23:59] And one last thing before I transition over to Charlie is that when we talk about notifications to agencies, there's a reaction point in DIT where we have to react and then notify, especially if it's critical from a security perspective.

[00:24:17] So as this app future and this data access changes, if there is a concern over data access or a platform, we may have to shut it off, notify the agency, and then figure out a way to get access to that data or mitigate that.

[00:24:35] So those are some things that we have to sort of look at from our notification perspective as well. Lastly, I just want to comment that every year we go through our security policies and we take a look to see what types of modifications or changes as the technology is evolving, as our landscape is evolving, as the threats change.

[00:24:58] We're also taking a look at the federal level, what NIST is providing, what type of guidance they're providing, the Center for Internet Security. We're taking a look at the developments with the Commonwealth of Virginia, new bills, new statutes, such as the cyber incident reporting bill that passed last July.

[00:25:18] And overall, we're taking a look at just everything that's going on in the community, the industry, and just seeing where the trends and the new best practices that are coming along and trying to take advantage of all those things. So, you know, as the attack surface changes, we're evolving with those changes as well.

[00:25:36] And that is it for the slide deck. Thank you very much. I just have one question and see if anyone else has questions. So not every county employee gets a mobile device.

[00:25:52] Not every county employee needs a mobile device. My question is, particularly for county employees that don't have mobile devices but from time to time need to do things outside of county, out of their work environment, do we allow that sort of access through people's personal device?

[00:26:11] And the reason I'm asking, you know, a lot of employers are moving towards bring-your-own-device strategies. Is that in any way compatible with our systems? You can access the county's portal, web portal, through your personal device, but that is going to require you to still sign in, use multi-factor.

[00:26:35] The only difference is there's nothing you can do that is going to allow that data to be transferred over to that personal phone. So we put the line at the data? Yes. So basically. Exactly. Okay. Very good. All right. I think part of that, too, is that's why we have those multiple tiers.

[00:26:52] So we have that control to the device, control to the app, and then control to that data as we move forwards. Very good. All right. Thank you. Mr. Chairman. Yeah, just, I think, a simple question. I mean, obviously, what the federal government is doing is constantly looking at these apps, and some have been in the news lately.

[00:27:09] So I guess my question is, if the federal government bans apps on their government-issued devices, what would be the reason why we wouldn't automatically replicate that? Actually, we're very proactive with that as we see what the federals are banning.

[00:27:29] We actually go back in and look at that and ban it from our side. A lot of what the federal is banning is because it opens up for exploitation, and that's why they're banning that. So we as a local government, we should be looking and following suit as well.

[00:27:44] So a lot of times we're following what they're banning. I know today in the news you probably heard about TikTok and being banned and all that. Well, that was one of the ones that was already on our black list. So we're kind of staying right there with them and trying to be there in the game as well.

[00:28:03] If I can, Supervisor McKenna, we also probably have, we banned those apps that they're banning now. We banned them before they did. Okay, good. Exactly what I wanted to hear. Thank you. I

also want to add one thing to it is that some of the apps, obviously, that we use in Fairfax County are not used in the federal government.

[00:28:22] So, I mean, there are alignments of sort of blocking apps, but there's also going to be apps that we are going to allow that we are using from a business process perspective. that may not be allowed at the federal government level. Not necessarily that they would block it.

[00:28:39] It's just they're not using it for their business process. Got it. All right. Thank you. Let's start down here and move down. Supervisor Herity. Let me start by thanking you because we were in front of the federal government even on TikTok. I mean, I've got a security clearance, so I knew about that a long time ago.

[00:28:58] Where are we on Signal, which is another one that's been kind of in the news lately? Signal is blocked. Okay. Has been blocked. Okay. All right. And mobile is a challenge, and there is a movement towards BYOD, bring your own device.

[00:29:16] And how many people do we currently have on mobile device management software using their personal devices? Or do we have that? For personal devices, we cannot use mobile device management for them. Okay.

[00:29:32] So we end up blocking on our side of the firewall for those devices coming in. So they've just got to go through the portal and get what they can get there, And you block all data going down. Exactly. So we're not using MDMs on personal devices right now? No, sir. Okay. And, Supervisor Herity, can I just say, with the Signal app, we block on our end, but if it's being forwarded to a personal phone, like Mike was saying, we don't have the purview to be able to deal with that.

[00:29:59] Yep. No, I understand. Personal devices, we can't, unless you've got an MDM on it with their approval and then you've got control over their phone and you can wipe it and do all those things, which, again, some companies have gone that route, but there's some serious issues with that as well.

[00:30:17] Kind of on the other side of it, you know, I've heard from some agencies that have wanted to use things like LinkedIn and that sort of thing for recruiting. How do we handle that? Is that just the app's got to go through the process?

[00:30:33] Can we give it to some people and not other people? And how has that been going again? And this information's a little dated, but I know some of the recruiters were trying to get a hold of LinkedIn and weren't able to. So how are we going to, and I'm going to sort of separate LinkedIn and put it to an entire process to make it a little bit more simplistic, is that we're looking at all apps to have just business justification around using that app or that platform.

[00:31:02] And then we would monitor that platform or that app over time to make sure that it is in compliance with the ever-changing environment of security or data retention or anything else. So those are really what we're trying to sort of focus on is making sure that it's either there's a business justification around it and that app is in compliance.

[00:31:25] And LinkedIn is one of those that would probably follow in that review process as long as there's justification to use it across the board. And I'll let you finish, and then I'll follow. And the other thing is we're looking at some of those types of apps that the federal government has already put in sort of like their white list category.

[00:31:44] Yeah. And so we just want to do our due diligence before we put it there. But certain apps will be in that. And LinkedIn is probably one that we'll be looking at and be putting in that list. And I'm sorry, but LinkedIn is not blocked. So if there's someone that cannot get to LinkedIn, that's a problem that I should know about.

[00:32:03] And I don't know how recent that is, but is that a change that's been within the last year? No, we've never blocked LinkedIn. Okay, good. And I'm more, the other one that I had heard about, the other COTS solution out there was Cvent or Eventbrite, those kinds of, are those on whitelist, blacklist?

[00:32:24] are they not not not sure supervisor but i will definitely take a look at that it shouldn't be i mean park authority was trying to do something back during the pandemic where they were trying to use a cot solution instead of waiting for an internal kind of solution i just it's it's that ever balance between being nimble and using cot solutions and being protected yes sir it's that's why we hope the process you guys have a tough job the process we've defined is is probably very mainstream and very easy for our agencies to use. And I don't look at it being a delay.

