U.S. Department of Homeland Security
Privacy Office

Data Privacy and Integrity Advisory Committee (DPIAC)
Public Meeting Teleconference

April 26, 2022
90 K Street, N.E.
12th Floor, Room 1204
Washington, D.C. 20002

Transcribed by:
Alderson Court Reporting
Washington, D.C. 20036
(202) 289-2260

Table of Contents

PROCEEDINGS……4
Agenda Item: Call to Order and Roll Call……..……4
Agenda Item: Chairperson Remarks……6
Agenda Item: Chief Privacy Officer Remarks……6
Agenda Item: Subcommittee Report -- Information Sharing Across the DHS Enterprise……7
Agenda Item: Full Committee -- Discuss and Vote on Recommendations……..10
Agenda Item: Subcommittee Report -- DHS's Transition to Cloud Services……15
Agenda Item: Full Committee -- Discuss and Vote on Recommendations……..19
Agenda Item: Public Comment……...20
Agenda Item: Adjourn……21

Committee Members Present:

Lisa J. Sotto, Chair
William Bice, Designated Federal Official
Dennis Dayman
Michael Fitzpatrick
Mark A. Francis
Sarah Knight
John Kropf
Rosal Mashall
Ade Odutola
Chris Pahl, Ph.D.
Charles C. Palmer, Ph.D.
Harriet Pearson
Tom Plofchan
Sasha Romanosky, Ph.D.
N. Cameron Russell
Thomas Siu
Chris Teitzel
Ray Thomas, Jr.
Ron Whitworth

Other Participants:
Lynn Parker Dupree, Chief Privacy Officer

PROCEEDINGS

Agenda Item: Call to Order and Roll Call

MR. WILLIAM BICE: Good morning, everyone, and welcome. It is now 10:00 a.m., and the public meeting of the Data Privacy and Integrity Advisory Committee is now called to order.

We have committee members and members of the public joining us today. If you have any difficulties hearing or seeing at any time, please let me know. And remember to please mute your microphones until the time for the Q&A or public comment section is announced.

The meeting agenda and items were posted earlier on the advisory committee website. That is listed under "meeting information."

I will take a roll call before I turn it over to our committee chairperson, Lisa Sotto, for opening remarks.

Sharon Anolik? Sharon?

[No response.]

MR. WILLIAM BICE: Okay. Dennis Dayman?

MR. DENNIS DAYMAN: I am present.

MR. WILLIAM BICE: Thank you, sir. Michael Fitzpatrick?

MR. MICHAEL FITZPATRICK: Present.

MR. WILLIAM BICE: Thank you, sir. Mark Francis? Mark Francis?

[No response.]

MR. WILLIAM BICE: Okay, moving on. Sarah Knight? Sarah Knight?

[No response.]

MR. WILLIAM BICE: John Kropf?

MR. JOHN KROPF: Present.

MR. WILLIAM BICE: Thank you, sir. Rosal Mashall?

MS. ROSAL MASHALL: Present.

MR. WILLIAM BICE: Thank you. Ade Odutola?

MR. ADE ODUTOLA: Present. Thank you.

MR. WILLIAM BICE: Thank you. Chris Pahl? Chris Pahl?

[No response.]

MR. WILLIAM BICE: Charles Palmer? Charles Palmer?

[No response.]

MR. WILLIAM BICE: Harriet Pearson? I believe I saw her come on.

MS. HARRIET PEARSON: I am here. Hello.

MR. WILLIAM BICE: Thank you. Tom Plofchan?

MR. TOM PLOFCHAN: Good morning.

MR. WILLIAM BICE: Good morning. Thank you.

Sasha Romanosky?

DR. SASHA ROMANOSKY: Here.

MR. WILLIAM BICE: Thank you. Cameron Russell?

MR. N. CAMERON RUSSELL: Present.

MR. WILLIAM BICE: Thank you. Thomas Siu?

MR. THOMAS SIU: Good morning. Present.

MR. WILLIAM BICE: Good morning. I see Ms. Sotto.

Chris Teitzel?

MR. CHRIS TEITZEL: Present.

MR. WILLIAM BICE: Thank you. Ray Thomas?

MR. RAY THOMAS, JR.: Present.

MR. WILLIAM BICE: Thank you. Surbhi Tugnawat? Surbhi?

[No response.]

MR. WILLIAM BICE: Okay. Thank you again for joining us, and I'll now turn this over to Ms. Sotto.

Thank you.

Agenda Item: Chairperson Remarks

MS. LISA J. SOTTO: Thank you so much, Bill, and apologies for joining by phone. My computer was not cooperating.

So thank you all very much for joining us today. Good morning, and welcome to this meeting of the Data Privacy and Integrity Advisory Committee.

Before we begin, I'd like to remind everyone to please mute your mikes while committee members are discussing and voting on the recommendations that we will be making today. Any members of the public who would like to address the committee during the public comment portion of the session, we ask that you please email us at privacycommittee@hq.dhs.gov, or you can write it in the chat on your computer.

So the purpose of today's meeting is to allow the full committee to review and vote on recommendations from the committee's October 2020 taskings on information sharing, as well as the Department's transition to cloud services.

So I will now turn it over to Chief Privacy Officer Lynn Parker Dupree, who will provide some brief remarks, and then we will dive into our taskings.

Agenda Item: Chief Privacy Officer Remarks

MS. LYNN PARKER DUPREE: Thank you very much, and good morning, everyone. Thank you for joining today's Data Privacy and Integrity Advisory Committee meeting. I'm happy to have the opportunity to greet you all again and to thank you for your work on behalf of the public and the Department.

At our last meeting, I gave you all an update on the Privacy Office's recent work and the current priorities for the office. Today, the focus of this meeting is on your response to previous taskings. I appreciate all the work that you've done to determine if there are associated privacy risks associated with the Department's transition to cloud services that would merit a new-term tasking and for your consideration of best practices to ensure the effective implementation of privacy

requirements for information sharing across the DHS enterprise.

I look forward to reviewing your recommendations in these areas, and thank you again for sharing your expertise on these issues with us.

MS. LISA J. SOTTO: All right. I think back to our task at hand. Thank you so much.

So it's now time to move forward with committee activities, and I will turn the floor over to Dennis Dayman. Dennis is chair of the Policy Subcommittee.

Agenda Item: Subcommittee Report -- Information Sharing Across the DHS Enterprise

MR. DENNIS DAYMAN: Well, thank you very much, Lisa. I appreciate that.

And welcome, everybody. I'll quickly walk through a little bit on what our Policy Subcommittee was tasked with, and as we go through this, we'll be presenting on the slide deck. So on the first slide here, I just wanted to talk a little bit about what our fact-finding has been.

The committee, the DPIAC Committee, as you know, was tasked with providing any recommendations on how the Privacy Office could better oversee any information sharing practices within DHS or other additional offices or other components. Those other components could be in relation to other Federal agencies, foreign partners, or even in the private sector.

And to really understand the existing information practices that DHS had, this subcommittee and its members reviewed a lot of different documents, including things from the public and the nonpublic materials side from DHS. We did meet over the last year or so with DHS personnel to look at how the governance structures are within DHS and how they work with leveraging governance bodies and any technologies to track any of the information sharing practices that are happening within DHS.

We also looked at several other additional distinct processes, such as privacy compliance documentation like privacy impact assessments, or any other departmental processes that could be leveraged or, again, looking at what any updated or establishing any updated privacy policies would happen.

As we move to the next slide, as a reminder, the Privacy Office within DHS already has a framework of policies, procedures, and guidance to administer its privacy program very well and has statutory authority to ensure that DHS across the board has information sharing agreements and that they also comply with any Privacy Act or the E-Government Act, as well as DHS's own privacy policies.

The privacy policy for renewing -- for reviewing those information sharing access agreements is really rooted in the Homeland Security Act of 2002, which really calls for the office to ensure that its use of technology sustains and does not, obviously, erode any privacy protections. And it also instructs that office to work with other privacy officers and other privacy points of contacts and employees to make sure that they're submitting things like their information sharing access agreements, or ISAAs, in any PII sharing that DHS does.

So, again, the Privacy Office does a very good job of this. And again, what we are tasked with here is to look at how further we can improve with today's change in technology, with today's change within the Government, and as DHS grows in a lot of different ways, again, how they could continue to do that.