[00:32:57] Previously, it probably has been a delay because we've tried to take a little bit more time. And now, again, going with the federal government's model of what they've whitelisted and what we see them using, if it's business-related, there's going to have to be a hard fight against why we shouldn't allow them to use it. And all my questions are a little dated. I will revisit with that. So I appreciate, again, I appreciate the balance for one and the job you're doing for two, but at the same time we've got to do everything we can to be as efficient as we can. We'll double check, but I think Eventbrite did go through our review board and it's allowed, so we'll just

[00:33:34] double check. Thank you. I have a question about the forced passcode password expiration. You mentioned NEST, and so for people that don't know, the National Institute for Standards and technology. And so when they were originally published in 2017 and updated in 2020, they don't recommend having people update their passwords. I have to read this because I never heard this term before. Verifiers should not require memorized secrets to be changed arbitrarily, for example, periodically. However, verifiers shall force a change if there is evidence of compromise of

[00:34:13] the authenticator. So just reading that and reading about, you know, when people know their password is going to change every three months, they're not going to have a good password. So I guess I'm wondering why we're still doing that process. That's the first I've heard that being said. I mean, I haven't looked at that in quite some time then, I guess, because I will take it back and review that. Okay. And I just want to make sure that that is exactly what they're recommending. So it is in SP 800-63B. Okay. I'm familiar with this. So what they've started

[00:34:51] to recommend is passphrases instead of a, you know, a 6 to 10 character. What they want is basically a many sentence to be your password, and it would be less likely to be cracked using tools that can decrypt, and because most people use common passwords.

[00:35:12] Right, and change one letter. So the recommendations now are that you have a longer set of characters as a passphrase. that's something unique to you, and you wouldn't have to change your password as frequently because it would be less likely to have a dictionary tool that could crack that password.

[00:35:35] So if we set in policies that increase the character length required for passwords, there's some integration challenges with other systems as well. We have a lot of legacy systems here at the county.

[00:35:52] So there's, while that is a recommendation, there's also limitations on how that longer passphrase could work for systems that may not support it. But we hear, and I'd actually love to do that, and the benefit to the password change is that passwords are compromised all the time.

[00:36:10] People use the same passwords across many different systems that are non-county, and when those things are compromised, if we have a three-month time frame and the hack happened six months ago, we're in a much better position rather than forcing password resets for everybody.

[00:36:27] I guess, you know, the other hand, I wonder, you know, how much time are we spending when people forget their password or can't get into their password? Kim's smiling right now as I'm talking. And so it's also that resource issue, right? And so when I read these recommendations, they've been around for a while. My password's pretty long, I have to tell you. I just personally think it's something we should look at because I think it makes all our employees' lives easier.

[00:36:53] It saves staff time. Thank you. Thank you. Longer passwords assume good typing, too. And that's well noted. When I get into talking about strategy, we'll talk a little bit about what we're looking for in the future when it comes to security and passwords.

[00:37:10] Thank you. Any other questions? Supervisualize. Thank you, Mr. Chairman. Just a quick question for Charles and then a comment. So I noted that when you were talking, you mentioned that we are looking for best practices in data management and also in mobile applications.

[00:37:31] And you also mentioned that we're working with emerging technologies. Could you kind of tell me how you're doing that specifically? So I have a great, great team. Yep. It's still on. It's still on. We have a great team that's constantly looking at the various products and services that are coming.

[00:37:49] We attend events frequently and analyzing the vendors and their services that are available. We are, you know, always reading blogs, always reading, leveraging our partners and hearing about the new capabilities that exist out there.

[00:38:09] I mean, I think that's probably one of the strengths of our team is our ability to do that. But in terms of the types of taking advantage of some of the services that exist now, you know, I talked about continuous attack service testing, right? The most common thing right now, or at least historically, has been using something with penetration testing for something that's a point-in-time test, compliance checkbox-type service.

[00:38:33] What we've moved towards is something called continuous testing, where a team is behind that that is taking a look at our attack service on a reoccurring basis so that they can identify issues outside of that single point-in-time test. Another thing that we're in the process of having implemented here at the county is something called managed defense.

[00:38:56] We're going to be using one of the major incident response providers to provide some additional supplemental monitoring of our endpoints. And I would like to thank you all on this one because we're using some ARPA and CARES funding to help achieve some of these things. And we very much appreciate these opportunities for this stuff because ultimately these types of services that we're

looking to supplement our in-person staff is adding a major enhancement to our cybersecurity capabilities across the board.

**[00:39:24]** But overall, we're taking a look at where the industry is going and how we can adjust and be nimble. That's great. Supervisor Lusk, we'd be happy to talk to you. Yes. More detail if you want, one-on-one, but we don't want to go into too many. I'm not asking you to give up any trade secrets here, so obviously.

**[00:39:43]** But we can comment on publicly. This is perfect, so I appreciate that. Can I ask a follow-up to that? Are we able to work with local companies here in Fairfax County? Do we have opportunities to support those that are growing here in this market? Absolutely.

**[00:40:00]** You know, contract vehicles and RFP solicitations and things like that are absolutely how we'd acquire services. But Mike and I, on a reoccurring basis, meet with many different people, including local technology companies, to hear about their services.

**[00:40:17]** Okay. Absolutely love that. And then the last thing I'll do is just offer my acknowledgement of the great work you do in protecting our systems. We don't have breaches. We don't have these attacks that are being publicized in the newspapers. But no, no.

**[00:40:34]** Hey, hey, I want to be clear in saying that you're doing great work. This is obvious, I mean, because we see differences in other locations. So, yes, knock on wood, but you're doing something right to make sure that this is not happening. So I just want to say that publicly.

**[00:40:50]** Thank you. Thank you. All right. Supervisor Gross, and then we'll move on to the presentation. Thank you. Looking at security and the kinds of phishing and so forth that we might get. Right now on my iPad, I have a notice from my iCloud storage is almost full, and I'm thinking, huh?

**[00:41:12]** And it says, you know, you have so much remaining and you can upgrade for only 99 cents a month. Now, I presume that this is probably not phishing, but it's not something from the county. You're not telling me that my iCloud storage is full.