So if we move to the next slide here, I'll give you just a quick overview, and then we'll walk through the three or so or the paces of recommendations that we have to this. But the overview is that we know the information sharing access agreements may inherently require obviously sharing of PII to achieve any projects that DHS might be working on, right? And any improper use or disclosure of information may impact obviously national security or other interests of the United States, or it could harm the individual that the PII relates to or violate any laws. And obviously, the ISAA should adopt a specific set of consistent baseline controls to prevent that stuff from happening and procedures.

The subcommittee's recommendations really are based on three central objectives, right, to address the privacy of PII within these ISAAs. Things such as greater consistency across any ISAA that might be put out, any greater oversight or accountability of information sharing access agreements, and then a greater engagement across all DHS offices and components related to this information sharing that's happening. And that these following objectives are really now coming out of this tasking or coming from the tasking that was given to us.

The OIG report that had already been released prior to this and any materials and information that was reviewed by this committee around, again, those privacy laws and best practices as what we've understood them to be. So -- we move to the next slide here.

So one of the first ones here is that consistency across the ISAAs that I just mentioned, right? An ISAA privacy addendum could be circulated in a template form, if you will, and be attached to any contemplated ISAA with a minimal effort, we believe, to provide significant privacy controls and oversights to those agreements.

Things such as like alerting the Privacy Office before entering into an ISAA or in the event of a security incident involving any PII or upon renewal or any mature

modifications to an existing ISAA or anywhere the past 5 years, right, or upon termination or expiring of an ISAA, or lastly, in the event of any adverse changes to impacting PII would be very helpful.

Obviously, setting a pace on requirement to comply with the applicable laws and Federal standards concerning privacy and security of PII, and then imposing basic controls on the use and disclosure of PII. And lastly, ensuring cooperation with the DHS Privacy Office as necessary.

So, again, upgrading and taking a look at these ISAAs and understanding how the organizations that would be signing off on them, right, before they go off and do any PII sharing across any organization within DHS or, again, like I mentioned earlier, within other aspects outside of DHS would be very helpful.

The second part to this is just the oversight of those ISAAs. So things like tracking systems and automization -- sorry, not automization -- and automation, right, that DHS, in talking with the Privacy Office, they have identified the need for a new compliance tracking system. While they currently have one in-house right now, and they've been working on some of these things, a new compliance tracking system with automated reporting features would be nice for the office.

And so what we're also making recommendation is that the DHS office should undertake an assessment on further developing a program called PRIV-CATS to track these ISAAs further and in more detail. And then, again, the Privacy Office should assess whether a standalone tracking system for ISAAs would be more suitable either long term or even for an interim time period while making the necessary modifications to PRIV-CATS can be done.

The second part of that oversight would be to ensure and strengthen accountability for notices to that Privacy Office, right? DHS officials responsible, obviously, for implementing ISAAs again that share that PII, they should be notifying the Privacy Office of the proposed sharing of PII through some sort of system, whether that's a Web form or an email address. And so, again, when entering into those ISAAs or, again, renewing them or expiration of them or we're discovering those changes, what I talked about before, in the consistency and adopting and the promulgating those ISAA privacy addendums would also be a big help in what this committee has found.

And then, lastly, on the oversight piece is the inventory, or the existing inventory, right? With the PRIV-CATS tracking system in place and in combination with the engagement efforts identified, the Privacy Office would be in a better position to work with different offices or DHS offices and components to inventory and identify any current ISAAs and add them to its system as well as consider whether or not any current, in-effect ISAAs should be supplemented with a privacy assessment as well.

And then lastly would be the engagement. There obviously are challenges, right, in achieving any coordination and cooperation across DHS officers and offices and components, right? Each of which have tons of limited resources and priorities and all kinds of challenges that can inhibit the necessary coordination with this Privacy Office.

While the DPIAC has limited insight into all the realities, right, and other privacy offices even outside of DHS, like our own, have faced similar challenges in other public and private sector organizations, we know that this is a problem and can be looked at as we continue to look at how those engagements can be done.

So while the DPIAC subcommittee believes that this determination should be made within the Privacy Office, possible targets could be to talk to those other component privacy offices, look at the legal functions who may negotiate and review and renew those ISAAs, and three, also can work with other personnel with authority to execute other ISAAs as required.

The ISAA privacy addendums, or the IPAs, could also be included in templates and other ISAA-related materials to promote and adopt use. And for broader outreach and education, right, there should be annual DHS privacy awareness training that can be amended to reference the importance of using ISAAs to the Privacy Office and the need to complete those privacy addendums as well.

So, in conclusion, and our last slide here for this Policy Subcommittee, would be that the recommendations presented in our full report that could be seen online already are based on privacy practices that have achieved effective results in other organizations either within the Government or within our own outside of the Government involved in data sharing for various purposes. And if adopted at the Department of Homeland Security, those recommendations might -- or may likewise result in more consistency on privacy considerations for those ISAAs, with more effective Privacy Office oversight and engagement moving forward for DHS.

So, with that, I'll turn that back over to you, Lisa, and we'll go to committee discussions and any votes.

MS. LISA J. SOTTO: Thank you so much, Dennis. And thank you very, very much to the subcommittee for your hard work on this. I know it's been a long haul, and we very, very much appreciate the work.

Agenda Item: Full Committee -- Discuss and Vote on Recommendations

MS. LISA J. SOTTO: So we'll now open it up for all committee members to

discuss recommendations by the Policy Subcommittee. As a reminder, we'll take public comment at the end of today's session. So the public is welcome to comment later on.

For members, if you have a question, please raise your hand or type it in the chat. And I'm a little hindered because I'm on phone. So, Bill, if you could help me to call on people, I would appreciate that. And if you're not speaking, please mute your mikes.

Or Sue-Ying maybe? I'm not sure who's able to -- okay. Are there any hands raised?

MR. WILLIAM BICE: Not at this time.

MS. LISA J. SOTTO: Okay. Anybody have any comment?

MR. WILLIAM BICE: One second here.

FEMALE SPEAKER: Would you like me to identify those with their hands raised?

MS. LISA J. SOTTO: Yes, that would be great.

MR. WILLIAM BICE: Yeah, I see Sasha has a comment.

MS. LISA J. SOTTO: Yes. Perfect. Okay, Sasha, please.

DR. SASHA ROMANOSKY: Yeah, hi, everyone. Sure, I'll go first and be the ice-breaker.

I was confused a little bit on the scope of the effort. The document that I had read initially spoke about how this would be useful within DHS and across -- and between DHS and other agencies and the private sector. But then the document itself seems to be just the information sharing agreements outside of DHS. And so I was wondering if somebody could clarify what the intent there is?

MR. DENNIS DAYMAN: Yeah, so I'm happy to jump on that. So I'm sorry if what I'm presenting here, just overall -- I don't know, Sasha, if you've actually read the final document that was actually published out yet, or are you looking at just the PowerPoint here?

DR. SASHA ROMANOSKY: No, I've read the document, yep.

MR. DENNIS DAYMAN: Okay, I wasn't too sure. Yeah. No, so -- yeah, so, basically, we looked at both sides of this, right? We looked at what happens

within DHS as an organization to DHS with another information sharing practice that might be happening within the Government itself outside of DHS, and that could be any additional data that might be required or used from DHS or what's in their control.

If you're asking also whether or not that might be related, I'm thinking are you asking whether that's related, so like vendors and other things or the companies that DHS might be working with? Is that also what you're looking for?

DR. SASHA ROMANOSKY: Well, I was just trying to figure out what the scope of the interest of creating, say, this IPA and disseminating the IPA was. Was it for all information sharing efforts, exchanges within DHS, or between DHS and outside DHS to other Federal agencies?

MR. DENNIS DAYMAN: It could be for both, actually.

DR. SASHA ROMANOSKY: Okay. Okay. So there was a specific caveat, I'll say, in the document that seemed to suggest it was only focusing on --

MR. DENNIS DAYMAN: Yes.

DR. SASHA ROMANOSKY: -- information sharing agreements between DHS and external partners, so other Federal agencies.

Thanks.

MR. DENNIS DAYMAN: Mm-hmm.

MR. WILLIAM BICE: Tom Plofchan has his hand raised.

MS. LISA J. SOTTO: Tom, please, go ahead.

MR. TOM PLOFCHAN: Thank you. Thank you, and good morning, everybody.

Just a quick question, Dennis. I thought the policy was comprehensive and clear in the overview of what you looked at and also the recommendations. As you've got to think about implementing that, one of the things that I think many of us have discussed before is that transition from policy to actual technical oversight when we start talking about data.