**[00:41:29]** If that's a legitimate email, it's from Apple. It does say something about it's a service provided by Apple. So this is just a sales pitch. basically and it's it's definitely not us we wouldn't be doing that i wouldn't think so no but this in then penny we would have to show you how to hover over that address to make sure it's really from apple and it doesn't just say apple there and makes because there are ways that you can check that email to make sure it's really from apple so i'll just i can delete it and then call you and ask you about my iCloud storage yes ma'am okay there's an awful lot gets deleted and

**[00:42:08]** it needs to get deleted but um i guess that's part of our our hygiene for our uh devices is to make sure that we clear it out every once in a while every actually i guess every evening maybe is the case all right gross we're going to sink we're going to sink kim and we're going to take it's very good it's it's very good to get in the practice of at least taking some time every other day to go through your email and make sure that uh you go through and keep the ones that are illegitimate, delete the one. If you're not sure of it, get rid of it. Oh, there are hundreds,

**[00:42:41]** hundreds a day that you get. Yes, we get thousands. I'm sure you do. All right, thank you. Fully compliant with our Freedom of Information Act. It's the security piece that I'm always concerned about. Are these phishing or are these legit? So, and I've learned a lot from you, Mike. Thank you.

[00:43:00] You're welcome. All right, very good. Thank you. Very, thank you. Excellent presentation, a good discussion, and thank you again for everything you're doing to keep us safe. I appreciate that. Let's move on now. We do have a presentation on the IT strategy for the next few years.

[00:43:19] Mr. Scott, turn it back over to you. Good morning. What we wanted to do is to talk about our strategy. I know I was in front of you probably about two years ago talking about a three-year strategy roadmap. Well, right now we're moving into a new roadmap, and so what I would like to do is set this up, tell you a story, and then how we're moving forth with our overall IT strategy.

[00:43:43] So, as you can see on the first slide, we have these three categories, reactive, proactive, and innovative. And if we look at reactive, that was during the time of the pandemic. We were very reactive. We actually completed a lot of our digital transformation strategies within that first few months of that.

[00:44:03] We became a more agile IT shop, responding to the needs of our customers and to keep business flowing for our citizens. And we learned a great deal about ourselves, that we can pivot, we can move forth, and that is what we need to continue to do as an organization.

[00:44:23] And so as we come out of the pandemic, we're moving more into a proactive arena. how do we work better with the business, understanding how we can use technology to innovate and provide better services. And then our future state is to be that innovator.

[00:44:42] We have to crawl and walk before we get there, because once we get to that top level, where do we go from there? So what we did was take a look and recalibrate ourselves as we move forward, as we started this journey to look at our overall strategic initiatives and what we wanted to accomplish in the next three years. So the first thing we did was we brought in an organization called Infotech Research Group. That is the fastest growing information technology and research firm. They help with strategic planning. They help to evaluate your current state and your

[00:45:20] future state. And so as we looked at this, we wanted to make sure we're moving from a reactive to a proactive and eventually to that innovation state. And addressing the core element of one of our 10 principle, which is to be a more effective and efficient government. And how did we get there? First of all, we took a look and make sure our missions were in line. Then we took a look at our visions to make sure they were in line. In the county, we looked at the values. And then we came up with our current guiding principles to address those values. And I just want to step through some

[00:45:56] of those guiding principles with us. As we talked about the IT strategic alignment, that was to provide technical strategies that align with the county's strategic direction. Our enterprise value focus was to provide that vision and leadership and that framework to evaluate and use emerging technologies. Customer-centric was to deliver the best experience to our customers, and there's three categories I would like to hone in on that. To know me, to value me, and to trust me.

[00:46:27] They are the core principles around looking at that whole support model for customer services. Innovation. We want to embrace innovation that enhances the digital experience and the modernization that we need to do as a county.

[00:46:43] And engage in resilient workforce, develop and maintain the technical skill sets to be competent in the current emerging technologies. As strategic collaboration, we wanted to make sure we were collaborating with our agencies to understand their business needs and to improve the overall county operations.

[00:47:03] Compliant and secure, you heard a lot from Charlie early, we want to continue to maintain our overall policies and procedural frameworks around laws or regulations to support the appropriate security and privacy concerns. Next slide.

[00:47:21] One of the things we asked InfoTech to do for us was to do a 360-degree evaluation of the current value of IT in the county and how we deliver IT in the county. When I first got this report, I'll be honest with you, I was kind of taken aback when I seen a lot of yellow, not a lot of green, but definitely not any red.

[00:47:43] But as I worked with the organization to understand this overall framework and what they were using, actually, they were very ecstatic about how well the county rated in this overall performance evaluation.

[00:47:59] This overall evaluation was compared to IT industries as a whole. So it's not looking at government. It's looking at the big corporations and where we fare in that overall evaluation. And if you look at IT satisfaction, we're only 2% off the average of some of those major industries.

[00:48:20] And if you look at IT value, we're actually average on IT value according to some of those leading industries. So that says a lot for the county in the way we're moving forth in the technology. And as you get to the middle section, although that's yellow, what they told me, Greg, being yellow is not bad.

[00:48:41] Because in that middle section, you're only off about anywhere from 2% to 7% of being above average or at average. And so I think we're moving in the right direction. And as you can see at the bottom, when you get to security, we're above average on a lot of that.

[00:48:58] And so that says a lot to the county and the investment as a board as you put into IT. We'll talk about some of the leading areas and improvement areas. I'll let Nate talk a little bit about that. So on the right-hand slide, part of this slide, there's the leading areas, which are the top three, and then the improvement areas, which are the lower three.

[00:49:19] How we did this is there's two different columns. One is satisfaction and one is importance. Satisfaction means really, am I satisfied with what is being delivered as a customer? Importance is what I consider as a customer to be important.

[00:49:35] So as you can see here on satisfaction rating on the top three, we have IT security, data quality, and network and communications infrastructure. As the importance, you see network and communication infrastructure, you see those related, IT security in both columns, but you see IT innovation as being something that's important, but not in the top three. In the bottom three, we look at the satisfaction. You could see that IT innovation, our customers are not as satisfied as they think they should be in innovation for IT,

[00:50:11] projects, and client-facing technology. And the importance are requirements gathering for the lower three. So these are the lower threes that aren't as important. Requirements gathering work orders in IT policy. Now, as you can see there, IT innovation is a high importance, but it's been a low satisfaction. That is sort of what correlates for us to look at this to say, how do we improve that innovation and to move that forwards as an IT organization to get more satisfied customers

[00:50:45] and also advance or drive the county and the IT forwards for initiatives that we have. And just a little bit more on the IT innovation, as we took a deeper dive into that, a lot of that is around

communications, being able to get out and tell the agencies what we have in our toolkit and how that could be used to innovate and improve efficiencies within the agencies.