Did the team or did the group, pardon me, look into actual ways to audit outside of audit policies, but to audit from a technical perspective the movement of PII across the interagency and to others? Or is that something that you think maybe is either sufficiently covered or might be the subject appropriately of a future tasking or effort?

Thank you.

MR. DENNIS DAYMAN: I think that would be -- so, yeah. So number one is, yes, we did discuss that in terms of technology, right? We talked a little bit about PRIV-CATS and where the privacy staff and other individuals that have worked on some of the data-sharing technologies are finding problems or finding concerns or finding ways to -- not concerns, but ways to improve on that, I should say. But we did talk a little bit about how that stuff could be tracked.

We didn't get into a whole lot of detail within that because a lot of that was out of the control, if you will, of the subcommittee itself understanding every bit of the technologies that are within DHS, and trying to be able to get access to all that information would have taken a lot longer than what I think this tasking was required for us to have to go through. But it was definitely brought up, and I believe potentially is that if, as DHS is looking at these recommendations and implementing those recommendations, right, start to see that there could be other improvements within that technology side of things, that the Privacy Office could definitely put another tasking out for that from a technology perspective.

But that was not a primary responsibility of the subcommittee overall because, again, it's too wide of a review technology wise because each organization within DHS does things a whole lot differently. And then hoping that in the privacy tracking system recommendations that we're making, that we would obviously want some sort of maintenance of not only tracking the agreements, but also then how that data was shared or what technology might have been used. They could definitely do that within that system.

MR. TOM PLOFCHAN: Thanks, Dennis. That's really helpful.

And appreciating the bottom-line answer there, Lisa, if I could suggest maybe in one of our next meetings, we could discuss the opportunity to support the Privacy Office in that important question of how policy transitions to actual database or technology-based auditing. That may be something where this team has the ability to offer some valuable recommendations to Ms. Dupree.

Thank you.

MR. DENNIS DAYMAN: Thank you.

MS. LISA J. SOTTO: Thank you for that great suggestion.

MR. WILLIAM BICE: Tom Siu has his hand raised.

MR. THOMAS SIU: Thank you. I think I'm just following right in the footsteps of

my colleague Tom.

The 2022 cyber incident reporting law has basically been on the books now for almost a month, and obviously, that postdates our policy discussions around these items. I would anticipate the first test of whether these recommendations are going to be valuable will occur, but obviously, we're not even in the near part of the rulemaking session for that legislation.

So I think we should keep that in mind that there's going to be a need for sharing of post incident information, which would clearly very likely -- having been in incidents myself -- provide information about PII or at least organizations that had been the subject of incidents, well, and mostly major attacks within the Federal sphere. And I think you're going to have to -- we'll have to exercise this in DHS soon.

So I want to keep that in mind that there will be new rulemaking that may cause us to change direction. But I just really wanted to make a comment that if -- we weren't anticipating that law coming into place, and I think we'll have to do more work ahead of that.

MR. DENNIS DAYMAN: Thank you.

MR. WILLIAM BICE: No other hands raised at this time.

MS. LISA J. SOTTO: Okay. If we are finished -- any others? Just going once, going twice?

[No response.]

MS. LISA J. SOTTO: Okay. Then I would ask please each committee member to write "yes" or "no."

[Audio feedback.]

MS. LISA J. SOTTO: Apologies. Can you hear me?

MR. WILLIAM BICE: Somewhat of an echo.

MS. LISA J. SOTTO: Can you hear me now?

MR. WILLIAM BICE: Yep.

MS. LISA J. SOTTO: Okay. I just switched to the computer with some IT help.

Okay. So if we have no further discussion, if committee members could please

write "yes" or "no" in the chat as to whether we should adopt the recommendations of the report, and we'll take a tally in a bit. And if "yes" have the majority, then the full committee will adopt the report with recommendations, and we'll submit the report to Chief Privacy Officer Dupree for consideration.

[Voting.]

MS. LISA J. SOTTO: All right, I'll give it just another second.

MR. WILLIAM BICE: I would just add if anyone is calling in from the phone that is voting as a member, please indicate -- identify yourself with your vote, please.

MS. LISA J. SOTTO: Okay. I think we will go ahead. We'll continue to take "yeses," but I think we'll go ahead with our program.

So I'd like to now turn things over to Emerging Technologies Subcommittee Chairperson Chris Teitzel. Chris is going to present the tasking that his subcommittee undertook.

Chris, over to you.

Agenda Item: Subcommittee Report -- DHS's Transition to Cloud Services

MR. CHRIS TEITZEL: Thank you, Lisa.

And I want to start off by thanking the Privacy Office for all the assistance that they provided during this tasking and continue to provide to us as a subcommittee.

First off, I want to go through an overview of what the tasking was, for those that may be new or haven't seen it yet. So the Emerging Technologies Subcommittee was tasked to consider the Department of Homeland Security's transition to cloud service technologies and the enhanced capabilities that this transition has provided the Department during the COVID-19 telework environment to determine if there are any associated privacy risks that would merit a near-term tasking.

So, in short, this was a tasking to see if there are future taskings available to the office and to this subcommittee. During the October 27, 2020, meeting, then Chief Information Officer Karen Evans briefed the DPIAC on the transition her office facilitated to enable teleworking and additional cloud migration during the COVID-19 pandemic. And as a quick overview, an average daily load of 10,000 teleworkers suddenly turned into 70,000 at the beginning of the pandemic as the lockdowns were starting and the quarantines were starting.

The Homeland Security Information Network saw a 200 percent increase in traffic, and DHS's HQ VPNs saw a 483 percent increase in traffic. So as we all went through in early 2020, there was a massive transition into teleworking. Luckily, the Department was prepared for this, had already begun to institute various technologies and online capabilities such as Office 365 and others that allowed for this transition to occur. And what we saw was nothing short of amazing in handling that transition and at the same time keeping the privacy and security at the forefront.

So outside of the productivity tools like Office 365 and others and teleworking, there has been and is continuing an ongoing migration and modernization of data and services that the OCIO is in charge of. And so that includes migrating data and services to the cloud where possible. Once migrated to the cloud, if there are the ability to consolidate data centers to make sure that we have a small of footprint as possible. And then once the data centers have been consolidated, the modernization of the remaining systems that do remain on premises in order to make sure that the Department continues to use the most up-to-date technology as possible.

So on the next slide, I'll go through some of the fact-finding that we did. We met with representatives of the OCIO to discuss and better understand the transition not only during COVID, but then also through the ongoing cloud migration initiatives. And again, this is a -- this was less of a -- we weren't finding much that hadn't already been uncovered. This was already into the transition, and the migrations had been going on for a few years now.

And so really it was to check in to see what was being done and how it was being done. Each system within DHS had undergone already evaluations to be determined if they could be moved to the cloud, either based on technology or sensitivity of the information or services that it provides.

Any system that was deemed not able or not ready to be moved was documented and has documented justification for why that has to stay on premises, and that's useful. As technology continues to evolve, we can go back to those documented justifications to see are those justifications still necessary, or can it, based on new technologies and new capabilities, then move to the cloud?

And then any "legacy system" that was not migrated to the cloud, as part of that evaluation, also had plans for rebuilding on modern technology. So ensuring that even if they were staying on premises or in a DHS data center that they had the same resilience and technologies available to it as their cloud counterparts.

And lastly, we were provided with the management directives and addendums

that played a critical role in guidance for how the systems are managed and migrated. And we talked through those management directives. They're publicly available. They're very long, very deep reading. But where there are gaps -- and there are gaps because, as we all know, technology moves much faster than policy can catch up to it. And so when there are gaps in those management directives, we asked them what do you do during that process? And they said that they work with the technology partners to fill those gaps and provide the best practices.

So the Department is not making up those gaps. They're bringing in technology partners and either the folks that are building it or helping them with migration to document and provide those best practices.

So on the next slide, in the report, you'll see that we break down -- we kind of take a step back. All of us are very technically minded, and we really want to get into the details of what systems and what technologies are being used. But really with this tasking what we wanted to do was step back to a high level and just say what are the overall risks of cloud migration?

And we broke it down into four pieces -- data security, data integrity, data privacy, and user training -- which, as you can probably guess, that's all the letters in the acronym for DPIAC, right? So, first off, with data security, we wanted to make sure that we noted that inventory and categorization of data in order to identify PII and ensure that we have a clear understanding of what is where, that's first and foremost to understanding how to secure it and if it is, indeed, PII.