[00:51:12] So that's something we're going to work on over the next course to make sure we get that in alignment with where we want it to move within those business areas. Let's move on to the next slide.

[00:51:27] So as we look at this next slide, it looks like Jenga, but really what we wanted to really hone in on here is where we are within this stack. And as you look at the bottom tier, 82% of industry is in those last two tiers.

[00:51:48] And the top three tiers is only 18% of business, IT business industry or IT industry that's in those three categories. and for us as a local government to be placed in that top three in that top 18 or in that low percentage of the 18 percent says a lot of where we're going and where we're heading with it in the county so i just wanted to draw that coalition here and showing you that we are making progress and we're progressing as a local government i don't think we'll find many local governments at that level through this industry survey.

[00:52:31] So as we move into this area of, we broke things into three tiers or areas, business support, IT excellence, and how to drive innovation.

[00:52:47] As we look at each area, it's really support, how we support the enterprise, how we run an efficient IT shop, and how we lead innovation. I think what we're really trying to move from is being more reactive and becoming really strategic thinking and moving into a more innovative area instead of being so reactive how we have been in the past and during the pandemic.

[00:53:17] To do that, we have to elevate what we're looking at and how we evaluate not only projects and business needs, but also how do we support the business to help them to also elevate to be more innovative. When we look at these things, it's enabling the community to make sure they have access to services. When we talk about business support, formalizing security governance and boundaries, those boundaries could be in cloud, they could be in service providers, they can be in partners. How do we make sure we understand where those boundaries are? As we talked previously

[00:53:54] about data and data access. How do we support different services? SaaS services, hybrid clouds, those are something of a path forwards for us. So we have to understand how do we support those specific initiatives through business support? How do we align those business requirements to the policies and the policies needed for us to move forwards? It's not about just an initiative, but the policies associated to that.

[00:54:23] And also, how do we standardize that from a security perspective, from an operational perspective? How do we make sure that as we move forwards, we are understanding what that business support is, and we align that with the needed standards and security and interoperability for moving forwards?

[00:54:45] and also skills and resources. As we'll talk later on, that is essential for us. When we talk about internal resources, when we talk about retention and other things, we have to also understand how do we manage those and have the right talent inside of Fairfax County to manage those future states. And then the second one we're going to talk about is IT excellent. And what is IT excellent and what are we hoping to gain from that.

[00:55:18] And number one is in improving our overall access to modern applications. We have to get into the mode of being more modern with our applications. And it's not just changing to a new application, but it's looking at the business impact and making sure that we're being efficiency in improving business process.

[00:55:38] Number one, another item under IT Excellence is increased integrity and data sharing and cost savings. How can we become better at sharing data across multiple organizations and within our own divisions within the county?

[00:55:56] But also looking holistic, how do we make sure outside of the county, how do we share that data? A good example is what we did with the CAD-to-CAD integration through the region here and how we share that information real-time, where it used to be by radio calling for mutual aid between jurisdictions.

[00:56:14] Now that's real-time through electronic services. So how do we get better in doing that is what we want to really focus on, IT Excellent. And the core of the IT Excellent is an enterprise architecture that establishes a managed practice that creates a more coherent set of principles, methods, and models that uses in the design and implementation of systems, enterprise best practices as well.

[00:56:43] And the last one, which we need to really hone in on, is driving innovation. And I like this quote, and I'll go a little more in depth in this. Today's innovation is tomorrow's expectations.

[00:56:59] That really resonates. You have to have that vision, and what we try to do as an organization is not look at what's going on in government, but what's going on in private industry. I know you guys probably heard a lot about ChatGPT, right, and how that's going, and it's ungoverned, it's an open platform, but just think of the possibilities.

[00:57:22] How could we start looking at and building business models for around ChatGPT? You look at where we're going with the overall modernization of data and integration of data here in the county and building out that whole plenary of how data is going to be used, looking at getting into domains and data lakes.

[00:57:43] Wouldn't it be nice for you as board members to be able to sit there and ask the question? And it crawls across that data and gives you that answer without calling the staff or an agency and saying, I need to understand how many of these widgets are we doing or how this business is going. That's what we want to get to as an organization.

[00:58:00] And to do that, we have to be visionaries. We have to look at what's going on in the private industry and then start modeling those use cases within the county government. And what we're trying to do now is get ahead of that way. I was in a conversation yesterday with one of our partners, and I was going through this.

[00:58:19] They were saying, I like that because you're really thinking about being on that vision. We don't want to be the leading edge. I mean, the leading edge, but we want to be on that leading edge, and that's how we're going to have to get there as being a visionary and understanding how new principles and how technology is changing daily and how do we take advantage of that using it in the government sector.

[00:58:39] So innovation is very key to where we go in the future. Okay, so on this next slide, I know this looks like a lot of information and a bunch of dots on a map, but I'll go ahead and try to explain it just a

little bit.

[00:59:00] I think what we're trying to explain here is that, and show here, is that a lot of our initiatives that we have over the last 12 months are in different areas of focus. I'm going to take one example of the data center failover.

[00:59:18] That's F, which is sort of in the top right-hand quadrant. It's really sort of outward focusing, as in like failovers from like applications and systems to get accessibility for, as well as trying to monetize or consolidate our data centers.

[00:59:35] into more efficient, cost-effective platforms. So that's really sort of trying to, as we look at these, it's really just to sort of categorize a lot of these initiatives that we have. Some of these initiatives on here are continually ever-changing and moving forward.

[00:59:55] So when we look at modernization, even though we say we've modernized, we're always looking at that next platform to move forwards. Complacency is not a thing that IT should be used to or should engage with. We can never be complacent.

[01:00:11] We have to always advance and have to always move forward. So we're always looking at that next platform. Even from security awareness and other things, we're always looking at the next. The biggest takeaway, I think, that we're trying to portray here is you look at a lot of these where you see the green ones, which are IT excellence, the blue ones, which are business support.

[01:00:31] The yellow are really the innovation. As you see here, we don't have as many innovative initiatives as I think we should moving forwards. So it's really trying to look at how are we balancing things that we're putting focus on and how are we making sure we include innovation as being part of those initiatives and balance those with the other things that we are looking at across the board.

[01:01:02] As we talked about earlier, mobile device management, that's one of them that we wanted to sort of talk about, too. You can see there that's in the bottom left-hand corner. It's obviously we're trying to improve capabilities, right? We're trying to improve and make data accessible to people in the field, as well as the mobile capabilities of being anywhere as a workforce.