And then, as the cloud migrations continue, we wanted to make sure that it was noted that permissions and sharing that existed in internal systems are continued into the cloud systems because, as we all know, if data is moving, it's at its most vulnerable state. And a missed permission here or a missed sharing there can all of a sudden make data that was not supposed to be public information now available to the public.

And then also part of this as, again, modern best practices, we also wanted to highlight a zero trust model critical to the modern cloud systems that everyone is moving to and, as an industry, we're starting to adopt. And zero trust really just says that the implicit trust of being within a system cannot be trusted. And so we have to make sure that we identify and authenticate every action, even within systems that we would believe to have authenticated individuals or systems already.

So then in the data integrity portion, we wanted to make sure that data is not modified or lost in route, which, again, as anyone who's been involved in data migrations and systems migrations know that that is a risk that comes up. But then also one of the benefits and detractions from moving to the cloud is the

ability for data sprawl, if you will. And so making sure that data retention planning for the copies and backups and data as it's moving are taken care of and taken into consideration because all of a sudden now you have the ability to have multiple copies of the data potentially in insecure places.

Lastly, for -- or not lastly, but in data privacy, we wanted to make sure to highlight that cataloguing and identifying what is PII and making sure that that is constantly being reevaluated to ensure that new data that may be collected that would be deemed PII is noted and identified. But then also looking at -- and in any migration you have the opportunity to ask yourself "Is this necessary?" Is this data necessary? Is it core to the system? And so in the process of migration, data minimization is also a big process that allows for kind of the clean-up of any PII that may not need to be moved.

And then, last but not least, no system is 100 percent, and the weakest part of every system is the users. And so we wanted to highlight the need to have user trainings not only on the technologies and the systems, but why the security measures and privacy measures are in place. And that can create a trained workforce that is now proactively looking for security issues or privacy issues and can be on the lookout for them.

So the next slide is our findings. We found that DHS's ongoing cloud migrations have been conducted with appropriate care and effort to keep data secure, private, and available. With this occurring in a backdrop of a global pandemic and a massive shift to remote work, the efforts by the OCIO and everyone involved at DHS, they are commendable. As I've stated before, it is no small feat to all of a sudden have that large of a shift in the systems and really test the capabilities of them.

The policy and management directives, we found that they're being followed as expected, that it's to be expected because that's what they're there for. And then in situations where the management directives do not exist, DHS is working well with the software providers to follow industry best practices and standards while simultaneously making sure that those gaps are noted and documented and then working on updating and implementing the appropriate management directives or addendums to those management directives in order to fill those gaps.

And so we found that the Department is actively and continually working to update its management directives to, again, catch up as technology continues along.

So our recommended next steps were we didn't find any taskings that we feel are necessary, but at this time, we also wanted to say here are some recommendations from the subcommittee on potential ways that the Department could continue to bolster these efforts.

And so, first off, we recommend that DHS conducts a review and inventory of all the management directives and addendums currently in place to ensure that any new technologies are appropriately covered by internal policies. Again, this is just looking at those gaps, saying what technologies are we using that aren't covered under management directives and seeing how you can catch up and make sure that the management directives do stay up to date and are a living document.

We also recommend that DHS review its OIG audit process to ensure that after initial migration, ongoing audits are conducted in appropriate cadence, along with ensuring audits include guidelines for third-party contracts. And this is just something that we wanted to make sure that OIG is involved in these audits before the migration, during the migration, and after the migration. But then there's a cadence that occurs in an ongoing basis where OIG comes back to ensure that the system or the data still meets the management directives.

And so we wanted to make sure that the Department also looks at including guidelines for third-party contracts because those are, again, a portion of the technology and the ecosystem that moves at times faster than policy can catch up to.

And last, we recommend that DHS proactively include and evaluate both privacy and security review early on in the discussions of any system or tool or data migration, and that ensures that privacy by design principles can be followed and accounted for early in the process and not caught during an audit afterwards.

We didn't note any situations where issues were caught during the audits. We didn't see any of those. But again, as best practices, the earlier that these privacy and security considerations that we laid out previously can be looked at and accounted for, it just makes it that much better and easier to go through the process.

And so, with that, I'll turn it back over to Lisa for a discussion.

MS. LISA J. SOTTO: Thank you so much, Chris.

And I just want to thank the members of the subcommittee. This was terrific work. It took, I know, a significant amount of time to get to these recommendations, and we really, really appreciate it, and I'm sure the Privacy Office will benefit from your findings. So thank you so much.