[01:01:25] And it's also more inward-facing as MDM. It's not an outwardly-facing thing. So that's sort of why it's categorized on there. So I'm going to sort of stop there for this graph. It is something just to have you all look at and digest and hopefully have some questions about at some point in time.

[01:01:43] But it's really just to give you a roadmap of things that we're looking at over the past 12 months. Yeah, let me just jump in real quick. I think one of the things that's worth noting, one of those part of the graphic is cost reduction.

[01:02:00] And I think it's important for us to keep in mind as we move towards IT innovation that doing things better, doing things more efficiently, doing things maybe even from time to time in a little bit of an IT disruption manner is going to be really important for us as a county going forward and a county government.

[01:02:24] You know, we've talked a lot about some of our longer term physical challenges in terms of our commercial tax base and, you know, what are we going to do about that? Well, basically by leveraging our IT investments to do things better, to do things more efficiently, I think it's going to be really important to help us get there.

[01:02:45] So this is an, I love this, dots on a map. It's great, it's great. Excellent. Great. All right, we'll move on to the next slide. Next slide. So as we reposition ourselves to look at our next three years and what are the goals that we want to hone in on.

[01:03:05] And some of these you've probably seen in the past, and we'll talk about that. But let me begin with digital transformation. Digital transformation does not have a definite, defined, final state.

[01:03:22] Instead, it's an evolution process without an end. And it is continuing to look at improvements, process improvements, and how do we take technology to gain better efficiencies and provide better customer services.

[01:03:40] Our second tier coming down is data management. Data quality is important to support the analytic goals of accounting. As I talked about earlier about using some of the stuff with the, what we're seeing with the bot technology, AI is a key.

[01:03:57] And if you don't have good data, you won't have good AI. So they go hand in hand. And so our thing is to modernize, continue to modernize our overall data platform to take advantage of machine learning in AI and to be able to look at the data and be able to ask questions and get answers about that.

[01:04:14] You know, I kind of live in this bubble where I think more holistic and where we should be and where technology can take us. You know, you think about where we are, and I'm still trying to hone in on data and digital transformation here, is being in that innovative state.

[01:04:33] You know, right now, a lot of things you do is transactional-based. You have to go into an application, put in some certain criteria to get to where you want to get and to either register or get results or something like that. Let's take it and look at the metaphors. That's a terminology that you're hearing now in the technology area where you're converging.

[01:04:53] A lot of this data, a lot of this process, right? And looking at how do we become from transactional to sort of like a bot type of interaction. You know, it would be nice if I could say, Gregory Scott, I live on such and such address in Fairfax County.

[01:05:09] Boom, here comes what I owe as a taxpayer. Here's what I owe as part of Parks and Rec. And being able to get all that information without going in and registering and doing nothing. That's the future state. That's what we need to get as an organization to be able to get to that.

[01:05:28] And how do we start modeling and doing that in a prototype? So to do that, we have to talk about data transformation. We have to talk about the data. The next thing down is cybersecurity. You heard Charlie give a good explanation of the overall zero-trust framework, and that is to really mitigate and mitigate our vulnerabilities.

[01:05:53] But I like to put this out there. Fairfax County, as an organization, we put our faith in zero trust. And that's where our motto should be as we move forth and looking at cybersecurity and making sure we still have that investment and looking at other possibilities to protect the county's data.

[01:06:12] Cloud computing. Cloud computing is something that we're going to continue to evolve. We have our own private cloud, but we also are a hybrid cloud. So we do believe in going into other cloud environments. We do have the on-ramps to all cloud environments, such as Azure, AWS, and Google.

[01:06:33] Workforce optimization is a key, right? If I look at our organization, we have almost close to 20% over the next three years in county IT that are eligible to retire. And so that becomes an overall key

goal for us, is how do we retain, train employees and the ability to hire new staff with the emerging technology skill sets.

[01:06:58] So as we look at these goals, we're looking at key objectives and how we measure and make sure that we're meeting these marks as we move forth with this.

[01:07:13] And as we go through some of these digital transformation, it's having that availability, having that infrastructure that allows us to look at innovation and to be innovated as a county. Data management is to increase our overall use of data and getting more insight and making better decisions using the data. Cloud computing, continue looking in how we look between build or using a SAS model. Cyber security, I'm not going to hit on that a lot, but that's still a key.

[01:07:48] One of the things we're looking into cybersecurity, as we were talking about passwords and phrases, is how do we bring biometrics in, okay? Biometrics and two-factor authentication is the future of security, and we want to be there, and we're looking into how we get there and being able to integrate our current applications to take advantage of that security platform.

[01:08:13] Workforce optimization is very dear and near to me. I want to talk about some of the things we did over the past year. I don't know if we brought this to the board or not, but last year was our first time doing internships with high schools. We had a good, solid group of kids here, some that didn't even know if they wanted to get into IT.

[01:08:36] But I was over-athused about what they brought to the table. We sat down with them, and we said, you know, if you look at the Fairfax County website, what do you see, and how is it useful for your age limit? and i was taken back for what they said but their their whole thing was around gamify and so we put a challenge to them okay tell us how we can do that so we actually have a couple of them still with us during the school year we didn't

[01:09:11] want to impede on their their their school but they wanted to stay with us and so what they're working on is an application a gaming application but learns you and teaches you the county and the government, and so I thought that was really a big bang and a good thing, but then, you know, it starts us to think about a different thought pattern and how technology could be really beneficial to that age. You know, if we're looking at the core of the county as one Fairfax, then we have to bring them up too and make sure that we're addressing their needs as we move

[01:09:48] forward. The other thing that we're done is, and we're very kind of very proud of what we've been able to do over the last several years with internships with the local universities, especially in cybersecurity. We were able to bring in a post-grad, and after that grad had finished, he stayed and became an employer of the county. Although the thing we're looking at is now as you get into the millennial workforce, they're only going to be here for two to three years, and we have to be able to plan for that. That's what happened when we brought in the grad from George

[01:10:23] mason they came here they were very productive they learned and after two and a half years they left so we have to be in we have to look at that and and and understand that that is the new type of important when it comes to it talent and then how do we build on that base we're also reaching out we had a meeting last week but it got canceled we got to reschedule for next week with nova community college with their big it program and when i heard about that doing the presentation here, I definitely wrote down notes and said we're going to follow up with them.

**[01:10:59]** And so now we're looking at having them as part of our internship. So we're really looking at how do we grow talent here in this region. It's on the mind of everybody in the government, our local municipalities.

**[01:11:16]** We all are struggling with this, and it's become one of our top priorities as the COG CIO committee is to look in this and figure out how we address this as a holistic picture. And so that is one of the things that I think we're going to have to keep our eyes on.

**[01:11:33]** We're looking at active recruiting. I thank you, Mr. Herdy, for bringing up LinkedIn. Actually, we're finding now that that is where a lot of mining of new employment is done. It's people just going out there and looking at LinkedIn and finding out who has the skill set and then driving them to these ads and stuff like that.

**[01:11:52]** So it's something that we as accounting should be looking into and that we're going to be looking into as we look to recruit the new workforce. So as we continue to look at our overall strategic roadmap and our refresh plan, what we're going to do over the next several months is reevaluate and make sure that we're hitting the targets.

**[01:12:16]** Some of the things we're doing right now is we're meeting with the agencies. We've actually got the FAR strategic plan, and we're going to look at that and overlay it with our strategic plan. The police is finalizing their strategic plan. We're going to be doing the same.

**[01:12:32]** And so far we've been reached out to from other agencies because they're in the process of doing their overall strategic plan. So we want to make sure that we have a good balance of knowing what they have and how IT can overlay and meet the missions that they're projecting over the next two to three years.

**[01:12:51]** So with that, I conclude this presentation and give you some time for questions. Thank you very much, Mr. Scott. Excellent presentation. Really happy you got this consultant in and, you know, you're looking at this in a different way and thinking holistically and strategically.

**[01:13:09]** I think that's really good. First, Chairman McKay. Yeah, good presentation. Just a couple quick questions. On the survey itself that we started with, did we collect any demographic data on that? I mean, were we seeing any patterns where, you know, some of the percent responses you were getting were much higher based on an age demographic, or did we not collect that information?

**[01:13:34]** We did not collect that information. That's something we'll work with the organization for our next round. What we did at this round is look internally, look at the agencies and what they were putting on public facing as well, and aggregate that.

**[01:13:51]** But as far as getting into our customer and constituent base, that's something we'd definitely look at. I think it would be useful just partly based on the last comments that we were making here a moment ago about our young people and what their response is.

**[01:14:07]** And, you know, these may be skewed depending on where you are, what your IT acumen is, and how you see these platforms. The other question I have on the metrics and reporting on our progress. Under digital transformation, one of the metrics that's listed there is no unplanned outages, and I know, you know, ideally you don't have outages at all.

**[01:14:29]** I guess my question is, after what we went through with PLUS, which, you know, I give EIT a lot of credit. I mean, that was a major undertaking. It certainly had its headaches along the way. But do you see anything similar to that in scale where we would have to have an outage of a county system for a prolonged period of time like that that we need to be aware of?

**[01:14:52]** Because that was necessary but very painful. And I'm just trying to look out on the horizon to see is there anything like that coming our way that we need to be aware of? I want to be correct in what I say.

**[01:15:11]** And we have to anticipate that as we move forward. But how do we put in corrective measures to mitigate some of that? And I think that's some of the lessons learned that we're getting from this overall implementation. But if you look at the PLUS system alone, you're looking at a system that's been in place for 25 years, and you're trying to take a chunk of that data and put it into an organized system.

**[01:15:39]** We kind of knew it going in. We thought it would be maybe 10%, but that percentage was greater than that Because we're trying to, I'll give you an analogy, trying to take an obstacle that is oblong and trying to fit it in a very narrow hole.

**[01:16:00]** And that's what we're faced up against. And to look at that process, and, you know, we're definitely going to do an evaluation of that, but also learn from that, what should we plan for the next time. I think that's really important.

**[01:16:15]** I'm sorry, go. Do you want to? The answer is yes. As we look forward to doing and upgrading systems that have been legacy systems for many, many years, one that comes to mind is through DTA.

**[01:16:35]** We're going to have to basically take all of our programs, all of our systems, figure out how long their lifespan is, and then create a roadmap to how to make it happen, whether we have to do two systems at one time until everything is absorbed or if we can figure out better ways and better scripts.

**[01:16:55]** So what I'm going to ask Greg and team to do is look at all of our systems, the length that they have been a part of our system or a part of our family, and figure out when they're going to be expired, and then come back to this committee and say, this is where we are, this is what it's going to cost, and this is how long it's going to take.

**[01:17:17]** And then also, thank you, Mr. Hill, for bringing that up, because that's one of the points in here as well, is modernizing our systems, right? And so as we look at that, what we want to do is look at the new processes that we're implementing.

**[01:17:34]** And that's to be more in an agile process, right? So you take a system like DTA, which has multiple components, okay? How do we become agile about that and do portions of that to start that win-win situation and not trying to do a big buying?

**[01:17:51]** The big buying evolution of technology is gone, okay? So now you have to chunk these things into smaller silos or smaller implementation steps to make sure that we're successful. So that is part of our overall strategy as we move forth and looking at some of these systems as we go down that road.

**[01:18:12]** It goes back to the complacency aspect of it. I think that there was the old idea of we've deployed a platform. Great, it works. Let's just keep it working, right? That has to go away. The idea that we are continually upgrading has to be that mindset.

[01:18:32] Even through the pandemic where we've made changes, that momentum cannot stop. We have to keep that moving forwards. We have to keep where we're saying, okay, what's the next thing we need to change? Stopping and having us stop and say, okay, we're in a good spot, just makes it a harder leap and a longer outage in the future.

[01:18:56] The reason why Plus was so long is because that was a 30-year-old system that we didn't have to bring up to today. If it's a system that's a year behind, that outage is shorter. So it's really getting to the point of saying, how do we upgrade these systems? How do we keep moving forwards?

[01:19:12] And how do we keep that momentum as we progress? Yeah, I think that's really important because patching something as opposed to starting over, I mean, obviously, we expect a different time frame. But that one in particular, I wish we had had, you know, that luxury all along the way, because that amount of outage for something that is that essential to our economy, you know, is really tough.

[01:19:38] And so I think the lessons learned part of that is really important. And that kind of relates to my last question, and I'm not going to hold you to this answer, so I'll tell you that beforehand. Don't answer it. But, you know, you were talking about, you know, for lack of a better term, kind of a citizen portal where a person in the county could go in and check their real estate taxes, their car taxes, their library card, their, you know, register their kids for summer camp, all under one username and password and account.

[01:20:08] And I'm just wondering, you know, how realistic is that in terms of time frame? Because I can only imagine. I know how many passwords I have for different county activities, not including about six that we have as parents of kids in FCPS on top of it.