Agenda Item: Full Committee -- Discuss and Vote on Recommendations

MS. LISA J. SOTTO: All right. Let's open it up now for all committee members to discuss the recommendations of the Emerging Technologies Subcommittee. As a reminder, we're going to take public comments at the end of the session, and this is the moment for member discussion.

So, for members, if you have a question, please raise your hand, or you can type it in the chat. And please also mute your mikes if you're not talking. So may I ask for questions?

I see none -- oh, Mr. Fitzpatrick, you have your hand raised. Please go ahead.

MR. MICHAEL FITZPATRICK: Good morning, everyone. Just also want to echo and commend the subcommittee for really excellent work.

I'm wondering within the scope of the recommendations on review and audits, I know there is mention of an appropriate cadence. I'm wondering if the subcommittee had a view on particular timeframes of when that work -- of what that appropriate cadence might be?

MR. CHRIS TEITZEL: We did discuss that. Part of what we wanted to make sure as part of this tasking is that we didn't dive too deep into the details, and we wanted to highlight that to really kind of kick off an internal processing, what is that cadence? Is it every year? Is it every 6 months? What does it look like? And it really can depend on the system and on the data that it involves.

But we did note that there was some ambiguity around that on when the OIG would come back in and how often it is. And really, with these systems, it's our recommendation that the reason why we said that needs to be looked into is because, as we all know, as we move more and more data into the cloud, those timelines likely need to shorten down and likely need to be more frequent, but we don't have an official recommendation on the exact timings for those.

MS. LISA J. SOTTO: Great. Any further questions?

[No response.]

MS. LISA J. SOTTO: Seeing and hearing none, so let's move forward to vote on the recommendations. If you could please write "yes" or "no" in the chat, and the question is should the committee adopt these recommendations as a full committee? So please write in the chat.

[Voting.]

MS. LISA J. SOTTO: Okay. And we'll tally these later. I'm not counting quite appropriately. So we'll tally these later. But assuming the "yes" have the

majority, then the full committee will adopt the recommendations, and we submit them to Chief Privacy Officer Dupree for consideration. So we'll continue to tally these later.

Let's move to the public comment session of our meeting.

Agenda Item: Public Comment

MS. LISA J. SOTTO: There were no comments to the mailbox, and nobody has preregistered to make a comment. So we'll keep the floor open to members of the public who might wish to speak.

So, please, if you do wish to speak, please write that in the chat or raise your hand, and if you could keep your remarks to under 3 minutes, we would appreciate that. If you're joining by phone, you can unmute by pressing *6.

Give it just a minute, see if there are any comments.

I see Bill. Bill, do you want to chime in?

MR. WILLIAM BICE: Yes, just one quick housekeeping note. I know that some folks joined after we did roll call so I want to get appropriate record for those individuals and make sure that I didn't miss someone because I know there are some folks calling in that may be members.

Sharon Anolik? Do not see her on the list here.

And Surbhi Tugnawat?

[No response.]

MR. WILLIAM BICE: Okay. I have Michael Fitzpatrick joined. Sarah Knight has joined. Rosal has joined, and Ron Whitworth has joined.

So I wanted to make sure that we got those on the record. Thank you.

MS. LISA J. SOTTO: Thank you for keeping us straight, Bill. We really appreciate it.

All right. Seeing and hearing no public comments, we will conclude our public comment portion.

If you would like to submit written comments, you do have an opportunity to do so. You could email them to privacycommittee@hq.dhs.gov. Please do so by May 10th. And just be aware that because the committee operates under the

provisions of the Federal Advisory Committee Act, all written comments will be treated as public documents and will be made available for public inspection.

Agenda Item: Adjourn

MS. LISA J. SOTTO: So, to conclude, many thanks to Chief Privacy Officer Lynn Parker Dupree, to our subcommittee chairs, to the subcommittee members who worked so hard on the report and the recommendations. We very, very much appreciate all your work and thank you for participating in today's meeting.

This concludes the meeting. We are grateful for your interest and encourage you to follow the committee's work by checking out our Web page. The minutes of today's meeting will be posted there in the near future.

And with that, our meeting is adjourned.

[Whereupon, at 10:46 a.m., the meeting was adjourned.]