[01:20:25] And everything has its own platform, you know, paying for your kid's school lunch, looking at their report card, you know, going on DTA and paying your taxes and going to the libraries. and it just it it begs the question of really how far away are we from getting to a point where our county operations and I'm not suggesting schools are included in this at this point although I do think it's something down the road that you know is should be a part of the conversation but at least at this point I mean how far away are we from having something like what you described realistically are we a couple of years are we longer than that what what is your What is your estimation of that?

[01:21:07] No, I don't think we're that far off. I would say within a year or two, we should be getting to that plateau. I mean, the advance of technology and how technology is advancing, I used to say monthly, but now it's almost a weekly thing.

[01:21:24] Something else is always coming out. And being able to take advantage of some of that is what we want to do. And, you know, my objective, my goal is to start miling that, start building that business use case, and then start putting that together.

[01:21:40] And then we can mature that overall advancement of those types of things and look at it more holistic throughout the county. I think it's really important to our own efficiency and also to customer service, you know, to our residents.

[01:21:56] And, you know, most people who live in the county interface with the county on so many different ways that we just need to make sure all of our agencies understand that. You shouldn't have to have a different password to, you know, go online, look at your real estate taxes. That's different from what you have to do to figure out your dog license.

[01:22:13] That's different than what you have to do to update your library card. That's different than what you have to do to go into parks and register for a camp and pay for it or, you know, reserve a playground, you know, whatever it is. I think a lot of people in the county are, you know, there's so many different doors to go down that need so many different credentials that we probably exhaust ourselves with all those different platforms, passwords, applications, monitoring.

[01:22:39] And the more we can bring those together in one portal for a resident, I mean, I think that would be huge. Not just, like I said, from a citizen standpoint or county resident standpoint, but from an operational standpoint. And so I'm intrigued by your answer.

[01:22:55] I was thinking it was going to be longer than that, so I'm hopeful. I'm not going to hold you to that, but I am hopeful that that's how rapidly we're thinking about this because I do think it provides a relief valve that we need. You hit on a couple of good points.

[01:23:11] Just this past week, the local CIOs in Northern Virginia, we got together and we started looking at how we can better exchange information between our localities. And you talk about, one of the things we talked about was wraparound service, right?

[01:23:27] And if you look at that and look at, we need to start here internally, but looking at how do we grow that externally, you take, we're such a transit area here, right? We have residents today that are Fairfax that moved to Lowne.

[01:23:42] We have residents that are in Alexandria that moved to Fairfax County. How nice would it be to have a service where once they move, we take all that information and we port it into our system. No more coming back through, what door do I need to go in to get this?

[01:23:58] What door do I need to go in to do that? But looking at that more holistic, that's what we need to be as we look at to advance government services. So Alicia Seard-McCormick, Deputy County Executive, thank you for not holding us to it, but this is why we have Greg. He's the visionary. He and his team help us keep moving forward because they're monitoring the technology.

[01:24:18] And the bigger issue is, or the challenge we will have, is the implementation, right? all of the various levels of all of the data, all of the apps, making sure business still functions, that we're following all the protocols. But absolutely, what he's seeing is where we want to push towards, which is why we did the assessment as part of our strategy.

[01:24:35] I do want to caveat that to one thing really quick. I just want to make sure that we put a – Does someone else have a question? No, no, no, don't move on. So I think part of that, too, is it's not just the IT. It's the agencies, it's the businesses, it's the business process.

[01:24:50] To push change, there has to be that partnership to make that move. I think that when Greg says one to two years, that's when we say, hey, everybody's on board, all the agencies are on board, all the business processes, let's move forwards. Anything where there's, you know, hiccups or things to prevent that move forwards, a lot of times that's not a technology thing.

[01:25:13] So we need to make sure that everybody is ready to make that step and make those initiatives to move forwards because it's not just a DIT initiative. And we want to be helpful to doing that because I know people, you know, set up their boundaries and it's one county and we can't have all these boundaries set up.

[01:25:33] If at the end of the day we're driving towards efficiency and better customer service, we want to be helpful if there are problems along the way that we can help that. Because it is, I know it's not all a DIT thing, part of it's culture, part of it's structural, part of it's historic, but we need to get over that and get to the next level.

[01:25:51] And I think, you know, clearly I think that's where the board is, and we want to be helpful to make sure that happens with our agencies because I understand what you're up against. And just to follow on that, if we could get a list of all the different systems across county government that require separate registration, have their own basically identity, I think that would be a good place to start.

[01:26:15] So, okay, got a lot of hands up. We're going to run a little bit late, but Mr. Stork's not here. supervisor gross and thank you of course all this that we're talking about requires the board to provide the revenues and the budget for this and for too long we were really lagging i think in what we were providing for um our our it so that's just a marker i have two quick questions on slide four where you've got the leading areas and the improvement areas where you're looking when you talking about customers, are you talking about county employees as your customers and county

[01:26:53] departments, or are you talking about the general population as a whole? I'm trying to figure out who's the customer here. So on this 360 review, it was the agency's internal. Okay. Okay. But obviously in DIT, as we, being a support agency, it cascades to the customers externally that that comes into us but our this review was just for the internal customer that our customers okay very helpful on on slide seven this graph that has all the little dots where do you want those

[01:27:27] dots to be at yeah when we're when we're when you're done i i think we want them a different color no i i don't no no um i think part of this was really just to visualize to show you where I think when you look at there's other corporations that do things they call it like a magic quad. Yeah. Right. So they want them like a dot. Yes. Right. In the top right hand corner.

[01:27:51] That's not this. Right. And so what this is is really just to show that there are things that we focus on that are internally facing that aren't necessarily internally facing as in things that improve efficiencies in the government that aren't directly connected to a constituent a business. So this was really just to show that there's a broad breadth on things that happen in DIT that are in a lot of different areas and a lot of different initiatives that we have. Even the GIS, which is A, it's right in the smack dab in the middle because of how it connects in different

[01:28:31] areas and what systems it connects. I'm glad I asked the question because at Cog and some other places, we're looking at those, you know, up in the far, as far up in the corner as you can get. And I was trying to interpret that here. Thank you very much. All right. Supervisor Palczyk.

[01:28:46] Thank you. I'll keep it brief. And I really appreciate this. And I guess my question is, the things we're discussing about is something I've been wondering. How do we look at or have we considered further investments in things like user experience, engagement, deployment managers?

[01:29:01] I know it's partly IT, like you said, and partly both internal user experience as well as the external user experience and having that, as we said, be a constant improvement, right, in outreach. So I don't know if that's something that would be helpful that we've considered or that we're already doing.

[01:29:19] Some of that we're already doing, especially around our web channel. That's something that we take and get that feedback. There's some things that we're working on now based on that feedback. And as

you've seen on the chart that Supervisor Gross was saying on page 7, you see an upgrade of the web there.

[01:29:41] And what we're really doing there is really making that more AI capabilities. And just to give you what's happening there is we're actually looking at the home assistant type of devices to be able to go through that and get information about Fairfax County doing that.

[01:29:59] But we're also putting Fairfax Bot and expanding that. That bot was out there ever since the pandemic. But what we're now is we've got that into multiple areas of the county. And going forth, that bot will be able to be done in English and Spanish.

[01:30:17] And so we're trying to adjust and move forward with that, with our language barrier. That's one of the things that we want to make sure we address as we're looking forward with this as well. So I appreciate that. I guess, and correct me if I'm wrong, the way it's done in the, I guess, IT and beyond sectors, the whole UX, is taking those small pieces and really looking at them more universally and having that constant design.

[01:30:43] So as we look at DTA, 100% agree we need to go there. But is that an opportunity for us to start saying, we need UX across the board, and we need UX, and perhaps people who have been doing that to be able to say there's the human factor of it, there's the IT factor of it, there's the scalability, and then there's the how do we work across different agencies and then the government side.

[01:31:07] So I don't know if that's something we're looking at already or where we are. When we look at new platforms, new applications, we look at the consistent user experience as well, not just user experiences of how they use that platform or what is the process associated to it, and also what is the follow-up from it, but making it consistent from a standard across the board.

[01:31:31] So those are things we also take into consideration as well when we look at new platforms and new deployments. So there is a consistency perspective from that. But user experience is huge, especially when we look at a good user experience versus a bad user experience.

[01:31:50] That is something we also take into consideration of how they not only have felt the experience was, sentiment of it, but also making sure that that's something that they want to experience again in the future.

[01:32:06] Yeah, and I guess if there's a way when you share, and I love what you're doing, when you're sharing that with us or when we're looking at enhancing our IT systems, if there's an easy way, I don't know how the field does it, to continually share that with us, to understand where we are on UX and on design and as we look at incorporating and rolling out new systems, such as, you know, such a big piece of it is the human factor.

[01:32:31] So, if there's a way for us to continually see that and understand where we are with UX and where we're going, at least I think I would find that pretty helpful. So, thank you. Thank you. All right. Supervisor Faust. Thank you.

[01:32:48] Thank you for your presentation today and thank you for years and years and years of protecting us. I mean, it's, it is, when you hear horror stories from other companies and governments and so forth, having you guys and your team is just awesome. The, you know, the conversion to plus we talked about, that's behind us. And it was difficult. And everybody knows why. And we appreciate that you were able to get it done. The questions that are coming

[01:33:22] up now are, you know, like user questions, whether it's user friendly enough, and I was wondering, is there an ongoing effort to, you know, listen to what, get feedback from the users and to address those concerns?

[01:33:40] Yes, yes. We do a weekly meeting with the business side of PLUS, which includes all areas of the PLUS team, and we're constantly looking at this, and one of the things we engaged last week was uh you know i shared with them what was coming up in the district and what they're doing they're actually going through the same type of thing we're going through is a new permitting system right and how they're getting in front of it and some of the things that we're going to start looking at and figuring out how do we give a better experience to our customers and using that and so so that's like having a permit wizard which will take you through

[01:34:19] the different steps if you're applying for this here's this and it's integrated with the system So it takes you right into the system and helps to give you that information, how to use it and how to fill out that permit or that application. So we definitely, you know, when you put up a system, you're always looking for ongoing improvements.

[01:34:37] And this is an area I think would benefit because from what we're hearing and still hearing from the business community and the building community is to make it, how do we make it better for them and give them a better user experience? So that's things that we have always taken into consideration and trying to build out that sort of like wizardry type of implementation to step them through that.

[01:35:00] That's wonderful. The other question I had just quickly, we've talked over the years about a mechanized project management system that, for example, in the transportation department, is there progress being made on that or has it been implemented?

[01:35:20] We're making progress. Yes, we haven't fully implemented that, but that's something that, you know, as we look at the overall project management and things that we're doing there, one of the things that we got out of our overall assessment is better project management and how do we really hone in on that.

[01:35:37] And we've got some areas that we're actually looking at and trying to get up and get improvement on. So, yes, it's still on our side. Just for my information, because I really am interested in that kind of stuff, Could you send me some information on where you're at and where you're working? Yes. Thank you.

[01:35:53] Okay. Thank you. All right. Thank you. And with apologies to Supervisor Stork, we have one more question. Supervisor. Just one more question. No, it's interesting as I sit here and listen, and I'm just going to ask the question, who do you really consider the user every time you talk user?

[01:36:12] I really consider our whole universe. I mean, as I'm talking the agency, as I'm talking with public interaction, That's a user of our technology. And that's why I appreciated you bringing up the whole cultural thing.

[01:36:28] And I noticed the 360 survey was really done on your internal customers, counting on them to give you the feedback from the external customers. And that doesn't always happen as good as it does. There are some agencies. I know DTA surveys their customers all the time, zoning and permitting.

**[01:36:47]** Not so. So I think that's the challenge more for the county executive How does he get the agencies on board with that, you know, the user satisfaction that you're looking for in the surveys of our external customers need to be wrapped into kind of that whole IT experience.

**[01:37:06]** So just a two-second comment. I'm a big fan of Leading Edge. I'm not a big fan of Bleeding Edge. So, I mean, just I'm sure you're keeping that in mind as you go through this. And I do appreciate, in addition to your presentation, your comments on workforce, because I think we're going to have to be very creative, especially in the IT area, but workforce is the challenge of the future.

**[01:37:27]** As you said, when people stay two years, the pensions don't, that doesn't, you know, that doesn't help pull people in, you know, remote workers. The IT world has gone to remote workers. We need to be able to hire workers from across the country that don't necessarily work in Maryland, Virginia, or live in Maryland, Virginia, D.C. or West Virginia, whatever those states we require them to live in.

**[01:37:49]** So I think we've got some work to do there. Because it's not just going to be IT where we have those issues in the future. And that's all I got. All right. Thank you. Appreciate it. Thank you for all the great presentation, the great discussion.

**[01:38:04]** I think we have some topics for future IT committee meetings as well. So thank you. And Mr. Storkhausen, five minutes. Okay. IT committee meeting is adjourned. Thank you.




Coraggio Consulting · aguyonx.com